2024 -- S 2802 SUBSTITUTE A

========
LC004391/SUB A
========

S T A T E O F R H O D E I S L A N D

IN GENERAL ASSEMBLY

JANUARY SESSION, A.D. 2024

A N A C T

RELATING TO INSURANCE -- EXAMINATIONS

Introduced By: Senator V. Susan Sosnowski

Date Introduced: March 22, 2024

Referred To: Senate Commerce

(Dept. of Business Regulation)

It is enacted by the General Assembly as follows:

SECTION 1. Section 27-13.1-3 of the General Laws in Chapter 27-13.1 entitled "Examinations" is hereby amended to read as follows:

27-13.1-3. Authority, scope, and scheduling of examinations.

(a) The director or any of ~~his or her~~ the director's examiners may conduct an examination under this chapter of any company as often as the director in ~~his or her~~ the director's sole discretion deems appropriate, but shall, at a minimum, conduct an examination of every insurer licensed in this state not less frequently than once every five (5) years. In scheduling and determining the nature, scope, and frequency of the examinations, the director shall consider such matters as the results of financial statement analyses and ratios, changes in management or ownership, actuarial opinions, reports of independent certified public accountants, and other criteria as set forth in the Financial Condition Examiners' Handbook adopted by the National Association of Insurance Commissioners and in effect when the director exercises discretion under this section.

(b) For purposes of completing an examination of a company under this chapter, the director may examine or investigate any person, or the business of any person, in so far as the examination or investigation is, in the sole discretion of the director, necessary or material to the examination of the company.

(c) In lieu of an examination under this chapter of a foreign or alien insurer licensed in this state, the director may accept an examination report on the company as prepared by the insurance department for the company's state of domicile or port of entry state only if:

(1) The insurance department was at the time of the examination accredited under the National Association of Insurance Commissioners' financial regulation standards and accreditation program; or

(2) The examination is performed under the supervision of an accredited insurance department or with the participation of one or more examiners who are employed by an accredited state insurance department and who, after a review of the examination work papers and report, state under oath that the examination was performed in a manner consistent with the standards and procedures required by their insurance department.

SECTION 2. Chapter 27-1 of the General Laws entitled "Domestic Insurance Companies" is hereby amended by adding thereto the following sections:

27-1-46. Information security program.

(a) Commensurate with the size and complexity of an insurer, the nature and scope of an insurer's activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the insurer or in the insurer's possession, custody or control, each domestic insurance company shall develop, implement, and maintain a comprehensive written information security program, based on the insurer's risk assessment and that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the insurer's information system. For purposes of this chapter, "information security program" means the administrative, technical, and physical safeguards that an insurer uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle, nonpublic information. "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. "Nonpublic information" means information that is not publicly available information and is:

(1) 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;

(2) Any information concerning a consumer which 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:

(i) Social security number;

(ii) Driver's license number or non-driver identification card number;

(iii) Account number, 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.

(3) 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, behavioral health, or medical 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.

(b) Objectives of information security program. An insurer'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. For purposes of this section, "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 an insurer's possession, custody or control; and

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

(c) Risk assessment. The insurer shall:

(1) Designate one or more employees, an affiliate, or an outside vendor designated to act on behalf of the insurer 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. "Third-party service providers" 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. Third-party service providers does not include licensed insurance producers;

(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 insurer's operations, 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 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.

(d) Risk management. Based on its risk assessment, the insurer shall:

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

(2) Determine which security measures listed below are appropriate and implement such security measures:

(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. “Authorized individual” means an individual known to and screened by the insurer, and determined to be necessary and appropriate to have access to the nonpublic information held by the insurer, and the insurer’s information systems;

(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 access at physical locations containing nonpublic information only to authorized individuals;

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

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

(vii) Utilize effective controls, which may include multi-factor 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 insurer;

(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;

(3) Include cybersecurity risks in the insurer'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 insurer in the risk assessment.

(e) Oversight by board of directors. If the insurer has a board of directors, the board or an appropriate committee of the board shall, at a minimum:

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

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

(i) The overall status of the information security program and the insurer's compliance with this chapter; and

(ii) 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, or recommendations for changes in the information security program; and

(3) If executive management delegates any of its responsibilities pursuant to this section, it shall oversee the development, implementation and maintenance of the insurer's information

security program prepared by the designee(s) and shall receive a report from the designee(s) complying with the requirements of the report to the board of directors.

