

2024 -- S 2802 SUBSTITUTE A

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

STATE OF RHODE ISLAND

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:

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

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

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

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

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

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

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

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

11 **27-1-46. Information security program.**

12 (a) Commensurate with the size and complexity of an insurer, the nature and scope of an
13 insurer's activities, including its use of third-party service providers, and the sensitivity of the
14 nonpublic information used by the insurer or in the insurer's possession, custody or control, each
15 domestic insurance company shall develop, implement, and maintain a comprehensive written
16 information security program, based on the insurer's risk assessment and that contains
17 administrative, technical, and physical safeguards for the protection of nonpublic information and
18 the insurer's information system. For purposes of this chapter, "information security program"
19 means the administrative, technical, and physical safeguards that an insurer uses to access, collect,
20 distribute, process, protect, store, use, transmit, dispose of, or otherwise handle, nonpublic
21 information. "Publicly available information" means any information that a licensee has a
22 reasonable basis to believe is lawfully made available to the general public from: federal, state or
23 local government records; widely distributed media; or disclosures to the general public that are
24 required to be made by federal, state or local law. "Nonpublic information" means information that
25 is not publicly available information and is:

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

29 (2) Any information concerning a consumer which because of name, number, personal
30 mark, or other identifier can be used to identify such consumer, in combination with any one or
31 more of the following data elements:

32 (i) Social security number;

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

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

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

3 (v) Biometric records.

4 (3) Any information or data, except age or gender, in any form or medium created by or
5 derived from a health care provider or a consumer and that relates to:

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

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

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

10 (b) Objectives of information security program. An insurer's information security program
11 shall be designed to:

12 (1) Protect the security and confidentiality of nonpublic information and the security of the
13 information system;

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

16 (3) Protect against unauthorized access to or use of nonpublic information, and minimize
17 the likelihood of harm to any consumer. For purposes of this section, "consumer" means an
18 individual, including, but not limited to, applicants, policyholders, insureds, beneficiaries,
19 claimants, and certificate holders, who is a resident of this state and whose nonpublic information
20 is in an insurer's possession, custody or control; and

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

23 (c) Risk assessment. The insurer shall:

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

26 (2) Identify reasonably foreseeable internal or external threats that could result in
27 unauthorized access, transmission, disclosure, misuse, alteration or destruction of nonpublic
28 information, including the security of information systems and nonpublic information that are
29 accessible to, or held by, third-party service providers. "Third-party service providers" means a
30 person, not otherwise defined as a licensee, that contracts with a licensee to maintain, process, store,
31 or otherwise is permitted access to nonpublic information through its provision of services to the
32 licensee. Third-party service providers does not include licensed insurance producers;

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

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

4 (i) Employee training and management;

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

7 (iii) Detecting, preventing, and responding to attacks, intrusions, or other systems failures;
8 and

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

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

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

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

19 (i) Place access controls on information systems, including controls to authenticate and
20 permit access only to authorized individuals to protect against the unauthorized acquisition of
21 nonpublic information. "Authorized individual" means an individual known to and screened by the
22 insurer, and determined to be necessary and appropriate to have access to the nonpublic information
23 held by the insurer, and the insurer's information systems;

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

27 (iii) Restrict access at physical locations containing nonpublic information only to
28 authorized individuals;

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

32 (v) Adopt secure development practices for in-house developed applications utilized by the
33 insurer and procedures for evaluating, assessing or testing the security of externally developed
34 applications utilized by the insurer.

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

3 (vii) Utilize effective controls, which may include multi-factor authentication procedures
4 for any individual accessing nonpublic information;

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

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

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

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

15 (3) Include cybersecurity risks in the insurer's enterprise risk management process;

16 (4) Stay informed regarding emerging threats or vulnerabilities and utilize reasonable
17 security measures when sharing information relative to the character of the sharing and the type of
18 information shared; and

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

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

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

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

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

29 (ii) Material matters related to the information security program, addressing issues such as
30 risk assessment, risk management and control decisions, third-party service provider arrangements,
31 results of testing, cybersecurity events or violations and management's responses thereto, or
32 recommendations for changes in the information security program; and

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

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

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

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

5 (2) An insurer shall take reasonable steps to request a third-party service provider to
6 implement appropriate administrative, technical, and physical measures to protect and secure the
7 information systems and nonpublic information that are accessible to, or held by, the third-party
8 service provider.

