SENATE SUBSTITUTE

FOR

HOUSE COMMITTEE SUBSTITUTE

FOR

HOUSE BILLS NOS. 974, 57, 1032 & 1141

AN ACT

To amend chapters 375 and 379, RSMo, by adding thereto twenty-seven new sections relating to insurance modernization through standards governing digital systems, with a delayed effective date for certain sections.

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

Section A. Chapters 375 and 379, RSMo, are amended by adding thereto twenty-seven 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, 375.1427, 379.1900, 379.1905, 379.1910, 379.1915, 379.1920, 379.1925, 379.1930, 379.1935, 379.1940, 379.1945, 379.1950, 379.1955, 379.1960, 379.1965, and 379.1970, 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, 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. 1. 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, applicants, policyholders, insureds, beneficiaries, claimants, and certificate holders, who is a resident of this state and whose nonpublic information is in a licensee's possession, custody, or control;

(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;

(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 definition, a licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine:

(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 five 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 practicable:

(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 four 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 two hundred fifty 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 practicable except that the licensee shall not release to the state or any other entity nonpublic information of the consumer unless given written authority by the consumer or otherwise required by law. 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 section 375.1410.

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 section 375.1410.

(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 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, the director or any person or entity who receives documents, materials, or other information while acting under the authority of the director under sections 375.1400 to 375.1427 may share such documents, materials, or other information with another state or federal governmental agency or officer or the National Association of Insurance Commissioners; provided that the recipient agrees in writing to maintain the confidentiality of such documents,

materials, or other information, and has verified in writing the legal authority to maintain such confidentiality. Except as permitted in this subsection, neither the director nor any person or entity who receives documents, materials, or other information under sections 375.1400 to 375.1427 shall be permitted to:

(1) Share or otherwise release the documents, materials, or other information to a third party;

(2) Share or otherwise release the documents, materials, or other information for commercial use; or

(3) Sell cyber event or nonpublic information of any person or entity.

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, Pub. L. 104-191, and the Health Information Technology for Economic and Clinical Health Act (HITECH), Pub. 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, Pub. 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. Sections 375.1400 to 375.1427 shall take effect on January 1, 2026. 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.

379.1900. Sections 379.1900 to 379.1970 shall be known and may be cited as the "Peer-to-Peer Car-Sharing Program Act".

379.1905. Nothing in sections 379.1900 to 379.1970 shall be construed to extend beyond insurance or have any implications for sections other than sections 379.1900 to 379.1970 including, but not limited to, sections related to motor vehicle regulation, airport regulation, or taxation. The provisions of sections 379.1900 to 379.1970 shall not be construed to affect any other provision of law, and nothing in sections 379.1900 to 379.1970 shall be construed to distinguish or equate peer-to-peer car-sharing programs and rental car companies except as otherwise provided in sections 379.1900 to 379.1970.

379.1910. For purposes of sections 379.1900 to 379.1970, except where otherwise provided, the following terms mean:

(1) "Car-sharing delivery period", the period of time during which a shared vehicle is being delivered to the

location of the car-sharing start time, if applicable, as documented by the governing car-sharing program agreement;

(2) "Car-sharing period", the period of time that commences with the car-sharing delivery period or, if there is no car-sharing delivery period, that commences with the car-sharing start time and in either case ends at the car-sharing termination time;

(3) "Car-sharing program agreement", the terms and conditions applicable to a shared vehicle owner and a shared vehicle driver that govern the use of a shared vehicle through a peer-to-peer car-sharing program. The term "car-sharing program agreement" shall not include a master rental agreement or a rental agreement, as such terms are defined in section 407.730;

(4) "Car-sharing start time", the time when the shared vehicle becomes subject to the control of the shared vehicle driver at or after the time the reservation of a shared vehicle is scheduled to begin as documented in the records of a peer-to-peer car-sharing program;

(5) "Car-sharing termination time", the earliest of the following events:

(a) The expiration of the agreed-upon period of time established for the use of a shared vehicle according to the terms of the car-sharing program agreement if the shared vehicle is delivered to the location agreed upon in the car-sharing program agreement;

(b) When the shared vehicle is returned to a location as alternatively agreed upon by the shared vehicle owner and the shared vehicle driver as communicated through a peer-to-peer car-sharing program, which alternatively agreed-upon location shall be incorporated into the car-sharing program agreement; or

(c) When the shared vehicle owner or the shared vehicle owner's authorized designee takes possession and control of the shared vehicle;

