

1 STATE OF OKLAHOMA

2 1st Session of the 59th Legislature (2023)

3 COMMITTEE SUBSTITUTE

4 FOR ENGROSSED

5 SENATE BILL NO. 543

By: Montgomery of the Senate

and

Sneed of the House

6
7
8
9
10 COMMITTEE SUBSTITUTE

11 An Act relating to insurance data security; creating
12 the Insurance Data Security Act; providing short
13 title; establishing act jurisdiction; construing
14 provision; defining terms; requiring licensees to
15 develop data security program with certain
16 inclusions; establishing intent of security programs
17 created pursuant to act; directing licensee to
18 conduct risk assessment; directing licensee to take
19 certain action following risk assessment result;
20 requiring certain supervising boards to take certain
21 actions to implement program; requiring licensee to
22 contract with third-party service provider subject to
23 certain conditions; requiring licensee to maintain
24 updates and revisions to program; requiring licensee
develop incident response plan; requiring certain
reports be submitted to the Insurance Commissioner;
requiring insurer to maintain certain records for
specific time period; requiring investigation after
certain cybersecurity event; establishing
investigation process; requiring notification of
certain event to the Commissioner; requiring
compliance with certain state laws; providing for
certain exemption; providing for the Commissioner to
investigate certain licensees for certain violations;
providing for confidentiality of certain information
relating to cybersecurity event; allowing
Commissioner to share certain data with national

1 association; construing provision; providing for rule
2 promulgation; providing certain exceptions to act;
3 establishing penalties; amending 51 O.S. 2021,
4 Section 24A.3, as last amended by Section 1, Chapter
5 402, O.S.L. 2022 (51 O.S. Supp. 2022, Section 24A.3),
6 which relates to the Oklahoma Open Records Act;
7 modifying definition; updating statutory language;
8 providing for codification; and providing an
9 effective date.

10 BE IT ENACTED BY THE PEOPLE OF THE STATE OF OKLAHOMA:

11 SECTION 1. NEW LAW A new section of law to be codified
12 in the Oklahoma Statutes as Section 670 of Title 36, unless there is
13 created a duplication in numbering, reads as follows:

14 This act shall be known and may be cited as the "Insurance Data
15 Security Act".

16 SECTION 2. NEW LAW A new section of law to be codified
17 in the Oklahoma Statutes as Section 671 of Title 36, unless there is
18 created a duplication in numbering, reads as follows:

19 A. Notwithstanding any other provision of law, the provisions
20 of this act shall be the exclusive state law for licensees subject
21 to the jurisdiction of the Insurance Commissioner for data security,
22 the investigation of a cybersecurity event, and notification to the
23 Commissioner.

24 B. This act shall not be construed to create or imply a private
cause of action for violations of its provisions.

1 SECTION 3. NEW LAW A new section of law to be codified
2 in the Oklahoma Statutes as Section 672 of Title 36, unless there is
3 created a duplication in numbering, reads as follows:

4 As used in this act:

5 1. "Authorized individual" means an individual known to and
6 screened by the licensee and determined to be necessary and
7 appropriate to have access to the nonpublic information held by the
8 licensee and its information systems;

9 2. "Commissioner" means the Insurance Commissioner;

10 3. "Consumer" means an individual, including but not limited to
11 applicants, policyholders, insureds, beneficiaries, claimants, and
12 certificate holders, who is a resident of this state and whose
13 nonpublic information is in the possession, custody, or control of a
14 licensee;

15 4. "Cybersecurity event" means an event resulting in
16 unauthorized access to or disruption or misuse of an information
17 system or nonpublic information stored on the information system.
18 The term cybersecurity event shall not include the unauthorized
19 acquisition of encrypted nonpublic information if the encryption,
20 process, or key is not also acquired, released, or used without
21 authorization. Cybersecurity event shall not include an event in
22 which the licensee has determined that the nonpublic information
23 accessed by an unauthorized person has not been used or released and
24 has been returned or destroyed;

1 5. "Department" means the Insurance Department;

2 6. "Encrypted" means the transformation of data into a form
3 which results in a low probability of assigning meaning without the
4 use of a protective process or key;

5 7. "Information security program" means the administrative,
6 technical, and physical safeguards that a licensee uses to access,
7 collect, distribute, process, protect, store, use, transmit, dispose
8 of, or otherwise handle nonpublic information;