9 (g) Program adjustments. The insurer shall monitor, evaluate and adjust, as appropriate,
10 the information security program consistent with any relevant changes in technology, the sensitivity
11 of its nonpublic information, internal or external threats to information, and the insurer's own
12 changing business arrangements, such as mergers and acquisitions, alliances and joint ventures,
13 outsourcing arrangements and changes to information systems.

14 (h) Incident response plan:

15 (1) As part of its information security program, each insurer shall establish a written
16 incident response plan designed to promptly respond to, and recover from, any cybersecurity event
17 that compromises the confidentiality, integrity or availability of nonpublic information in its
18 possession, the insurer 's information systems, or the continuing functionality of any aspect of the
19 insurer 's business or operations;

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

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

22 (ii) The goals of the incident response plan;

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

24 (iv) External and internal communications and information sharing;

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

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

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

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

1 stored on such information system. This does not include the unauthorized acquisition of encrypted
2 nonpublic information if the encryption, process or key is not also acquired, released, or used
3 without authorization. This also does not include an event with regard to which the insurer has
4 determined that the nonpublic information accessed by an unauthorized person has not been used
5 or released and has been returned or destroyed.

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

9 (A) Whether a cybersecurity event has occurred;

10 (B) Assess the nature and scope of the cybersecurity event;

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

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

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

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

25 (i) Annually, each insurer domiciled in this state shall submit to the commissioner a written
26 statement by April 15 certifying that the insurer is in compliance with the requirements set forth in
27 this section. Each insurer shall maintain for examination by the department all records, schedules
28 and data supporting this certificate for a period of five (5) years. To the extent an insurer has
29 identified areas, systems or processes that require material improvement, updating or redesign, the
30 insurer shall document the identification and the remedial efforts planned and underway to address
31 such areas, systems or processes. This documentation must be available for inspection by the
32 commissioner pursuant to a request under chapter 13.1 of title 27 or other statutory authority.

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

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

5 **27-1-47. Notification of a cybersecurity event.**

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

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

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

13 (i) Any consumer residing in this state; or

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

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

21 (1) Date of the cybersecurity event;

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

24 (3) How the cybersecurity event was discovered;

25 (4) Whether any lost, stolen, or breached information has been recovered and if so, how
26 this recovery was achieved;

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

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

30 (7) Description of the specific types of information acquired without authorization.
31 Specific types of information consisting of particular data elements including, for example, types
32 of medical information, types of financial information or types of information allowing
33 identification of the consumer;

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

1 event;

2 (9) The number of total consumers in this state affected by the cybersecurity event. The
3 insurer shall provide the best estimate in the initial report to the commissioner and update this
4 estimate with each subsequent report to the commissioner pursuant to this section;

5 (10) The results of any internal review identifying a lapse in either automated controls or
6 internal procedures, or confirming that all automated controls or internal procedures were followed;

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

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

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

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

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

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

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

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

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

27 (1)(i) In the case of a cybersecurity event involving nonpublic information that is used by
28 the insurer that is acting as an assuming insurer or in the possession, custody or control of an insurer
29 that is acting as an assuming insurer and that does not have a direct contractual relationship with
30 the affected consumers, the assuming insurer shall notify its affected ceding insurers and the
31 commissioner of its state of domicile within seventy-two (72) hours of making the determination
32 that a cybersecurity event has occurred;

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

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

3 (2)(i) In the case of a cybersecurity event involving nonpublic information that is in the
4 possession, custody or control of a third-party service provider of an insurer that is an assuming
5 insurer, the assuming insurer shall notify its affected ceding insurers and the commissioner of its
6 state of domicile within seventy-two (72) hours of receiving notice from its third-party service
7 provider that a cybersecurity event has occurred;

8 (ii) The ceding insurers that have a direct contractual relationship with affected consumers
9 shall fulfill the consumer notification requirements imposed under chapter 49.3 of title 11 and any
10 other notification requirements relating to a cybersecurity event imposed under this section.

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

12 (1) In the case of a cybersecurity event involving nonpublic information that is in the
13 possession, custody or control of an insurer that is an insurer or its third-party service provider and
14 for which a consumer accessed the insurer's services through an independent insurance producer,
15 the insurer shall notify the producers of record of all affected consumers as soon as practicable as
16 directed by the commissioner.

