



State of Tennessee

PUBLIC CHAPTER NO. 345

HOUSE BILL NO. 766

By Representatives Lamberth, Gant, Vaughan, Smith, Helton, Howell

Substituted for: Senate Bill No. 725

By Senators Johnson, Bailey, Stevens

AN ACT to amend Tennessee Code Annotated, Title 56, Chapter 2, relative to insurance data security.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF TENNESSEE:

SECTION 1. Tennessee Code Annotated, Title 56, Chapter 2, is amended by adding the following as a new part:

56-2-1001. Short title.

This part is known and may be cited as the "Insurance Data Security Law."

56-2-1002. Purpose and intent.

(a) This part establishes the exclusive standards for data security, licensees' investigations of cybersecurity events, and licensees' notification of cybersecurity events to the commissioner and affected consumers.

(b) This part does not create or imply a private cause of action for a violation of this part, nor does this part limit a private cause of action that otherwise exists.

56-2-1003. Part definitions.

As used in this part:

(1) "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 the licensee's information systems;

(2) "Commissioner" means the commissioner of commerce and insurance, or the commissioner's designee;

(3) "Consumer" means an individual, including an applicant, policyholder, insured, beneficiary, claimant, or certificate holder, who is a resident of this state and whose nonpublic information is in a licensee's possession, custody, or control;

(4) "Cybersecurity event":

(A) Means an event resulting in unauthorized access to, or disruption or misuse of, an information system or nonpublic information stored on an information system; and

(B) Does not include:

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

HB766

(ii) An event in which the licensee determines that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed;

(5) "Department" means the department of commerce and insurance;

(6) "Encrypted" means the transformation of data into a form that results in a low probability that its meaning is discernible without the use of a protective process or key;

(7) "Immediate family" means a spouse; child or grandchild by blood, adoption, or marriage; sibling; parent; or grandparent;

(8) "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;

(9) "Information system" means:

(A) A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic nonpublic information; or

(B) A specialized system, including an industrial or process control system, a telephone switching and private branch exchange system, and an environmental control system;

(10) "Licensee":

(A) Means a person:

(i) Licensed, authorized to operate, or registered pursuant to this title; or

(ii) Required to be licensed, authorized to operate, or registered pursuant to this title; and

(B) Does not include a purchasing group or risk retention group chartered and licensed in another state or a person acting as an assuming insurer and domiciled in another state or jurisdiction;

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

(A) Knowledge factors, such as by a password;

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

(C) Inherence factors, such as by a biometric characteristic;

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

(A) Business-related information of a licensee, in which the tampering with, unauthorized disclosure of, access to, or use of, would cause a material adverse impact to the business, operations, or security of the licensee;

(B) Information concerning a consumer that, because of a name, number, personal mark, or other identifier, can be used to identify that consumer, in combination with the following:

(i) A social security number;

(ii) A driver license number or non-driver identification card number;

(iii) A financial account number or credit or debit card number;

(iv) A security code, access code, or password that would permit access to the consumer's financial accounts; or

(v) Biometric records; or

(C) Information or data, except a person's age or sex, created by or derived from a healthcare provider or a consumer that relates to:

(i) The past, present, or future physical, mental, or behavioral health or health condition of a consumer or a member of a consumer's immediate family;

(ii) The provision of health care to a consumer; or

(iii) Payment for the provision of health care to a consumer;

(13) "Person" means an individual or non-governmental entity, including a sole proprietorship, corporation, limited liability company, partnership, trust, religious organization, association, nonprofit organization described in § 501(c) of the Internal Revenue Code that is exempt from federal income taxation under § 501(a) of the Internal Revenue Code (26 U.S.C. § 501(a)), or another legal entity, whether formed as a for-profit or not-for-profit entity;

(14) "Publicly available information" means information that a licensee has a reasonable basis to believe is lawfully made available to the public. For purposes of this subdivision (14), a licensee has a reasonable basis to believe that information is lawfully made available to the public if the licensee has taken steps reasonably necessary to determine:

(A) That the information is of a type that is available to the public through government records, widely distributed media, or public disclosures required by law; or

(B) That a consumer can direct that the information not be made available to the public and, if so, that the consumer has not made that direction;

(15) "Risk assessment" means the risk assessment that each licensee must conduct under § 56-2-1004(3); and

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

56-2-1004. Information security program.