9 8. "Information system" means a discrete set of electronic
10 information resources organized for the collection, processing,
11 maintenance, use, sharing, dissemination or disposition of nonpublic
12 information, as well as any specialized system such as industrial or
13 process controls systems, telephone switching and private branch
14 exchange systems, and environmental control systems;

15 9. "Licensee" means any person licensed, authorized to operate,
16 or registered, or required to be licensed, authorized to operate, or
17 registered, pursuant to Title 36 of the Oklahoma Statutes; provided,
18 however, that it shall not include a purchasing group or a risk
19 retention group chartered and licensed in a state other than this
20 state or a person that is acting as an assuming insurer that is
21 domiciled in another state or jurisdiction;

22 10. "Multi-factor authentication" means authentication through
23 verification of at least two (2) of the following types of
24 authentication factors:

- 1 a. knowledge factors, such as a password,
- 2 b. possession factors, such as a token or text message on
- 3 a mobile phone, or
- 4 c. inherence factors, such as a biometric characteristic;

5 11. "Nonpublic information" means electronic information that
6 is not publicly available and is:

- 7 a. business related information of a licensee, of which
- 8 the tampering with or unauthorized disclosure, access,
- 9 or use of would cause a material adverse impact to the
- 10 business, operations, or security of the licensee,
- 11 b. any information concerning a consumer that, because of
- 12 name, number, personal mark, or other identifier, can
- 13 be used to identify him or her, in combination with
- 14 any one or more of the following data elements:
 - 15 (1) social security number,
 - 16 (2) driver license number or nondriver identification
 - 17 card number,
 - 18 (3) financial account number, credit card number, or
 - 19 debit card number,
 - 20 (4) any security code, access code, or password that
 - 21 would permit access to a consumer's financial
 - 22 account, or
 - 23 (5) biometric records, or

1 c. any information or data, except age or gender, in any
2 form or medium created by or derived from a health
3 care provider or a consumer that can be used to
4 identify a particular consumer and that relates to:
5 (1) the past, present, or future physical, mental, or
6 behavioral health or condition of any consumer or
7 a member of the family of the consumer,
8 (2) the provision of health care to any consumer, or
9 (3) payment for the provision of health care to any
10 consumer;

11 12. "Person" means any individual or any nongovernmental
12 entity including but not limited to any nongovernmental
13 partnership, corporation, branch, agency, or association;

14 13. "Publicly available information" means any information that
15 a licensee has reasonable basis to believe is lawfully made
16 available to the general public from federal, state, or local
17 government records, widely distributed media, or disclosures to the
18 general public that are required to be made by federal, state, or
19 local law. For the purposes of this definition, a licensee has a
20 reasonable basis to believe that information is lawfully made
21 available to the general public if the licensee has taken steps to
22 determine:

23 a. that the information is of the type that is available
24 to the general public, and

1 b. whether a consumer can direct that the information not
2 be made available to the general public and, if so,
3 that such consumer has not done so; and

4 14. "Third-party service provider" means a person, not
5 otherwise defined as a licensee, that contracts with a licensee to
6 maintain, process, store, or otherwise is permitted access to
7 nonpublic information through its provision of services to the
8 licensee.

9 SECTION 4. NEW LAW A new section of law to be codified
10 in the Oklahoma Statutes as Section 673 of Title 36, unless there is
11 created a duplication in numbering, reads as follows:

12 A. Each licensee in this state shall develop, implement, and
13 maintain a comprehensive written information security program based
14 on the risk assessment of the licensee provided for in this act and
15 that contains administrative, technical, and physical safeguards for
16 the protection of nonpublic information and the information systems
17 of the licensee. The program shall be commensurate with the size and
18 complexity of the licensee, the nature and scope of the activities
19 of the licensee, including its use of third-party service providers,
20 and the sensitivity of the nonpublic information used by the
21 licensee or in the possession, custody, or control of the licensee.