(f) Oversight of third-party service provider arrangements.

(1) An insurer shall exercise due diligence in selecting its third-party service provider; and

(2) An insurer shall take reasonable steps to request 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.

(g) Program adjustments. The insurer 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 insurer's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to information systems.

(h) Incident response plan:

(1) As part of its information security program, each insurer 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 insurer 's information systems, or the continuing functionality of any aspect of the insurer 's business or operations;

(2) Such incident response plan shall 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.

(3) If the insurer learns that a cybersecurity event has or may have occurred, the insurer, or an outside vendor and/or service provider designated to act on behalf of the insurer, shall conduct a prompt investigation. For purposes of this section, “cybersecurity event” means an event resulting in unauthorized access to, disruption or misuse of, an information system or nonpublic information

stored on such information system. This 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. This also does not include an event with regard to which the insurer has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed.

(i) During the investigation, the insurer, or an outside vendor and/or service provider designated to act on behalf of the insurer, shall, at a minimum, determine as much of the following information as possible:

(A) 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 insurer's possession, custody or control.

(ii) If the insurer learns that a cybersecurity event has or may have occurred in a system maintained by a third-party service provider, and it has or may have impacted the insurer's nonpublic information, the insurer shall make reasonable efforts to complete the steps set forth in subsection (a) of this section or make reasonable efforts to confirm and document that the third-party service provider has completed those steps.

(iii) The insurer shall maintain records concerning all cybersecurity events for a period of at least five (5) years from the date of the cybersecurity event. The insurer shall produce those records upon demand of the commissioner pursuant to chapter 13.1 of title 27 or other statutory authority.

(i) Annually, each insurer domiciled in this state shall submit to the commissioner a written statement by April 15 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 (5) 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. This documentation must be available for inspection by the commissioner pursuant to a request under chapter 13.1 of title 27 or other statutory authority.

(j) If an insurer domiciled in this state has an information security program that is prepared for and in compliance with Pub. L. 104-191, 110 Stat. 1936, enacted August 21, 1996 (Health

Insurance Portability and Accountability Act) and related privacy, security and breach notification regulations pursuant to Code of Federal Regulations, Parts 160 and 164, and Pub. L. 111-5, 123 Stat. 226, enacted February 17, 2009 (Health Information Technology), insurers can rely on that plan to certify their compliance with subsection (i) of this section.

27-1-47. Notification of a cybersecurity event.

(a) Each domestic insurer shall notify the commissioner as promptly as possible but in no event later than three (3) business days from a determination that a cybersecurity event has occurred when either of the following criteria has been met:

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

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

(i) Any consumer residing in this state; or

(ii) Any material part of the normal operation(s) of the insurer.

(b) The insurer shall provide any information required by this section in electronic form as directed by the commissioner. The insurer shall have a continuing obligation to update and supplement initial and subsequent notifications to the commissioner concerning the cybersecurity event. The insurer shall provide as much of the following information as possible. The insurer should indicate whether it is making claims under chapter 2 of title 38 to any of the information provided. The following information shall be provided:

(1) Date of the cybersecurity event;

(2) 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 lost, stolen, or breached information has been recovered and if so, how this recovery was achieved;

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

(6) Whether the insurer has filed a police report or has notified any regulatory, government or law enforcement agencies and, if so, when such notification was provided;

(7) Description of the specific types of information acquired without authorization. Specific types of information consisting of 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 insurer shall provide the best estimate in the initial report to the commissioner and update this estimate with each subsequent report to the commissioner pursuant to this section;

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

(12) A copy of the insurer privacy policy and a statement outlining the steps the insurer will take to investigate and notify consumers affected by the cybersecurity event; and

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

(c) An insurer shall comply with chapter 49.3 of title 11, as applicable, and provide a copy of the notice sent to consumers under that chapter to the commissioner, when an insurer is required to notify the commissioner.

(d) Notice regarding cybersecurity events of third-party service providers:

(1) In the case of a cybersecurity event involving an insurer's nonpublic information in a system maintained by a third-party service provider, of which the insurer has become aware, the insurer shall treat that event as it would under subsection (a) of this section;

(2) The computation of the insurer's deadlines shall begin on the day after the third-party service provider notifies the insurer of the cybersecurity event or the insurer otherwise has actual knowledge of the cybersecurity event, whichever is sooner;

(3) Nothing in this chapter shall prevent or abrogate an agreement between an insurer and another insurer, a third-party service provider or any other party to fulfill any of the investigation requirements or notice requirements imposed under this section.