By July 1, 2022, unless provided otherwise in this section:

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

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

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

(B) Protect against 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 a consumer as a result of unauthorized access or use; and

(D) Define and periodically reevaluate a schedule for retaining nonpublic information and a mechanism for the destruction of nonpublic information when the information is no longer needed;

(3) A licensee shall conduct a risk assessment as follows:

(A) Designate one (1) or more employees, an affiliate, or an outside vendor acting on behalf of the licensee who is responsible for the licensee's 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 threats to the security of information systems and nonpublic information accessible to or held by third-party service providers;

(C) Assess the likelihood and potential damage of reasonably foreseeable internal or external threats, taking into consideration the sensitivity of the nonpublic information involved;

(D) Assess the sufficiency of policies, procedures, information systems, and other safeguards in place to manage threats throughout the licensee's operations, including in:

(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) Detection, prevention, and response to attacks, intrusions, or other information systems failures; and

(E) Implement information safeguards to manage the threats identified in the licensee's risk assessment and, no less than annually, assess the effectiveness of the safeguards' key controls, systems, and procedures;

(4) Based on a licensee's risk assessment, the licensee shall:

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

(B) Determine which of the following security measures are appropriate for the licensee and implement those security measures:

(i) Place access controls on information systems, including controls to authenticate and restrict access 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 licensee to achieve the licensee's business objectives in accordance with the relative importance of the data, personnel, devices, systems, and facilities to the licensee's business objectives and risk strategy;

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

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

(v) Adopt secure development practices for internally developed applications utilized by the licensee and procedures for evaluating, assessing, or testing the security of externally developed applications utilized by the licensee;

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

(vii) Utilize effective controls that may include multi-factor authentication procedures for authorized individuals 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 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, technological failures, or other catastrophic events; 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) Remain informed regarding emerging threats or vulnerabilities to the licensee and utilize reasonable security measures when sharing information, relative to the nature of the sharing and the type of information being shared; or

(E) Provide 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, then the board or an appropriate committee of the board shall, at a minimum:

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

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

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

(ii) Material matters related to the licensee's information security program, including risk assessment, risk management and control decisions, third-party service provider arrangements, results of testing, cybersecurity events or violations and the licensee's responses thereto, and recommendations for changes to the information security program; and

(C) If the licensee's executive management delegates any of the executive management's responsibilities under this section, then the executive management must oversee the development, implementation, and maintenance of the licensee's information security program prepared by the delegates and must either prepare the report or receive a copy of the report prepared by the delegates pursuant to subdivision (5)(B);

(6) A licensee shall exercise due diligence in selecting a third-party service provider and, by July 1, 2023, require that each third-party service provider implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information accessible to, or held by, the third-party service provider;

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

(8)

(A) As part of a licensee's information security program, a licensee must establish a written incident response plan designed to promptly respond to, and recover from, a cybersecurity event that compromises the confidentiality, integrity, or availability of the licensee's nonpublic information or information systems or the continuing functionality of the licensee's operations;

(B) The incident response plan must address:

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

(ii) The goals of the licensee's incident response plan;

(iii) The definition of roles, responsibilities, and levels of decision-making authority relating to a cybersecurity event;

(iv) External and internal communications and information sharing;

(v) The requirements for remediating 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; and

(9)

(A) Each insurer domiciled in this state shall submit to the commissioner by April 15 of each year written certification that the insurer is in compliance with this section. Each insurer shall maintain for examination by the department all records, schedules, and data supporting the certification for a period of five (5) years from the date of the corresponding certification.