22 B. An information security program of a licensee shall be
23 designed to:

1 1. Protect the security and confidentiality of nonpublic
2 information and the security of the information systems;

3 2. Protect against any threats or hazards to the security or
4 integrity of nonpublic information and the information systems;

5 3. Protect against unauthorized access to or use of nonpublic
6 information, and minimize the likelihood of harm to any consumer;
7 and

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

11 C. The licensee shall:

12 1. Designate one or more employees, an affiliate, or an outside
13 vendor designated to act on behalf of the licensee who is
14 responsible for the information security program;

15 2. Identify reasonably foreseeable internal or external threats
16 that could result in unauthorized access, transmission, disclosure,
17 misuse, alteration, or destruction of nonpublic information
18 including, but not limited to, the security of information systems
19 and nonpublic information that are accessible to, or held by, third-
20 party service providers;

21 3. Assess the likelihood and potential damage of these threats,
22 taking into consideration the sensitivity of the nonpublic
23 information;

24

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

- 5 a. employee training and management,
- 6 b. information systems, including, but not limited to,
7 network and software design, as well as information
8 classification, governance, processing, storage,
9 transmission, and disposal, and
- 10 c. detecting, preventing, and responding to attacks,
11 intrusions, or other systems failures; and

12 5. Implement information safeguards to manage the threats
13 identified in its ongoing assessment, and no less than annually,
14 assess the effectiveness of the key controls, systems, and
15 procedures of the safeguards.

16 D. Based on the results of the risk assessment, the licensee
17 shall:

18 1. Design its information security program to mitigate the
19 identified risks, commensurate with the size and complexity of the
20 licensee, the nature and scope of the activities of the licensee
21 including its use of third-party service providers, and the
22 sensitivity of the nonpublic information used by the licensee or in
23 the possession, custody, or control of the licensee;

1 2. Determine and implement security measures deemed
2 appropriate, including:

- 3 a. place access controls on information systems
4 including controls to authenticate and permit access
5 only to authorized individuals to protect against the
6 unauthorized acquisition of nonpublic information,
- 7 b. identify and manage the data, personnel, devices,
8 systems, and facilities that enable the organization
9 to achieve business purposes in accordance with their
10 relative importance to business objectives and the
11 risk strategy of the organization,
- 12 c. restrict physical access to nonpublic information to
13 authorized individuals only,
- 14 d. protect by encryption or other appropriate means, all
15 nonpublic information while being transmitted over an
16 external network and all nonpublic information stored
17 on a laptop computer or other portable computing or
18 storage device or media,
- 19 e. adopt secure development practices for in-house
20 developed applications utilized by the licensee,
- 21 f. modify the information system in accordance with the
22 information security program of the licensee,

23
24

- 1 g. utilize effective controls, which may include multi-
- 2 factor authentication procedures for any authorized
- 3 individual accessing nonpublic information,
- 4 h. regularly test and monitor systems and procedures to
- 5 detect actual and attempted attacks on, or intrusions
- 6 into, information systems,
- 7 i. include audit trails within the information security
- 8 program designed to detect and respond to
- 9 cybersecurity events and designed to reconstruct
- 10 material financial transactions sufficient to support
- 11 normal operations and obligations of the licensee,
- 12 j. implement measures to protect against destruction,
- 13 loss, or damage of nonpublic information due to
- 14 environmental hazards such as fire and water damage or
- 15 other catastrophic events or technological failures,
- 16 and
- 17 k. develop, implement, and maintain procedures for the
- 18 secure disposal of nonpublic information in any format;

19 3. Include cybersecurity risks in the enterprise risk management
20 process of the licensee;

21 4. Stay informed regarding emerging threats or vulnerabilities
22 and utilize reasonable security measures when sharing information
23 relative to the character of the sharing and the type of information
24 shared; and

1 5. Provide its personnel with cybersecurity awareness training
2 that is updated as necessary to reflect risks identified by the
3 licensee in the risk assessment.

4 E. If the licensee has a board of directors, the board or an
5 appropriate committee of the board, at a minimum, within one year of
6 the effective date of this act, shall:

7 1. Require the executive management of the licensee or its
8 delegates to develop, implement, and maintain the information
9 security program of the licensee;

10 2. Require the executive management of the licensee or its
11 delegates to report to the Insurance Commissioner in writing, at
12 least annually, the following information:

13 a. the overall status of the information security program
14 and the compliance of the licensee with this act, and

15 b. material matters related to the information security
16 program, addressing issues such as risk assessment,
17 risk management and control decisions, third-party
18 service provider arrangements, results of testing,
19 cybersecurity events or violations and responses of
20 the management to those events or violations, and
21 recommendations for changes in the information
22 security program; and

23 3. If executive management delegates any of its
24 responsibilities, it shall oversee the development, implementation,

1 and maintenance of the information security program of the licensee
2 prepared by the delegate or delegates and shall receive a report
3 from the delegate or delegates complying with the requirements of
4 the report to the board.