(6) "Peer-to-peer car sharing", the authorized use of a vehicle by an individual other than the vehicle's owner through a peer-to-peer car-sharing program. The term "peer-to-peer car sharing" shall not include a rental car or rental activity, as described in section 407.732;

(7) "Peer-to-peer car-sharing program", a business platform that connects vehicle owners with drivers to enable the sharing of vehicles for financial consideration. The term "peer-to-peer car-sharing program" shall not include a car rental company, as defined in section 407.730;

(8) "Shared vehicle", a vehicle that is available for sharing through a peer-to-peer car-sharing program. The term "shared vehicle" shall not include a rental car, as described in section 407.732;

(9) "Shared vehicle driver", an individual who has been authorized to drive the shared vehicle by the shared vehicle owner under a car-sharing program agreement. The term "shared vehicle driver" shall not include an authorized driver, as defined in section 407.730;

(10) "Shared vehicle owner", the registered owner, or a person or entity designated by the registered owner, of a vehicle made available for sharing to shared vehicle drivers through a peer-to-peer car-sharing program. The term "shared vehicle owner" shall not include a car rental company, as defined in section 407.730.

379.1915. 1. Except as provided in subsection 2 of this section, a peer-to-peer car-sharing program shall assume liability of a shared vehicle owner for:

(1) Bodily injury or property damage to third parties;

(2) Uninsured and underinsured motorist losses; or

(3) To the extent personal injury protection coverage is required by law, personal injury protection losses;

during the car-sharing period in an amount stated in the peer-to-peer car-sharing program agreement, which amount shall not be less than the amount required under chapter 303.

2. Notwithstanding the definition of "car-sharing termination time" in section 379.1910, the assumption of liability under subsection 1 of this section shall not apply to any shared vehicle owner when:

(1) A shared vehicle owner makes an intentional or fraudulent material misrepresentation or omission to the peer-to-peer car-sharing program before the car-sharing period in which the loss occurred; or

(2) Acting in concert with a shared vehicle driver who fails to return the shared vehicle in accordance with the terms of the car-sharing program agreement.

3. Notwithstanding the definition of "car-sharing termination time" in section 379.1910, the assumption of liability under subsection 1 of this section shall apply to bodily injury losses, property damage losses, uninsured and underinsured motorist losses, or to the extent personal injury protection coverage is required by law, personal injury protection losses, by damaged third parties as required by chapter 303.

4. A peer-to-peer car-sharing program shall ensure that, during each car-sharing period, the shared vehicle owner and the shared vehicle driver are insured under a motor vehicle liability insurance policy that provides insurance coverage in amounts no less than the minimum amounts set forth in chapter 303, and that:

(1) Recognizes that the shared vehicle insured under the policy is made available and used through a peer-to-peer car-sharing program; or

(2) Does not exclude use of a shared vehicle by a shared vehicle driver.

5. The insurance described under subsection 4 of this section may be satisfied by motor vehicle liability insurance maintained by:

(1) A shared vehicle owner;

(2) A shared vehicle driver;

(3) A peer-to-peer car-sharing program; or

(4) A shared vehicle owner, a shared vehicle driver, and a peer-to-peer car-sharing program.

6. The insurance described in subsection 5 of this section that is satisfying the insurance requirement of subsection 4 of this section shall be primary during each car-sharing period. If a claim occurs in another state with minimum financial responsibility limits higher than the minimum financial responsibility requirements in chapter 303 during the car-sharing period, the coverage maintained under subsection 5 of this section shall satisfy the difference in minimum coverage amounts up to the applicable policy limits.

7. The insurer, insurers, or peer-to-peer car-sharing program providing coverage under subsection 4 or 5 of this section shall assume primary liability for a claim when:

(1) A dispute exists as to who was in control of the shared vehicle at the time of the loss and the peer-to-peer car-sharing program does not have available, did not retain, or fails to provide the information required by section 379.1930; or

(2) A dispute exists as to whether the shared vehicle was returned to the alternatively agreed-upon location as required under paragraph (b) of subdivision (5) of section 379.1910.

8. If insurance maintained by a shared vehicle owner or shared vehicle driver in accordance with subsection 5 of

this section has lapsed or does not provide the required coverage, insurance maintained by a peer-to-peer car-sharing program shall provide the coverage required by subsection 4 of this section, beginning with the first dollar of a claim, and have the duty to defend such claim except under circumstances as set forth in subsection 2 of this section.