(B) If an insurer identifies areas, systems, or processes requiring material improvement, updating, or redesign, then the insurer must document planned and ongoing remedial efforts to address those areas, systems, or processes, and the documentation must be made available for inspection by the commissioner upon request.

56-2-1005. Investigation of a cybersecurity event.

(a) If a licensee learns that a cybersecurity event has or may have occurred, then 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 outside vendor or service provider shall, at a minimum:

(1) Determine whether a cybersecurity event has occurred;

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

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

(4) Take 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.

(c) If the licensee learns that a cybersecurity event has or may have occurred in a system maintained by a third-party service provider, then the licensee shall complete, or confirm and document that the third-party service provider has completed, the actions required by subsection (b).

(d) The licensee shall maintain records concerning all cybersecurity events for a period of at least five (5) years from the date of discovery of the cybersecurity event and shall provide those records to the commissioner upon request.

(e) If the licensee conducts an investigation or review of a potential or suspected cybersecurity event and determines that an event is not a cybersecurity event, then the licensee must reduce that determination to writing and maintain that writing for a period of at least five (5) years from the date of discovery of the event. The licensee shall provide the writing to the commissioner upon request.

56-2-1006. Notification of a cybersecurity event.

(a) A licensee shall notify the commissioner as soon as practicable, and in no event more than three (3) business days, following a determination that a cybersecurity event has occurred if:

(1)

(A) The licensee is domiciled in this state, in the case of an insurer, as defined in § 56-6-102, or this state is the licensee's home state, in the case of an insurance producer, as defined in § 56-6-102; and

(B) The cybersecurity event has a reasonable likelihood of materially harming a consumer residing in this state or a material part of the licensee's normal operations; or

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

(A) A cybersecurity event of which notice must be provided to a government body, self-regulatory agency, or other supervisory body pursuant to state or federal law; or

(B) A cybersecurity event with a reasonable likelihood of materially harming a consumer residing in this state or a material part of the licensee's normal operations.

(b)

(1) A licensee that must notify the commissioner under subsection (a) shall provide to the commissioner, in a format directed by the commissioner, as much of the following information as is available:

(A) The date of the cybersecurity event;

(B) A description of how the nonpublic information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers with respect to the nonpublic information, if any;

(C) How the cybersecurity event was discovered;

(D) Whether lost, stolen, or breached nonpublic information has been recovered and, if so, how recovery was accomplished;

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

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

(G) A description of the specific types of nonpublic information or particular data elements acquired without authorization, which may include types of medical information, types of financial information, or types of information allowing for consumer identification;

(H) The period during which the licensee's 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 its best estimate of this number of consumers in its initial report to the commissioner and update this estimate with each subsequent report to the commissioner pursuant to this subsection (b);

(J) The results of an internal review and whether the review identified whether automated controls or internal procedures were followed or adhered to;

(K) A description of the efforts to remediate the situation that permitted the cybersecurity event to occur;

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

(M) The name of a person who is both knowledgeable regarding the cybersecurity event and authorized to act on behalf of the licensee to

serve as a representative of the licensee for contact from the commissioner; and

(N) A copy of the notice sent to affected consumers, if the notice is required under subsection (c).

(2) Licensees shall continually provide material updates or supplements to the information provided under subdivision (b)(1).

(c) Following a determination that a cybersecurity event has occurred and that the cybersecurity event has a reasonable likelihood of materially harming a consumer, a licensee shall notify consumers residing in this state whose nonpublic information has been acquired, or reasonably believed to have been acquired, by the cybersecurity event. The disclosure must be made no later than forty-five (45) days after the determination of the cybersecurity event, unless a longer period of time is required due to the legitimate needs of law enforcement. For purposes of this section, notice may be provided by:

(1) Written notice;

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001, or if the licensee's primary method of communication with the consumer has been by electronic means. Electronic means may include email notification; or

(3) Substitute notice, if the licensee demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), the affected class of subject persons to be notified exceeds five hundred thousand (500,000) persons, or the licensee does not have sufficient contact information and the notice consists of the following:

(A) Email notice, when the licensee has an email address for the consumer;

(B) Conspicuous posting of the notice on the licensee's website, if the licensee maintains a website page; and

(C) Notification to major statewide media.