5 F. A licensee shall exercise due diligence in selecting its
6 third-party service provider and shall require the provider to
7 implement appropriate administrative, technical, and physical
8 measures to protect and secure the information systems and nonpublic
9 information that are accessible to, or held by, the third-party
10 service provider.

11 G. The licensee shall monitor, evaluate, and adjust, as
12 appropriate, the information security program consistent with any
13 relevant changes in technology, the sensitivity of its nonpublic
14 information, internal or external threats to information and the
15 changing business arrangements of the licensee, such as mergers and
16 acquisitions, alliances and joint ventures, outsourcing
17 arrangements, and changes to information systems.

18 H. As part of its information security program, each licensee
19 shall establish a written incident response plan designed to
20 promptly respond to, and recover from, any cybersecurity event that
21 compromises the confidentiality, integrity, or availability of
22 nonpublic information in its possession, the information systems of
23 the licensee, or the continuing functionality of any aspect of the
24 business or operations of the licensee.

1 The incident response plan shall address the following areas:

- 2 1. The internal process for responding to a cybersecurity
3 event;
- 4 2. The goals of the incident response plan;
- 5 3. The definition of clear roles, responsibilities, and levels
6 of decision-making authority;
- 7 4. External and internal communications and information
8 sharing;
- 9 5. Identification of requirements for the remediation of any
10 identified weaknesses in information systems and associated
11 controls;
- 12 6. Documentation and reporting regarding cybersecurity events
13 and related incident response activities; and
- 14 7. The evaluation and revision as necessary of the incident
15 response plan following a cybersecurity event.

16 I. Annually, each insurer domiciled in this state shall submit
17 to the Commissioner a written statement by April 15, certifying that
18 the insurer complies with the requirements set forth in this section.
19 Each insurer shall maintain, for examination by the Insurance
20 Department, all records, schedules, and data supporting this
21 certificate for a period of five (5) years. To the extent an
22 insurer has identified areas, systems, or processes that require
23 material improvement, updating, or redesign, the insurer shall
24 document the identification and the remedial efforts planned and

1 underway to address such areas, systems, or processes. The
2 documentation shall be available for inspection by the Commissioner
3 upon request.

4 SECTION 5. NEW LAW A new section of law to be codified
5 in the Oklahoma Statutes as Section 674 of Title 36, unless there is
6 created a duplication in numbering, reads as follows:

7 A. If the licensee learns that a cybersecurity event has or
8 may have occurred, the licensee, or an outside vendor or service
9 provider designated to act on behalf of the licensee, shall conduct
10 a prompt investigation.

11 B. During the investigation, the licensee, or an outside vendor
12 or service provider designated to act on behalf of the licensee,
13 shall, at a minimum:

14 1. Determine whether a cybersecurity event has occurred;

15 2. Assess the nature and scope of the cybersecurity event;

16 3. Identify any nonpublic information that may have been
17 involved in the cybersecurity event; and

18 4. Perform or oversee reasonable measures to restore the
19 security of the information systems compromised in the cybersecurity
20 event in order to prevent further unauthorized acquisition, release,
21 or use of nonpublic information in the possession, custody, or
22 control of the licensee.

23 C. If the licensee learns that a cybersecurity event has or may
24 have occurred in a system maintained by a third-party service

1 provider, the licensee shall complete the steps listed in subsection
2 B of this section or confirm and document that the third-party
3 service provider has completed those steps.

4 D. The licensee shall maintain records concerning all
5 cybersecurity events for a period of at least five (5) years from
6 the date of the cybersecurity event and shall produce those records
7 upon request by the Insurance Commissioner.

8 SECTION 6. NEW LAW A new section of law to be codified
9 in the Oklahoma Statutes as Section 675 of Title 36, unless there is
10 created a duplication in numbering, reads as follows:

11 A. Every licensee shall notify the Insurance Commissioner
12 without unreasonable delay, but not later than three business days,
13 from a determination that a cybersecurity event involving nonpublic
14 information that is in the possession of a licensee has occurred
15 when either of the following criteria has been met:

16 1. This state is the state of domicile of the licensee, in the
17 case of an insurer, or this state is the home state of the licensee,
18 in the case of a producer, as those terms are defined in the
19 Oklahoma Producer Licensing Act, Sections 1435.1 through 1435.41 of
20 Title 36 of the Oklahoma Statutes, and the cybersecurity event has a
21 reasonable likelihood of materially harming any material part of the
22 normal operations of the licensee or any consumer residing in this
23 state; or
24

1 2. The licensee reasonably believes that the nonpublic
2 information involved is of two hundred fifty (250) or more consumers
3 residing in this state and is either of the following:

4 a. a cybersecurity event impacting the licensee of which
5 notice is required to be provided to any government
6 body, self-regulatory agency, or any other supervisory
7 body pursuant to any state or federal law, or

8 b. a cybersecurity event that has a reasonable likelihood
9 of materially harming:

10 (1) any consumer residing in this state, or

11 (2) any material part of the normal operation or
12 operations of the licensee.

13 B. The licensee making the notification required in subsection
14 A of this section shall provide as much of the following information
15 as possible, electronically in the manner and form prescribed by the
16 Commissioner, along with any applicable fees. The licensee shall
17 have a continuing obligation to update and supplement initial and
18 subsequent notifications to the Commissioner regarding material
19 changes to previously provided information relating to the
20 cybersecurity event. The licensee shall provide:

21 1. Date of the cybersecurity event;

22 2. Description of how the information was exposed, lost,
23 stolen, or breached including, but not limited to, the specific
24 roles and responsibilities of third-party service providers, if any;

- 1 3. How the cybersecurity event was discovered;
- 2 4. Whether any lost, stolen, or breached information has been
3 recovered and, if so, how this was done;
- 4 5. The identity of the source of the cybersecurity event;
- 5 6. Whether the licensee has filed a police report or has
6 notified any regulatory, government, or law enforcement agencies
7 and, if so, when such notification was provided;
- 8 7. Description of the specific types of information acquired
9 without authorization. The term "specific types of information"
10 means particular data elements including, but not limited to, types
11 of medical information, financial information, or information
12 allowing identification of the consumer;
- 13 8. The period during which the information system was
14 compromised by the cybersecurity event;
- 15 9. The number of total consumers in this state affected by the
16 cybersecurity event. The licensee shall provide the best estimate
17 in the initial report to the Commissioner and update this estimate
18 with each subsequent report to the Commissioner pursuant to this
19 section;
- 20 10. The results of any internal review identifying a lapse in
21 either automated controls or internal procedures, or confirming that
22 all automated controls or internal procedures were followed;
- 23 11. Description of efforts being undertaken to remediate the
24 situation which permitted the cybersecurity event to occur;

1 12. A copy of the privacy policy of the licensee and a
2 statement outlining the steps the licensee will take to investigate
3 and notify consumers affected by the cybersecurity event; and

4 13. Name of a contact person who is both familiar with the
5 cybersecurity event and authorized to act for the licensee.

6 C. A licensee shall comply with the procedures of the Security
7 Breach Notification Act, Section 161 et seq. of Title 24 of the
8 Oklahoma Statutes, to notify affected consumers and provide a copy
9 of the notice sent to consumers under that statute to the
10 Commissioner, when a licensee is required to notify the Commissioner
11 under subsection A of this section.

12 D. 1. In the case of a cybersecurity event in a system
13 maintained by a third-party service provider, of which the licensee
14 has become aware, the licensee shall treat the event as it would
15 under subsection A of this section unless the third-party service
16 provider provides the notice required under subsection A of this
17 section to the Commissioner and the licensee.

18 2. The computation of deadlines of the licensee shall begin on
19 the day after the third-party service provider notifies the licensee
20 of the cybersecurity event or the licensee otherwise has actual
21 knowledge of the cybersecurity event, whichever is sooner.

22 3. Nothing in this act shall prevent or abrogate an agreement
23 between a licensee and another licensee, a third-party service
24

1 provider, or any other party to fulfill any of the investigation
2 requirements impose or notice requirements imposed under this act.

3 E. 1. In the case of a cybersecurity event involving nonpublic
4 information that is used by the licensee that is acting as an
5 assuming insurer, or in the possession, custody, or control of a
6 licensee, that is acting as an assuming insurer and that does not
7 have a direct contractual relationship with the affected consumers,
8 the assuming insurer shall notify its affected ceding insurers and
9 the Commissioner of its state of domicile within three (3) business
10 days of making the determination that a cybersecurity event has
11 occurred. The ceding insurers that have a direct contractual
12 relationship with affected consumers shall fulfill the consumer
13 notification requirements imposed under the Security Breach
14 Notification Act, Section 161 et seq. of Title 24 of the Oklahoma
15 Statutes, and any other notification requirements relating to a
16 cybersecurity event imposed under this section.