9. Coverage under an automobile insurance policy maintained by the peer-to-peer car-sharing program shall not be dependent on another automobile insurer first denying a claim nor shall another automobile insurance policy be required to first deny a claim.

10. Nothing in this section:

(1) Limits the liability of the peer-to-peer car-sharing program for any act or omission of the peer-to-peer car-sharing program itself that results in injury to any person as a result of the use of a shared vehicle through a peer-to-peer car-sharing program; or

(2) Limits the ability of the peer-to-peer car-sharing program to, by contract, seek indemnification from the shared vehicle owner or the shared vehicle driver for economic loss sustained by the peer-to-peer car-sharing program resulting from a breach of the terms and conditions of the car-sharing program agreement.

379.1920. At the time when a vehicle owner registers as a shared vehicle owner on a peer-to-peer car-sharing program and prior to the time when the shared vehicle owner makes a shared vehicle available for car sharing on the peer-to-peer car-sharing program, the peer-to-peer car-sharing program shall notify the shared vehicle owner that, if the shared vehicle has a lien against it, the use of the shared vehicle through a peer-to-peer car-sharing program, including use without physical damage coverage, may violate the terms of the contract with the lienholder.

379.1925. 1. An authorized insurer that writes motor vehicle liability insurance in this state may exclude any and all coverage and the duty to defend or indemnify for any claim afforded under a shared vehicle owner's motor vehicle liability insurance policy including, but not limited to:

(1) Liability coverage for bodily injury and property damage;

(2) Personal injury protection coverage;

(3) Uninsured and underinsured motorist coverage;

(4) Medical payments coverage;

(5) Comprehensive physical damage coverage; and

(6) Collision physical damage coverage.

2. Nothing in sections 379.1900 to 379.1970 invalidates or limits an exclusion contained in a motor vehicle liability insurance policy, including any insurance policy in use or approved for use that excludes coverage for motor vehicles made available for rent, sharing, or hire or for any business use.

3. Nothing in sections 379.1900 to 379.1970 invalidates, limits, or restricts an insurer's ability under existing law to underwrite any insurance policy. Nothing in sections 379.1900 to 379.1970 invalidates, limits, or restricts an insurer's ability under existing law to cancel and nonrenew policies.

379.1930. A peer-to-peer car-sharing program shall collect and verify records pertaining to the use of a vehicle including, but not limited to, times used, car-sharing period pick-up and drop-off locations, fees paid by the shared vehicle driver, and revenues received by the shared vehicle owner. The peer-to-peer car-sharing program shall provide such information upon request to the shared vehicle owner, the shared vehicle owner's insurer, or the shared vehicle driver's insurer to facilitate a claim

coverage investigation, settlement, negotiation, or litigation. The peer-to-peer car-sharing program shall retain the records for a time period not less than the applicable personal injury statute of limitations.

379.1935. A peer-to-peer car-sharing program and a shared vehicle owner shall be exempt from vicarious liability, consistent with 49 U.S.C. Section 30106, under any state or local law that imposes liability solely based on vehicle ownership.

379.1940. A motor vehicle insurer that defends or indemnifies a claim against a shared vehicle that is excluded under the terms of its policy shall have the right to seek recovery against the motor vehicle insurer of the peer-to-peer car-sharing program if the claim is:

(1) Made against the shared vehicle owner or the shared vehicle driver for loss or injury that occurs during the car-sharing period; and

(2) Excluded under the terms of its policy.

379.1945. 1. Notwithstanding any other law, statute, rule, or regulation to the contrary, a peer-to-peer car-sharing program shall have an insurable interest in a shared vehicle during the car-sharing period.

2. Nothing in this section creates liability on a peer-to-peer car-sharing program to maintain the coverage mandated by section 379.1915.

3. A peer-to-peer car-sharing program may own and maintain as the named insured one or more policies of motor vehicle liability insurance that provides coverage for:

(1) Liabilities assumed by the peer-to-peer car-sharing program under a peer-to-peer car-sharing program agreement;

(2) Any liability of the shared vehicle owner;

(3) Damage or loss to the shared vehicle; or

(4) Any liability of the shared vehicle driver.

