Z-0521.1

SENATE BILL 5956

State of Washington 67th Legislature 2022 Regular Session

By Senators Stanford and Nguyen; by request of Insurance Commissioner

Read first time 01/27/22. Referred to Committee on Business, Financial Services & Trade.

AN ACT Relating to insurance data security; adding a new chapter to Title 48 RCW; prescribing penalties; and providing an effective date.

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

NEW SECTION. **Sec. 1.** This chapter may be known and cited as the insurance data security act.

NEW SECTION. **Sec. 2.** (1) The purpose and intent of this act is to establish standards for data security and standards for the investigation of and notification to the commissioner of a cybersecurity event applicable to licensees, as defined in section 3 of this act.

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

(3) Nothing in this act may be construed or interpreted as preempting, superseding, or otherwise limiting the attorney general's authority to enforce either chapter 19.255 or 19.86 RCW, or both.

NEW SECTION. **Sec. 3.** The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(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 its information systems.

(2) "Commissioner" means the insurance commissioner of this state.

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

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

(a) "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.

(b) "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.

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

(6) "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.

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

(8) "Licensee" means any person licensed, authorized, or registered, or required to be licensed, authorized, or registered under Title 48 RCW, but does 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.

(9) "Multifactor authentication" means authentication through verification of at least two of the following types of authentication factors:

(a) Knowledge factors, such as a password;

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

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

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

(i) Social security number;

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

(iii) Account number or credit or debit card number;

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

(v) Biometric records; or

(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:

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

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

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

(11) "Person" has the same meaning as in RCW 48.01.070.

(12)(a) "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from: Federal, state, or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state, or local law.

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

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

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

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

(14) "Third-party service provider" means 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.

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

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

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

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

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

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

(3) As part of its risk assessment, the licensee must:

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

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

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

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

(i) Employee training and management;

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

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

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

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

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

(b) Determine which of the following security measures are appropriate and implement the appropriate security measures accordingly:

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

(ii) Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy;

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

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

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

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

(vii) Utilize effective controls, which may include multifactor authentication procedures for any individual accessing nonpublic information;

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

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

(x) Implement measures to protect against destruction, loss, or damage of nonpublic information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures; and

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

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

(d) Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information

relative to the character of the sharing and the type of information shared; and

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

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

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

(ii) 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 this act; 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.

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

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

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

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

(b) The incident response plan must address the following areas:

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

(ii) The goals of the incident response plan;

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

(iv) External and internal communications and information sharing;

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

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

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

(9) Annually, each insurer domiciled in this state must submit to the commissioner, a written statement by April 15th of each year, certifying that the insurer is in compliance with the requirements set forth in this section. Each insurer must maintain for examination by the commissioner 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 must document the identification and the remedial efforts planned and underway to address the areas, systems, or processes. The documentation must be available for inspection by the commissioner.

NEW SECTION. **Sec. 5.** (1) If a licensee learns that a cybersecurity event has or may have occurred the licensee or either an outside vendor or service provider, or both, designated to act on behalf of the licensee, must conduct a prompt investigation.

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

(a) Determine whether a cybersecurity event has occurred;

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

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

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

(3) If the licensee learns that a cybersecurity event has or may have occurred in a system maintained by a third-party service provider, the licensee must 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 must maintain records concerning all cybersecurity events for a period of at least five years from the date of the cybersecurity event and must produce those records upon demand of the commissioner.

NEW SECTION. **Sec. 6.** (1) Each licensee must notify the commissioner as promptly as possible but in no event later than three business days from a determination that a cybersecurity event has occurred when either of the following criteria has been met:

(a)(i) This state is the licensee's state of domicile, in the case of an insurer, as that term is defined in RCW 48.17.010;

(ii) This state is the licensee's home state, in the case of an insurance producer, as that term is defined in RCW 48.17.010; or

(iii) When the licensee is not an insurer or an insurance producer, the licensee is a person who is either formed under the laws of this state, or whose residence or principal place of business is located in this state, or both; or

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

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

(ii) 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 operation or operations of the licensee.

(2)(a) As part of the notification to the commissioner required under subsection (1) of this section, the licensee must provide as much of the following information as possible:

(i) Date of the cybersecurity event;

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

(iii) How the cybersecurity event was discovered;

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

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

(vi) 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;

(vii) Description of the specific types of information accessed or 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;

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

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

(x) 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;

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

(xii) 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

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

(b) The licensee must provide the information in electronic form as directed by the commissioner. The licensee has a continuing

obligation to update and supplement initial and subsequent notifications to the commissioner concerning the cybersecurity event, as new information dictates.

(3) Licensees must comply with chapter 19.255 RCW, as applicable, and provide notice to the attorney general and a copy of the notice sent to consumers under that chapter to the commissioner, when a licensee is required to notify the commissioner under subsection (1) of this section.

(4)(a) In the case of a cybersecurity event in a system maintained by a third-party service provider, of which the licensee has become aware, the licensee must treat the event as it would under subsection (1) of this section.

(b) The computation of licensee's deadlines begins on the day after the third-party service provider notifies the licensee of the cybersecurity event or the licensee otherwise has actual knowledge of the cybersecurity event, whichever is sooner.

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

(5)(a)(i) In the case of a cybersecurity event involving nonpublic information that is used by the licensee 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 must notify its affected ceding insurers and the commissioner of its state of domicile within three business days of making the determination that a cybersecurity event has occurred.

(ii) The ceding insurers that have a direct contractual relationship with affected consumers must fulfill the consumer notification requirements imposed under chapter 19.255 RCW and any other notification requirements relating to a cybersecurity event imposed under this section.

