FIRST REGULAR SESSION

SENATE BILL NO. 385

103RD GENERAL ASSEMBLY

INTRODUCED BY SENATOR TRENT.

0432S.01I KRISTINA MARTIN, Secretary

AN ACT

To amend chapter 375, RSMo, by adding thereto twelve new sections relating to insurance companies' data security, with an effective date.

Be it enacted by the General Assembly of the State of Missouri, as follows:

Section A. Chapter 375, RSMo, is amended by adding thereto twelve new sections, to be known as sections 375.1400, 375.1402, 375.1405, 375.1407, 375.1410, 375.1412, 375.1415, 375.1417, 375.1420, 375.1422, 375.1425, and 375.1427, to read as follows:

375.1400. 1. Sections 375.1400 to 375.1427 shall be known and may be cited as the "Insurance Data Security Act".

2. Notwithstanding any other provision of law to the contrary, sections 375.1400 to 375.1427 establish the exclusive state standards applicable to licensees for data security, the investigation of a cybersecurity event as defined in section 375.1402, and notification to the director.

3. Sections 375.1400 to 375.1427 shall not be construed to create or imply a private cause of action for violation of their provisions, nor shall such sections be construed to curtail a private cause of action that would otherwise exist in the absence of sections 375.1400 to 375.1427.

375.1402. As used in sections 375.1400 to 375.1427, the following terms mean:

(1) "Authorized person", an individual known to and authorized 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;

(2) "Consumer", an individual including, but not limited to, 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;

(3) "Cybersecurity event", an event resulting in unauthorized access to, malicious disruption of, or misuse of an information system or nonpublic information in the possession, custody, or control of a licensee or an authorized person; however:

(a) 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; and

(b) The term "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;

(4) "Department", the department of commerce and insurance;

(5) "Director", the director of the department of commerce and insurance;

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

(7) "HIPAA", the federal Health Insurance Portability and Accountability Act (42 U.S.C. Section 1320d, et seq.);

(8) "Information security program", 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", 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 and process controls systems, telephone switching and private branch exchange systems, and environmental control systems;

(10) "Licensee", any person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered under 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 licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction;

(11) "Multi-factor authentication", 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; or

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

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

(a) Business-related information of a licensee, the tampering with which, or unauthorized disclosure, access, or

use of which, would cause a material adverse impact to the business, operations, or security of the licensee;

(b) Any information concerning a consumer that, 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:

a. Social Security number;

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

c. Financial account number or credit or debit card number;

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

e. Biometric records; or

f. Military identification number;

(c) 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 and that relates to:

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

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

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

The term "nonpublic information" does not include a consumer's personally identifiable information that has been anonymized using a method no less secure than the safe harbor method under HIPAA;

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

(14) "Publicly available information", 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 subdivision, 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:

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

(b) 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;

(15) "Risk assessment", the risk assessment that each licensee is required to conduct under subsection 3 of section 375.1405;

(16) "State", the state of Missouri;

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

375.1405. 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 that is 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:

(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; and

(4) 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:

(1) 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;

(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:

(a) Employee training and management;

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

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

(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.

4. Based on its risk assessment, the licensee shall:

(1) Design its information security program to mitigate the identified risks, commensurate with the size and complexity 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;

(2) Determine which of the following security measures are appropriate and implement such security measures:

(a) Place access controls on information systems, including controls to authenticate and permit access only to authorized persons 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 access at physical locations containing nonpublic information only to authorized persons;

(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 utilized by the licensee and procedures for evaluating, assessing, or testing the security of externally developed applications utilized by the licensee;

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

(g) Utilize effective controls, which may include multi-factor 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; and

(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 and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared; and

(5) 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:

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

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

(a) The overall status of the information security program and the licensee's compliance with sections 375.1400 to 375.1427; and

(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 its responsibilities under section 375.1405, it 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.

6. (1) A licensee shall exercise due diligence in selecting its third-party service provider.

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

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

(2) The goals of the incident response plan;

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

(4) External and internal communications and information sharing;

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

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

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

9. Annually by April fifteenth, each insurer domiciled in this state shall submit to the director a written statement 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 three 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 shall be available for inspection by the director.

375.1407. 1. If the 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.

2. During the investigation, the licensee, or an outside vendor or service provider designated to act on

behalf of the licensee, shall, at a minimum, determine as much of the following information as 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; and

(4) 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 shall 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 three years from the date of the cybersecurity event and shall produce those records upon demand of the director.

375.1410. 1. Each licensee shall notify the director as promptly as practicable, 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 a 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, as those terms are defined

in section 375.012, and the cybersecurity event has a reasonable likelihood of materially harming a consumer residing in this state or a reasonable likelihood of materially harming any material part of the normal operations of the licensee; or

(2) The licensee reasonably believes that the nonpublic information involved is of one thousand or more consumers residing in this state and is either of the following:

(a) 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 under any state or federal law; or

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

a. Any consumer residing in this state; or

b. Any material part of the normal operations 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 director. The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the director regarding material changes to previously provided information relating to the cybersecurity event:

(1) The date of the cybersecurity event;

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

(3) How the cybersecurity event was discovered;

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

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

(6) 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;

(7) A 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;

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

(9) 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 director and update this estimate with each subsequent report to the director under this section;

(10) 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;

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

(12) 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

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

3. The licensee shall comply with section 407.1500, as applicable, and provide a copy of the notice sent to consumers under that section to the director when a licensee is required to notify the director under subsection 1 of this section.