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

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

21 **27-2-29. Information security program.**

22 (a) Commensurate with the size and complexity of an insurer, the nature and scope of an
23 insurers activities, including its use of third-party service providers, and the sensitivity of the
24 nonpublic information used by the insurer or in the insurer's possession, custody or control, each
25 foreign insurance company shall develop, implement, and maintain a comprehensive written
26 information security program, based on the insurer's risk assessment and that contains
27 administrative, technical, and physical safeguards for the protection of nonpublic information and
28 the insurer's information system. For purposes of this section, "information security program"
29 means the administrative, technical, and physical safeguards that an insurer uses to access, collect,
30 distribute, process, protect, store, use, transmit, dispose of, or otherwise handle nonpublic
31 information. "Publicly available information" means any information that a licensee has a
32 reasonable basis to believe is lawfully made available to the general public from: federal, state or
33 local government records; widely distributed media; or disclosures to the general public that are
34 required to be made by federal, state or local law. "Nonpublic information" means information that

1 is not publicly available information and is:

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

5 (2) Any information concerning a consumer which because of name, number, personal
6 mark, or other identifier can be used to identify such consumer, in combination with any one or
7 more of the following data elements:

8 (i) Social security number;
9 (ii) Driver's license number or non-driver identification card number;
10 (iii) Account number, credit or debit card number;
11 (iv) Any security code, access code or password that would permit access to a consumer's
12 financial account; or

13 (v) Biometric records;

14 (3) Any information or data, except age or gender, in any form or medium created by or
15 derived from a health care provider or a consumer and that relates to:

16 (i) The past, present or future physical, mental, behavioral health, or medical condition of
17 any consumer or a member of the consumer's family;
18 (ii) The provision of health care to any consumer; or
19 (iii) Payment for the provision of health care to any consumer,

20 (b) Objectives of information security program. An insurer's information security program
21 shall be designed to:

22 (1) Protect the security and confidentiality of nonpublic information and the security of the
23 information system.

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

26 (3) Protect against unauthorized access to or use of nonpublic information, and minimize
27 the likelihood of harm to any consumer. For the purposes of this section "consumer" means an
28 individual, including, but not limited to, applicants, policyholders, insureds, beneficiaries,
29 claimants, and certificate holders who is a resident of this state and whose nonpublic information
30 is in an insurer's possession, custody or control.; and

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

33 (c) Risk assessment. The insurer shall:

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

1 on behalf of the insurer who is responsible for the information security program;

2 (2) Identify reasonably foreseeable internal or external threats that could result in
3 unauthorized access, transmission, disclosure, misuse, alteration or destruction of nonpublic
4 information, including the security of information systems and nonpublic information that are
5 accessible to, or held by, third-party service providers. For purposes of this section, “third-party
6 service providers” means a person, not otherwise defined as a licensee, that contracts with a licensee
7 to maintain, process, store or otherwise is permitted access to nonpublic information through its
8 provision of services to the licensee;

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

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

14 (i) Employee training and management;

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

17 (iii) Detecting, preventing, and responding to attacks, intrusions, or other systems failures;
18 and

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

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

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

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

29 (i) Place access controls on information systems, including controls to authenticate and
30 permit access only to authorized individuals to protect against the unauthorized acquisition of
31 nonpublic information. Authorized individual means an individual known to and screened by the
32 insurer and determined to be necessary and appropriate to have access to the nonpublic information
33 held by the insurer and its information systems;

34 (ii) Identify and manage the data, personnel, devices, systems, and facilities that enable the

1 organization to achieve business purposes in accordance with their relative importance to business
2 objectives and the organization's risk strategy;

3 (iii) Restrict access at physical locations containing nonpublic information only to
4 authorized individuals;

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

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

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

13 (vii) Utilize effective controls, which may include multi-factor authentication procedures
14 for any individual accessing nonpublic information;

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

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

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

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

25 (3) Include cybersecurity risks in the insurer 's enterprise risk management process;
26 (4) Stay informed regarding emerging threats or vulnerabilities and utilize reasonable
27 security measures when sharing information relative to the character of the sharing and the type of
28 information shared; and

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

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

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

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

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

5 (ii) Material matters related to the information security program, addressing issues such as
6 risk assessment, risk management and control decisions, third-party service provider arrangements,
7 results of testing, cybersecurity events or violations and management's responses thereto, or
8 recommendations for changes in the information security program; and

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

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

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

15 (2) An insurer shall take reasonable steps to request a third-party service provider to
16 implement appropriate administrative, technical, and physical measures to protect and secure the
17 information systems and nonpublic information that are accessible to, or held by, the third-party
18 service provider.