(d)

(1) If a licensee becomes aware of a cybersecurity event in the licensee's information system maintained by a third-party service provider, then the licensee must treat the event as if it occurred in an information system maintained by the licensee for purposes of subsection (a).

(2) The licensee's time limitations for purposes of providing notification under subsection (a) begin running when the third-party service provider notifies the licensee of the cybersecurity event or the licensee otherwise gains actual knowledge of the cybersecurity event, whichever is sooner.

(3) This part does not limit or abrogate an agreement between a licensee and another party to fulfill the investigation requirements imposed under § 56-2-1005 or the notice requirements imposed under this section.

(e)

(1)

(A) In the case of a cybersecurity event involving nonpublic information that is used by, or in the possession, custody, or control of, a licensee acting as an assuming insurer that does not have a direct contractual relationship with the affected consumers, the assuming

insurer shall notify the affected ceding insurers and the commissioner of the licensee's state of domicile within three (3) business days of determining that a cybersecurity event has occurred.

(B) The ceding insurers that have a direct contractual relationship with affected consumers must fulfill the consumer notification requirements required under this section.

(2)

(A) In the case of a cybersecurity event involving nonpublic information 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 the affected ceding insurers and the commissioner of the licensee's state of domicile within three (3) business days of the third-party service provider notifying the licensee of the cybersecurity event or the licensee otherwise gaining actual knowledge of the cybersecurity event, whichever is sooner.

(B) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements required under this section.

(3) Except as provided in this subsection (e), a licensee acting as assuming insurer has no other notice obligations relating to a cybersecurity event under this section.

(f) In the case of a cybersecurity event involving nonpublic information in the possession, custody, or control of a licensee that is an insurer, or the 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 this part, the insurer shall notify the producers of record of all affected consumers, if known, as soon as practicable, but not later than when such notice is provided to the affected consumers. The insurer is excused from this obligation in those instances in which the insurer does not have the current producer of record information for an individual consumer.

56-2-1007. Authority of commissioner.

(a) In addition to authority under chapter 1, part 4 of this title, the commissioner has the authority to examine and investigate a licensee to determine whether the licensee has been or is engaged in conduct in violation of this part. Those examinations or investigations must be conducted in accordance with chapter 1, part 4 of this title.

(b) If the commissioner has reason to believe that a licensee has been or is engaged in conduct in this state that violates this part, then the commissioner may take necessary or appropriate action to enforce this part in accordance with part 3 of this chapter.

56-2-1008. Confidentiality.

(a) Documents, materials, or information in the department's control or possession that are furnished by a licensee, or an employee or agent acting on behalf of the licensee, pursuant to § 56-2-1004(9) or § 56-2-1006(b), or that are obtained by the commissioner in connection with an investigation or examination pursuant to § 56-2-1007:

(1) Are confidential and not open for inspection by members of the public under title 10, chapter 7 or § 56-1-602; and

(2) Are not subject to subpoena, subject to discovery, or admissible in evidence in a private civil action, except that the commissioner may use the documents, materials, or information in the furtherance of regulatory or legal action by the commissioner.

HB766

(b) The commissioner, or a person who received documents, materials, or information while acting under the authority of the commissioner, is not permitted or required to testify in a private civil action concerning documents, materials, or information made confidential under subsection (a).

(c) Notwithstanding subsection (a), to assist in the commissioner's duties under this part, the commissioner may:

(1) Share documents, materials, or information made confidential under subsection (a) with other state, federal, or international regulatory agencies or law enforcement authorities, the national association of insurance commissioners or its affiliates or subsidiaries, or a third-party consultant or vendor of the department, as long as the recipient agrees in writing to maintain the confidential nature of the documents, materials, or information;

(2) Receive documents, materials, or information, including otherwise confidential documents, materials, or information, from the national association of insurance commissioners or its affiliates or subsidiaries, or from regulatory or law enforcement officials of other foreign or domestic jurisdictions, and the commissioner must maintain as confidential any document, material, or information received with notice or the understanding that it is confidential under the laws of the source jurisdiction; and

(3) Enter into agreements governing sharing and use of documents, materials, or information consistent with this subsection (c).