379.1950. Each car-sharing program agreement made in this state shall disclose to the shared vehicle owner and the shared vehicle driver:

(1) Any right of the peer-to-peer car-sharing program to seek indemnification from the shared vehicle owner or the shared vehicle driver for economic loss sustained by the peer-to-peer car-sharing program resulting from a breach of the terms and conditions of the car-sharing program agreement;

(2) That a motor vehicle liability insurance policy issued to the shared vehicle owner for the shared vehicle or to the shared vehicle driver does not provide a defense or indemnification for any claim asserted by the peer-to-peer car-sharing program;

(3) That the peer-to-peer car-sharing program's insurance coverage on the shared vehicle owner and the shared vehicle driver is in effect only during each car-sharing period and that, for any use of the shared vehicle by the shared vehicle driver after the car-sharing termination time, the shared vehicle driver and the shared vehicle owner may not have insurance coverage;

(4) The daily rate, fees, and if applicable, any insurance or protection package costs that are charged to the shared vehicle owner or the shared vehicle driver;

(5) That the shared vehicle owner's motor vehicle liability insurance may not provide coverage for a shared vehicle;

(6) An emergency telephone number to personnel capable of fielding roadside assistance and other customer service inquiries; and

(7) Whether there are conditions under which a shared vehicle driver is required to maintain a personal automobile

insurance policy with certain applicable coverage limits on a primary basis in order to book a shared motor vehicle.

379.1955. 1. A peer-to-peer car-sharing program shall not enter into a peer-to-peer car-sharing program agreement with a driver unless the driver who will operate the shared vehicle:

(1) Holds a driver's license issued by this state that authorizes the driver to operate vehicles of the class of the shared vehicle;

(2) Is a nonresident who:

(a) Has a driver's license issued by the state or country of the driver's residence that authorizes the driver in that state or country to drive vehicles of the class of the shared vehicle; and

(b) Is at least the same age as the age required of a resident to drive in this state; or

(3) Otherwise is specifically authorized by this state to drive vehicles of the class of the shared vehicle.

2. A peer-to-peer car-sharing program shall keep a record of:

(1) The name and address of the shared vehicle driver;

(2) The number of the driver's license of the shared vehicle driver and of each other person, if any, who will operate the shared vehicle; and

(3) The place of issuance of the driver's license.

379.1960. A peer-to-peer car-sharing program shall have sole responsibility for any equipment, such as a GPS system or other special equipment, that is put in or on the vehicle to monitor or facilitate the car-sharing transaction and shall agree to indemnify and hold harmless the shared vehicle owner for any damage to or theft of such equipment during the car-sharing period not caused by the shared vehicle owner. The peer-to-peer car-sharing program has the

right to seek indemnity from the shared vehicle driver for any loss or damage to such equipment that occurs during the car-sharing period.

379.1965. 1. At the time when a vehicle owner registers as a shared vehicle owner on a peer-to-peer car-sharing program and prior to the time when the shared vehicle owner makes a shared vehicle available for car sharing on the peer-to-peer car-sharing program, the peer-to-peer car-sharing program shall:

(1) Verify that the shared vehicle does not have any safety recalls on the vehicle for which the repairs have not been made; and

(2) Notify the shared vehicle owner of the requirements under subsection 2 of this section.

2. (1) If the shared vehicle owner has received an actual notice of a safety recall on the vehicle, the shared vehicle owner shall not make the vehicle available as a shared vehicle on a peer-to-peer car-sharing program until the safety recall repair has been made.

(2) If a shared vehicle owner receives an actual notice of a safety recall on a shared vehicle while the shared vehicle is made available on the peer-to-peer car-sharing program, the shared vehicle owner shall remove the shared vehicle as available on the peer-to-peer car-sharing program as soon as practicable after receiving the notice of the safety recall and until the safety recall repair has been made.

(3) If a shared vehicle owner receives an actual notice of a safety recall while the shared vehicle is being used in the possession of a shared vehicle driver, as soon as practicable after receiving the notice of the safety recall, the shared vehicle owner shall notify the peer-to-

peer car-sharing program about the safety recall so that the shared vehicle owner may address the safety recall repair.

379.1970. The department of commerce and insurance may promulgate all necessary rules and regulations for the administration of sections 379.1900 to 379.1970. 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 pursuant to 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 the effective date of this section shall be invalid and void.

Section B. The enactment of sections 379.1900, 379.1905, 379.1910, 379.1915, 379.1920, 379.1925, 379.1930, 379.1935, 379.1940, 379.1945, 379.1950, 379.1955, 379.1960, 379.1965, and 379.1970 of this act shall become effective on January 1, 2026.