17 2. In the case of a cybersecurity event involving nonpublic
18 information that is in the possession, custody, or control of a
19 third-party service provider of a licensee that is an assuming
20 insurer, the assuming insurer shall notify its affected ceding
21 insurers and the Commissioner of its state of domicile within three
22 (3) business days of receiving notice from its third-party service
23 provider that a cybersecurity event has occurred. The ceding
24 insurers that have a direct contractual relationship with affected

1 consumers shall fulfill the consumer notification requirements
2 imposed under Security Breach Notification Act, Section 161 et seq.
3 of Title 24 of the Oklahoma Statutes, and any other notification
4 requirements relating to a cybersecurity event imposed under this
5 section.

6 F. In the case of a cybersecurity event involving nonpublic
7 information that is in the possession, custody, or control of a
8 licensee that is an insurer or its third-party service provider for
9 which a consumer accessed the services of the insurer through an
10 independent insurance producer, and for which consumer notice is
11 required by this act or the Security Breach Notification Act,
12 Section 161 et seq. of Title 24 of the Oklahoma Statutes, the
13 insurer shall notify the producers of record of all affected
14 consumers of the cybersecurity event no later than the time at which
15 notice is provided to the affected consumers. The insurer is
16 excused from this obligation for any producers who are not
17 authorized by law or contract to sell, solicit, or negotiate on
18 behalf of the insurer, and in those instances in which the insurer
19 does not have the current producer of record information for an
20 individual consumer. Any licensee acting as an assuming insurer
21 shall have no other notice obligations relating to a cybersecurity
22 event or other data breach under this section or any other law of
23 this state.

24

1 SECTION 7. NEW LAW A new section of law to be codified
2 in the Oklahoma Statutes as Section 676 of Title 36, unless there is
3 created a duplication in numbering, reads as follows:

4 A. The Insurance Commissioner shall have power to examine and
5 investigate the affairs of any licensee to determine whether the
6 licensee has been or is engaged in any conduct in violation of the
7 provisions of this act or any rules promulgated thereto. This power
8 is in addition to the powers which the Commissioner has under
9 applicable provisions of the Insurance Code including, but not
10 limited to, Sections 309.1 through 309.6, 332, and 1250.4 of Title
11 36 of the Oklahoma Statutes.

12 B. Whenever the Commissioner has reason to believe that a
13 licensee has been or is engaged in conduct in this state that
14 violates any provision of this act, the Commissioner may take action
15 that is necessary or appropriate to enforce the provisions.

16 SECTION 8. NEW LAW A new section of law to be codified
17 in the Oklahoma Statutes as Section 677 of Title 36, unless there is
18 created a duplication in numbering, reads as follows:

19 A. Any documents, materials, or other information in the
20 control or possession of the Insurance Department that are furnished
21 by a licensee or an employee or agent thereof acting on behalf of a
22 licensee pursuant to the provisions of Section 4 and Section 6 of
23 this act or that are obtained by the Insurance Commissioner in an
24 investigation or examination pursuant to Section 7 of this act shall

1 be confidential by law and privileged, shall not be subject to the
2 Oklahoma Open Records Act, shall not be subject to subpoena, and
3 shall not be subject to discovery or admissible in evidence in any
4 private civil action. However, the Commissioner is authorized to
5 use the documents, materials, or other information in the
6 furtherance of any regulatory or legal action brought as a part of
7 the Commissioner's duties. The Commissioner shall not otherwise
8 make the documents, materials, or other information public without
9 the prior written consent of the licensee.

10 B. Neither the Commissioner nor any person who received
11 documents, materials, or other information while acting under the
12 authority of the Commissioner shall be permitted or required to
13 testify in any private civil action concerning any confidential
14 documents, materials, or information subject to subsection A of this
15 section.