(d) A waiver of an applicable privilege or confidentiality does not occur as a result of the disclosure of documents, materials, or information by or to the commissioner under subsection (c).

(e) This part does not prohibit the commissioner from releasing final, adjudicated actions open to public inspection under title 10, chapter 7 or § 56-1-602 to a database or other clearinghouse service maintained by the national association of insurance commissioners or its affiliates or subsidiaries.

56-2-1009. Exceptions.

(a)

(1) This part does not apply to:

(A) A licensee who employs less than twenty-five (25) individuals, regardless of whether the individuals are employees or independent contractors;

(B) A licensee with less than five million dollars (\$5,000,000) in gross annual revenue; or

(C) A licensee with less than ten million dollars (\$10,000,000) in year-end total assets.

(2) A licensee subject to and governed by the privacy, security, and breach notification rules issued by the United States department of health and human services, 45 CFR Parts 160 and 164, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d et seq.), and the federal Health Information Technology for Economic and Clinical Health (HITECH) Act (42 U.S.C. § 300jj et seq. and 42 U.S.C. § 17901 et seq.), and that maintains nonpublic information in the same manner as protected health information meets the requirements of §§ 56-2-1004 and 56-2-1006(c) if the licensee is compliant with, and submits a written statement certifying its compliance with, the federal Health Insurance Portability and Accountability Act of 1996 and the federal Health Information Technology for Economic and Clinical Health.

HB766

(3) A licensee subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 (15 U.S.C. §§ 6801-6809 and 6821-6827) that meets the requirements of § 56- 2-1006(c) if the licensee is compliant with, and submits a written statement certifying its compliance with, Title V of the federal Gramm-Leach-Bliley Act of 1999.

(4) An employee, agent, representative, or designee of a licensee, who is also a licensee, is exempt from § 56-2-1004 if the activities of the employee, agent, representative, or designee are covered by the other licensee's information security program.

(b) If a licensee ceases to qualify for an exception under subsection (a), then the licensee has one hundred eighty (180) days from the time the licensee no longer qualifies for the exception to comply with this part.

56-2-1010. Penalties.

The commissioner may seek penalties under § 56-2-305 for a violation of this part.

56-2-1011. Rules.

The commissioner may promulgate rules to effectuate this part. The rules must be promulgated in accordance with the Uniform Administrative Procedures Act, compiled in title 4, chapter 5.

SECTION 2. If any provision of this act or the application of any provision of this act to any person or circumstance is held invalid, then the invalidity does not affect other provisions or applications of the act that can be given effect without the invalid provision or application, and to that end, the provisions of this act are severable.

SECTION 3. The headings to sections in this act are for reference purposes only and do not constitute a part of the law enacted by this act. However, the Tennessee Code Commission is requested to include the headings in any compilation or publication containing this act.

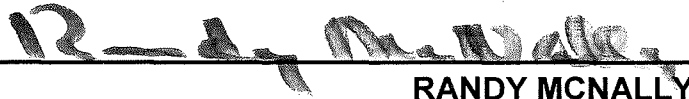
SECTION 4. For the purpose of promulgating rules, this act takes effect upon becoming a law, the public welfare requiring it. For all other purposes, this act takes effect July 1, 2021, the public welfare requiring it, and applies to breaches that occur or are discovered on or after that date.

HOUSE BILL NO. 766

PASSED: April 21, 2021



CAMERON SEXTON, SPEAKER
HOUSE OF REPRESENTATIVES



RANDY MCNALLY
SPEAKER OF THE SENATE

APPROVED this 6th day of May 2021



BILL LEE, GOVERNOR