4. (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, the licensee shall treat such event as it would under subsection 1 of this section.

(2) The computation of a 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.

(3) Nothing in sections 375.1400 to 375.1427 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 375.1407 or notice requirements imposed under this section.

5. (1) (a) In the event of a cybersecurity event involving nonpublic information that is used by the licensee that is acting as an assuming insurer or in the possession, custody, or control of a licensee that 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 or director of insurance for 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 imposed under section 407.1500 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 the state.

(2) (a) In the event 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 or director of insurance for 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 imposed under section 407.1500 and any other notification requirements relating to a cybersecurity event imposed under this section.

6. 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 law, including section 407.1500, 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 those instances in which it does not have the

current producer of record information for any individual consumer.

375.1412. 1. The director 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 sections 375.1400 to 375.1427. This power is in addition to the powers the director has under the law. Any such investigation or examination shall be conducted under section 374.190 or 374.205.

2. Whenever the director has reason to believe that a licensee has been or is engaged in conduct in this state that violates sections 375.1400 to 375.1427, the director may take action that is necessary or appropriate to enforce the provisions of sections 375.1400 to 375.1427.

375.1415. 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 under subsection 9 of section 375.1405 or subsection 2 of section 375.1410 or that is obtained by the director in an investigation or examination under section 375.1412 shall be confidential by law and privileged, shall not be subject to disclosure under chapter 610, shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action. However, the director 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 director's duties.

2. Neither the director nor any person or entity who received documents, materials, or other information while acting under the authority of the director 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. Consistent with the insurance data security act's goal of safeguarding consumer nonpublic information, neither the director nor any person or entity who receives documents, materials, or other information while acting under the authority of the director shall be permitted to share or otherwise release the documents, materials, or other information to a third party including, but not limited to, other state, federal, or international regulatory agencies or law enforcement agencies.

4. In order to assist in the performance of the director's duties under sections 375.1400 to 375.1427, the director:

(1) 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; and

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

5. 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 director under this section or as a result of sharing as authorized in subsection 3 of this section.

6. Nothing in sections 375.1400 to 375.1427 shall prohibit the director from releasing final adjudicated actions that are open to public inspection under chapter 610 to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates, or subsidiaries.

375.1417. 1. The following exceptions shall apply to sections 375.1400 to 375.1427:

(1) A licensee with fewer than ten employees, including any independent contractors, is exempt from the provisions of section 375.1405;

(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 160 and 164, established under the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, and the Health Information Technology for Economic and Clinical Health Act (HITECH), P.L. 111-5, and that maintains nonpublic information in the same manner as protected health information shall be deemed to comply with the requirements of sections 375.1400 to 375.1427, except for the director notification requirements in subsections 1 and 2 of section 375.1410;

(3) An employee, agent, representative, or designee of a licensee, who is also a licensee, is exempt from section 375.1405 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;

(4) Producers that have fewer than fifty employees, less than five million dollars in gross annual revenue, or less than ten million dollars in year-end total assets; and

(5) 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 (Interagency Guidelines) as set forth under Sections 501 and 505 of the federal Gramm-Leach-Bliley Act, P.L. 106-102, shall be considered to meet the requirements of section 375.1405 and any rules, regulations, or procedures established thereunder, provided that the licensee produces, upon request, documentation satisfactory to the director 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 calendar days to comply with sections 375.1400 to 375.1427.

375.1420. In the case of a violation of sections 375.1400 to 375.1427, a licensee may be subject to penalties as provided by law, including sections 374.046, 374.048, and 374.049.

375.1422. The director of the department of commerce and insurance may promulgate rules as necessary for the implementation of sections 375.1400 to 375.1427. Any rule or portion of a rule, as that term is defined in section 536.010, that is created under the authority delegated in this section shall become effective only if it complies with and is subject to all of the provisions of chapter 536 and, if applicable, section 536.028. This section and chapter 536 are nonseverable and if any of the powers vested with the general assembly under chapter 536 to review, to delay the effective date, or to disapprove and annul a rule are subsequently held unconstitutional, then the grant of

rulemaking authority and any rule proposed or adopted after August 28, 2025, shall be invalid and void.

375.1425. If any provision of sections 375.1400 to 375.1427 or the application thereof to any person or circumstance is for any reason held to be invalid, the remainder of sections 375.1400 to 375.1427 and the application of such provision to other persons or circumstances shall not be affected thereby.

375.1427. Licensees shall have until January 1, 2027, to implement section 375.1405 and until January 1, 2028, to implement subsection 6 of section 375.1405.

Section B. Section A of this act shall become effective on January 1, 2026.

✓