(e) Notice regarding cybersecurity events of reinsurers to insurers:

(1)(i) In the case of a cybersecurity event involving nonpublic information that is used by the insurer that is acting as an assuming insurer or in the possession, custody or control of an insurer 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 of its state of domicile within seventy-two (72) hours of making the determination that a cybersecurity event has occurred;

(ii) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under chapter 49.3 of title 11,

("identity theft protection act of 2015"), and any other notification requirements relating to a cybersecurity event imposed under this section.

(2)(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 an insurer that is an assuming insurer, the assuming insurer shall notify its affected ceding insurers and the commissioner of its state of domicile within seventy-two (72) hours 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 shall fulfill the consumer notification requirements imposed under chapter 49.3 of title 11 and any other notification requirements relating to a cybersecurity event imposed under this section.

(f) Notice regarding cybersecurity events of insurers to producers of record.

(1) In the case of a cybersecurity event involving nonpublic information that is in the possession, custody or control of an insurer 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 shall notify the producers of record of all affected consumers as soon as practicable as directed by the commissioner.

(2) 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.

SECTION 3. Chapter 27-2 of the General Laws entitled "Foreign Insurance Companies" is hereby amended by adding thereto the following sections:

27-2-29. Information security program.

(a) Commensurate with the size and complexity of an insurer, the nature and scope of an insurers activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the insurer or in the insurer’s possession, custody or control, each foreign insurance company shall develop, implement, and maintain a comprehensive written information security program, based on the insurer's risk assessment and that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the insurer's information system. For purposes of this section, “information security program” means the administrative, technical, and physical safeguards that an insurer uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle nonpublic information. "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. “Nonpublic information” means information that

is not publicly available information and is:

(1) 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;

(2) Any information concerning a consumer which 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:

(i) Social security number;

(ii) Driver's license number or non-driver identification card number;

(iii) Account number, 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;

(3) 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, behavioral health, or medical 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,

(b) Objectives of information security program. An insurer'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. For the purposes of this section “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 an insurer’s possession, custody or control.; and

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

(c) Risk assessment. The insurer shall:

(1) Designate one or more employees, an affiliate, or an outside vendor designated to act

on behalf of the insurer 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. For purposes of this section, “third-party service providers” 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;

(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 insurer 's operations, 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 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.

(d) Risk management. Based on its risk assessment, the insurer shall:

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

(2) Determine which security measures listed below are appropriate and implement such security measures:

(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. Authorized individual means an individual known to and screened by the insurer and determined to be necessary and appropriate to have access to the nonpublic information held by the insurer and its information systems;

(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 access at physical locations containing nonpublic information only to authorized individuals;

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

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

(vii) Utilize effective controls, which may include multi-factor 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 insurer;

(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;

(3) Include cybersecurity risks in the insurer '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 insurer in the risk assessment.

(e) Oversight by board of directors. If the insurer has a board of directors, the board or an appropriate committee of the board shall, at a minimum:

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

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

(i) The overall status of the information security program and the insurer's compliance with this chapter; and

(ii) 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, or recommendations for changes in the information security program; and

(3) If executive management delegates any of its responsibilities pursuant to this section, it shall oversee the development, implementation and maintenance of the insurer's information security program prepared by the designee(s) and shall receive a report from the designee(s) complying with the requirements of the report to the board of directors.

(f) Oversight of third-party service provider arrangements.

(1) An insurer shall exercise due diligence in selecting its third-party service provider; and

(2) An insurer shall take reasonable steps to request 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.

(g) Program adjustments. The insurer 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 insurer's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to information systems.

(h) Incident response plan:

(1) As part of its information security program, each insurer 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 insurer's information systems, or the continuing functionality of any aspect of the insurer's business or operations;

(2) Such incident response plan shall 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.

(3) If the insurer learns that a cybersecurity event has or may have occurred, the insurer, or an outside vendor and/or service provider designated to act on behalf of the insurer, shall conduct a prompt investigation. For the purposes of this section, "cybersecurity event" means an event resulting in unauthorized access to, disruption or misuse of, an information system or nonpublic information stored on such information system. This 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. This also does not include an event with regard to which the insurer has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed.

(i) During the investigation, the insurer, or an outside vendor and/or service provider designated to act on behalf of the insurer, shall, at a minimum, determine as much of the following information as possible:

(A) 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 insurer's possession, custody or control.