16 C. In order to assist in the performance of the duties of the
17 Commissioner under this act, the Commissioner:

18 1. May share documents, materials, or other information
19 including the confidential and privileged documents, materials, or
20 information subject to subsection A of this section, with other
21 state, federal, and international regulatory agencies, with the
22 National Association of Insurance Commissioners and its affiliates
23 or subsidiaries and with state, federal, and international law
24 enforcement authorities; provided, that the recipient agrees in

1 writing to maintain the confidentiality and privileged status of the
2 document, material, or other information;

3 2. May receive documents, materials, or information including
4 otherwise confidential and privileged documents, materials, or
5 information, from the National Association of Insurance
6 Commissioners, its affiliates or subsidiaries, and from regulatory
7 and law enforcement officials of other foreign or domestic
8 jurisdictions, and shall maintain as confidential or privileged any
9 document, material, or information received with notice or the
10 understanding that it is confidential or privileged under the laws
11 of the jurisdiction that is the source of the document, material, or
12 information;

13 3. May share documents, materials, or other information subject
14 to subsection A of this section, with a third-party consultant or
15 vendor; provided, the consultant agrees in writing to maintain the
16 confidentiality and privileged status of the document, material, or
17 other information; and

18 4. May enter into agreements governing sharing and use of
19 information consistent with this subsection.

20 D. No waiver of any applicable privilege or claim of
21 confidentiality in the documents, materials, or information shall
22 occur as a result of disclosure to the Insurance Commissioner under
23 this section or as a result of sharing as authorized in subsection C
24 of this section.

1 E. Nothing in this act shall prohibit the Commissioner from
2 releasing final, adjudicated actions that are open to public
3 inspection pursuant to the Oklahoma Open Records Act, to a database
4 or other clearinghouse service maintained by the National
5 Association of Insurance Commissioners, its affiliates, or
6 subsidiaries.

7 F. Documents, materials, or other information in the possession
8 or control of the National Association of Insurance Commissioners or
9 a third-party consultant or vendor pursuant to this act shall not be
10 construed to be public information, shall not be subject to the
11 Oklahoma Open Records Act, shall not be subject to subpoena, and
12 shall not be subject to discovery or admissible as evidence in any
13 private civil action.

14 SECTION 9. NEW LAW A new section of law to be codified
15 in the Oklahoma Statutes as Section 678 of Title 36, unless there is
16 created a duplication in numbering, reads as follows:

17 A. The Insurance Commissioner may promulgate any rules
18 necessary to carry out the provisions of this section.

19 B. 1. The following exceptions shall apply to this act:

20 a. a licensee with less than Five Million Dollars
21 (\$5,000,000.00) in gross annual revenue, is exempt
22 from this act,

23 b. a licensee subject to the Health Insurance Portability
24 and Accountability Act, Pub. L. 104-191, 110 Stat.

1 1936, as amended, that has established and maintains
2 an information security program pursuant to such
3 statutes, rules, regulations, procedures, or
4 guidelines established thereunder, will be considered
5 to meet the requirements of Section 4 of this act,
6 provided that the licensee is compliant with and
7 submits a written statement to the Commissioner
8 certifying its compliance with the same, and

9 c. an employee, agent, representative, or designee of a
10 licensee, who is also a licensee, is exempt from this
11 act and shall not be required to develop their own
12 information security program to the extent that the
13 employee, agent, representative, or designee is
14 covered by the information security program of the
15 licensee.

16 2. If a licensee ceases to qualify for an exception, the
17 licensee shall have one hundred eighty (180) days to comply with the
18 provisions of this act.

19 C. In the case of a violation of this act, a licensee may be
20 penalized in accordance with any applicable sections of the
21 Insurance Code, including, but not limited to, Section 908 of Title
22 36 of the Oklahoma Statutes, or any other provision providing for
23 penalties that the licensee is subject to under the license or
24 permit of the licensee. Nothing in this act shall be construed to

1 impose any civil liability for any violation of this act or omission
2 to act by the licensee or employees of the licensee.

3 D. The provisions of this act shall take precedence over any
4 other state laws applicable to licensees for data security and the
5 investigation of a cybersecurity event.

6 SECTION 10. NEW LAW A new section of law to be codified
7 in the Oklahoma Statutes as Section 679 of Title 36, unless there is
8 created a duplication in numbering, reads as follows:

9 Licensees shall have one (1) year from the effective date of
10 this act to implement Section 4 of this act and two (2) years from
11 the effective date of this act to implement subsection F of Section
12 4 of this act.

13 SECTION 11. This act shall become effective November 1, 2023.

14

15 59-1-8119 MJ 04/04/23

16

17

18

19

20

21

22

23

24