(b)(i) In the case of a cybersecurity event involving nonpublic information that is in the possession, custody, or control of a third-party service provider of a licensee that is an assuming insurer, the assuming insurer must notify its affected ceding insurers and the commissioner of its state of domicile within three

business days of receiving notice from its third-party service provider that a cybersecurity event has occurred.

(ii) The ceding insurers that have a direct contractual relationship with affected consumers must fulfill the consumer notification requirements imposed under chapter 19.255 RCW and any other notification requirements relating to a cybersecurity event imposed under this section.

(6)(a) 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 and for which a consumer accessed the insurer's services through an independent insurance producer, the insurer must notify the producers of record of all affected consumers no later than the insurer gives notice to consumers as required under RCW 19.255.010.

(b) The insurer is excused from this obligation for those instances in which it does not have the current insurance producer of record information for any individual consumer.

NEW SECTION. **Sec. 7.** (1) The commissioner has power to examine and investigate into the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of this act. This power is in addition to the powers which the commissioner has under this title. Any investigation or examination must be conducted under this title.

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

NEW SECTION. **Sec. 8.** (1) Any documents, materials, or other information in the control or possession of the commissioner that are furnished by a licensee or an employee or agent acting on behalf of a licensee under sections 4(9) and 6(2)(a) (ii) through (v), (viii), (x), and (xi) of this act, or that are obtained by the commissioner in an investigation or examination under section 7 of this act are confidential, are not subject to chapter 42.56 RCW, are not subject to subpoena, and are not subject to discovery or admissible in evidence in any private civil action. However, the commissioner is authorized to use the documents, materials, or other information in

the furtherance of any regulatory or legal action brought as a part of the commissioner's regular duties.

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

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

(a) Share documents, materials, or other information, including the confidential and privileged documents, materials, or information subject to subsection (1) of this section, with the following recipients provided that the recipient agrees in writing to maintain the confidentiality and privileged status of the documents, materials, or other information: The attorney general; other state, federal, and international regulatory agencies; the national association of insurance commissioners and its affiliates or subsidiaries; and state, federal, and international law enforcement authorities. The attorney general is bound by separate confidentiality and trade secret authorities;

(b) Receive documents, materials, or information, including otherwise confidential and privileged documents, materials, or information, from the national association of insurance commissioners and its affiliates or subsidiaries, and from regulatory and law enforcement officials of other foreign or domestic jurisdictions. The commissioner shall maintain as confidential or privileged any documents, materials, or information received with notice or understanding that they are confidential or privileged under the laws of the jurisdiction that is the source of the documents, materials, or information;

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

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

(4) A waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information does not occur as a result of disclosure to the commissioner under this section or as a result of sharing as authorized in subsection (3) of this section.

(5) Nothing in this chapter prohibits the commissioner from releasing final, adjudicated actions that are open to public inspection under chapter 42.56 RCW to a database or other clearinghouse service maintained by the national association of insurance commissioners and its affiliates or subsidiaries.

(6) Any documents, materials, or other information in the control or possession of the national association of insurance commissioners or a third-party consultant or vendor under sections 4(9) and 6(2)(a)(ii) through (v), (viii), (x), and (xi) of this act, or that are obtained by the commissioner in an investigation or examination under section 7 of this act are confidential, are not subject to chapter 42.56 RCW, are not subject to subpoena, and are not subject to discovery or admissible in evidence in any private civil action.

(7)(a) If the licensee contacts a law enforcement agency after learning of a cybersecurity event that has or may have occurred and the law enforcement agency determines that the notification required under chapter 19.255 RCW will impede a criminal investigation, the licensee must still provide the notice to the commissioner as required by section 6 of this act.

(b) Until the law enforcement agency determines that the disclosure required under chapter 19.255 RCW will not compromise the investigation, any documents, materials, or other information in the control or possession of the commissioner that are furnished by a licensee, or an employee or agent acting on behalf of a licensee under section 6 of this act, are confidential, are not subject to chapter 42.56 RCW, are not subject to subpoena, and are not subject to discovery or admissible in evidence in any private civil action. However, the commissioner is permitted to share the documents, materials, and other information as provided in subsection (3) of this section.

(c) After the law enforcement agency has determined that the disclosure required under chapter 19.255 RCW will not compromise the investigation, the confidentiality provided under subsections (1) and (6) of this section apply.

NEW SECTION. **Sec. 9.** (1) The following exceptions apply to this chapter:

(a) A licensee with fewer than 10 employees, including any independent contractors, is exempt from section 4 of this act;

(b) A licensee subject to the federal health insurance portability and accountability act (P.L. 104-191, August 21, 1996, 110 Stat. 1936) that has established and maintains an information security program under the statutes, rules, regulations, procedures, or guidelines established under that act, will be considered to meet the requirements of section 4 of this act, provided that the licensee is compliant with, and submits a written statement certifying its compliance with, section 4 of this act;

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

(2) In the event that a licensee ceases to qualify for an exception, the licensee has 180 days to comply with this chapter.

NEW SECTION. **Sec. 10.** In the case of a violation of this chapter, a licensee may be penalized under any penalty provision of this code applicable to that licensee.

NEW SECTION. **Sec. 11.** The commissioner may adopt rules to implement and administer this chapter.

NEW SECTION. **Sec. 12.** If any provision of this act or its application to any person or circumstance is held invalid, the remainder of the act or the application of the provision to other persons or circumstances is not affected.

NEW SECTION. **Sec. 13.** (1) This act takes effect July 1, 2022.

(2) Except for section 4(6) of this act, licensees have one year from the effective date of this section to implement section 4 of this act. Licensees have two years from the effective date of this section to implement section 4(6) of this act.

NEW SECTION. **Sec. 14.** Sections 1 through 11 of this act constitute a new chapter in Title 48 RCW.

--- END ---