(ii) If the insurer learns that a cybersecurity event has or may have occurred in a system maintained by a third-party service provider, and it has or may have impacted the insurer's nonpublic information, the insurer shall make reasonable efforts to complete the steps set forth in subsection (h)(3)(i) of this section or make reasonable efforts to confirm and document that the third-party service provider has completed those steps.

(iii) The insurer shall maintain records concerning all cybersecurity events for a period of at least five (5) years from the date of the cybersecurity event. The insurer and shall produce those records upon demand of the commissioner pursuant to chapter 13.1 of title 27 or other statutory authority.

27-2-30. Notification of a cybersecurity event.

(a) Each insurer shall notify the commissioner as promptly as possible but in no event later than three (3) business days from a determination that a cybersecurity event has occurred when the insurer reasonably believes that the nonpublic information involved affects two hundred fifty (250) or more consumers residing in this state and that either of the following apply:

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

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

(i) Any consumer residing in this state; or

(ii) Any material part of the normal operation(s) of the insurer.

(b) The insurer shall provide any information required by this section in electronic form as directed by the commissioner. The insurer shall have a continuing obligation to update and supplement initial and subsequent notifications to the commissioner concerning the cybersecurity event. The insurer should indicate whether it is making claims under chapter 2 of title 38 to any of the information provided. The following information shall be provided:

(1) Date of the cybersecurity event;

(2) 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 lost, stolen, or breached information has been recovered and if so, how this recovery was achieved;

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

(6) Whether the insurer has filed a police report or has notified any regulatory, government or law enforcement agencies and, if so, when such notification was provided;

(7) Description of the specific types of information acquired without authorization. Specific types of information consisting of 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 insurer shall provide the best estimate in the initial report to the commissioner and update this estimate with each subsequent report to the commissioner pursuant to this section;

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

(12) A copy of the insurer privacy policy and a statement outlining the steps the insurer will take to investigate and notify consumers affected by the cybersecurity event; and

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

(c) An insurer shall comply with chapter 49.3 of title 11, as applicable, and provide a copy of the notice sent to consumers under that chapter to the commissioner, when an insurer is required to notify the commissioner.

(d) Notice regarding cybersecurity events of third-party service providers:

(1) In the case of a cybersecurity event involving an insurer 's nonpublic information in a system maintained by a third-party service provider, of which the insurer has become aware, the insurer shall treat that event as it would under subsection (a) of this section;

(2) The computation of the insurer's deadlines shall begin on the day after the third-party service provider notifies the insurer of the cybersecurity event or the insurer otherwise has actual knowledge of the cybersecurity event, whichever is sooner;

(3) Nothing in this chapter shall prevent or abrogate an agreement between an insurer and another insurer, a third-party service provider or any other party to fulfill any of the investigation requirements imposed under § 27-1.3-5 or notice requirements imposed under this section.

(e) Notice regarding cybersecurity events of reinsurers to insurers:

(1)(i) In the case of a cybersecurity event involving nonpublic information that is used by the insurer that is acting as an assuming insurer or in the possession, custody or control of an insurer 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 of its state of domicile within seventy-two (72) hours of making the determination that a cybersecurity event has occurred;

(ii) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under chapter 49.3 of title 11, ("identity theft protection act of 2015"), and any other notification requirements relating to a cybersecurity event imposed under this section;

(2)(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 an insurer that is an assuming

insurer, the assuming insurer shall notify its affected ceding insurers and the commissioner of its state of domicile within seventy-two (72) hours 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 shall fulfill the consumer notification requirements imposed under chapter 49.3 of title 11 and any other notification requirements relating to a cybersecurity event imposed under this section.

(f) Notice regarding cybersecurity events of insurers to producers of record.

(1) In the case of a cybersecurity event involving nonpublic information that is in the possession, custody or control of 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 shall notify the producers of record of all affected consumers as soon as practicable as directed by the commissioner.

(2) 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.

SECTION 4. This act shall take effect on January 1, 2025.

========
LC004391/SUB A
========

EXPLANATION

BY THE LEGISLATIVE COUNCIL

OF

A N A C T

RELATING TO INSURANCE -- EXAMINATIONS

***

This act would amend the statutory provisions regarding domestic and foreign insurers and insurer examinations to provide provisions with regard to cybersecurity events involving Rhode Island consumers.

This act would take effect on January 1, 2025.

========
LC004391/SUB A
========