19 (g) Program adjustments. The insurer shall monitor, evaluate and adjust, as appropriate,
20 the information security program consistent with any relevant changes in technology, the sensitivity
21 of its nonpublic information, internal or external threats to information, and the insurer's own
22 changing business arrangements, such as mergers and acquisitions, alliances and joint ventures,
23 outsourcing arrangements and changes to information systems.

24 (h) Incident response plan:

25 (1) As part of its information security program, each insurer shall establish a written
26 incident response plan designed to promptly respond to, and recover from, any cybersecurity event
27 that compromises the confidentiality, integrity or availability of nonpublic information in its
28 possession, the insurer's information systems, or the continuing functionality of any aspect of the
29 insurer's business or operations;

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

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

32 (ii) The goals of the incident response plan;

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

34 (iv) External and internal communications and information sharing;

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

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

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

7 (3) If the insurer learns that a cybersecurity event has or may have occurred, the insurer, or
8 an outside vendor and/or service provider designated to act on behalf of the insurer, shall conduct
9 a prompt investigation. For the purposes of this section, “cybersecurity event” means an event
10 resulting in unauthorized access to, disruption or misuse of, an information system or nonpublic
11 information stored on such information system. This does not include the unauthorized acquisition
12 of encrypted nonpublic information if the encryption, process, or key is not also acquired, released,
13 or used without authorization. This also does not include an event with regard to which the insurer
14 has determined that the nonpublic information accessed by an unauthorized person has not been
15 used or released and has been returned or destroyed.

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

19 (A) Whether a cybersecurity event has occurred;

20 (B) Assess the nature and scope of the cybersecurity event;

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

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

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

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

1 **27-2-30. Notification of a cybersecurity event.**

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

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

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

10 (i) Any consumer residing in this state; or

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

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

17 (1) Date of the cybersecurity event;

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

20 (3) How the cybersecurity event was discovered;

21 (4) Whether any lost, stolen, or breached information has been recovered and if so, how
22 this recovery was achieved;

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

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

26 (7) Description of the specific types of information acquired without authorization.
27 Specific types of information consisting of particular data elements including, for example, types
28 of medical information, types of financial information or types of information allowing
29 identification of the consumer;

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

32 (9) The number of total consumers in this state affected by the cybersecurity event. The
33 insurer shall provide the best estimate in the initial report to the commissioner and update this
34 estimate with each subsequent report to the commissioner pursuant to this section;

1 (10) The results of any internal review identifying a lapse in either automated controls or
2 internal procedures, or confirming that all automated controls or internal procedures were followed;

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

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

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

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

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

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

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

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

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

23 (1)(i) In the case of a cybersecurity event involving nonpublic information that is used by
24 the insurer that is acting as an assuming insurer or in the possession, custody or control of an insurer
25 that is acting as an assuming insurer and that does not have a direct contractual relationship with
26 the affected consumers, the assuming insurer shall notify its affected ceding insurers and the
27 commissioner of its state of domicile within seventy-two (72) hours of making the determination
28 that a cybersecurity event has occurred;

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

33 (2)(i) In the case of a cybersecurity event involving nonpublic information that is in the
34 possession, custody or control of a third-party service provider of an insurer that is an assuming

1 insurer, the assuming insurer shall notify its affected ceding insurers and the commissioner of its
2 state of domicile within seventy-two (72) hours of receiving notice from its third-party service
3 provider that a cybersecurity event has occurred;

4 (ii) The ceding insurers that have a direct contractual relationship with affected consumers
5 shall fulfill the consumer notification requirements imposed under chapter 49.3 of title 11 and any
6 other notification requirements relating to a cybersecurity event imposed under this section.

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

8 (1) In the case of a cybersecurity event involving nonpublic information that is in the
9 possession, custody or control of an insurer or its third-party service provider and for which a
10 consumer accessed the insurer's services through an independent insurance producer, the insurer
11 shall notify the producers of record of all affected consumers as soon as practicable as directed by
12 the commissioner.

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

15 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

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

4 This act would take effect on January 1, 2025.

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