

1 STATE OF OKLAHOMA

2 2nd Session of the 57th Legislature (2020)

3 COMMITTEE SUBSTITUTE
4 FOR

5 SENATE BILL 1919

6 By: Stanislawski of the Senate

7 and

8 Sims of the House

9 COMMITTEE SUBSTITUTE

10 An Act relating to insurance; creating the Insurance
11 Data Security Act; defining terms; requiring licensed
12 insurers to develop and maintain a comprehensive
13 information security program based on certain
14 factors; providing objectives of security program;
15 requiring licensee to conduct certain assessment of
16 risk factors and ensure sufficiency of safeguarding
17 data policies and procedures; requiring use of data
18 from assessment to determine design of information
19 security program and necessary security measures;
20 requiring licensee to be updated on cybersecurity
21 threats and provide employees with certain training
22 on threats; requiring board of directors or executive
23 management of licensee to develop and maintain
24 information security program and provide certain
report to management; requiring licensee to select
third-party service provider to protect information
system and certain information; requiring licensee to
monitor and adjust information security program;
requiring licensee to create an incident response to
cybersecurity threat plan; establishing requirements
for plan; requiring certain insurers to submit
certification of compliance with certain
requirements; requiring Insurance Department to
maintain certifications and certain documents for
inspection; requiring certain persons to conduct
investigation after cybersecurity threat;
establishing terms of investigation; requiring
remedial actions be taken after investigation;

1 requiring records on investigation be kept for
2 certain time period; requiring licensees to notify
3 Insurance Commissioner after cybersecurity threat in
4 certain circumstances in certain form; establishing
5 requirements of notification; requiring licensee to
6 comply with Security Breach Notification Act;
7 requiring licensee to notify certain persons after
8 notifying Commissioner; requiring application of
9 certain requirements after cybersecurity event to
10 information system maintained by third-party
11 provider; construing provision; requiring assuming
12 insurers to provide notice of cybersecurity event to
13 ceding insurers in certain timeframe; requiring
14 ceding insurers to notify certain persons; requiring
15 licensee to notify certain persons who accessed
16 licensee's services in certain manner about
17 cybersecurity event; providing exception; authorizing
18 Commissioner to examine and investigate licensees;
19 authorizing Commissioner to enforce provisions of
20 act; declaring certain documents and materials kept
21 pursuant to this act as confidential and not subject
22 to certain legal actions; authorizing Commissioner to
23 use documents and materials in certain legal actions;
24 prohibiting certain persons from being compelled to
testify concerning the documents and materials;
authorizing the Commissioner to receive and share
certain documents with certain persons; authorizing
Commissioner to enter into certain agreements;
construing clause; classifying certain documents as
confidential; providing exceptions to applicability
of act; authorizing certain penalty for violation of
act; authorizing Commissioner to promulgate rules;
providing for codification; and providing an
effective date.

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

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

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

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

6 As used in this act:

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

11 2. "Commissioner" means the Insurance Commissioner of this
12 state;

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

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

21 The term cybersecurity event shall not include the unauthorized
22 acquisition of encrypted nonpublic information if the encryption,
23 process or key is not also acquired, released or used without
24 authorization. Cybersecurity event does not include an event in

1 which the licensee has determined that the nonpublic information
2 accessed by an unauthorized person has not been used or released and
3 has been returned or destroyed;

4 5. "Department" means the Insurance Department;

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

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

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

19 9. "Licensee" means any person licensed, authorized to operate
20 or registered, or required to be licensed, authorized or registered
21 pursuant to Title 36 of the Oklahoma Statutes, provided, however,
22 that it shall not include a purchasing group or a risk retention
23 group chartered and licensed in a state other than this state or a
24

1 person that is acting as an assuming insurer that is domiciled in
2 another state or jurisdiction;

3 10. "Multi-factor authentication" means authentication through
4 verification of at least two (2) of the following types of
5 authentication factors:

- 6 a. knowledge factors, such as a password,
- 7 b. possession factors, such as a token or text message on
8 a mobile phone, or
- 9 c. inherence factors, such as a biometric characteristic;

10 11. "Non-public information" means electronic information that
11 is not publicly available and is:

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

1 (4) any security code, access code or password that
2 would permit access to a consumer's financial
3 account, or

4 (5) biometric records, and

5 c. any information or data, except age or gender, in any
6 form or medium created by or derived from a health
7 care provider or a consumer that can be used to
8 identify a particular consumer and that relates to:

9 (1) the past, present or future physical, mental or
10 behavioral health or condition of any consumer
11 or a member of the family of the consumer,

12 (2) the provision of health care to any consumer, or

13 (3) payment for the provision of health care to any
14 consumer;

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

18 13. "Publicly available information" means any information that
19 a licensee has reasonable basis to believe is lawfully made
20 available to the general public from federal, state or local
21 government records, widely distributed media or disclosures to the
22 general public that are required to be made by federal, state or
23 local law.

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

- 4 a. that the information is of the type that is available
5 to the general public, and
- 6 b. whether a consumer can direct that the information not
7 be made available to the general public and, if so,
8 that such consumer has not done so; and

9 14. "Third-party service provider" means a person, not
10 otherwise defined as a licensee, that contracts with a licensee to
11 maintain, process, store or otherwise is permitted access to
12 nonpublic information through its provision of services to the
13 licensee.

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

17 A. Each licensee in this state shall develop, implement and
18 maintain a comprehensive written information security program based
19 on the risk assessment of the licensee provided for in this act and
20 that contains administrative, technical and physical safeguards for
21 the protection of nonpublic information and the information system of
22 the licensee. The program shall be commensurate with the size and
23 complexity of the licensee, the nature and scope of the activities
24 of the licensee including its use of third-party service providers

1 and the sensitivity of the nonpublic information used by the
2 licensee or in the possession, custody or control of the licensee,

3 B. An information security program of a licensee shall be
4 designed to:

5 1. Protect the security and confidentiality of nonpublic
6 information and the security of the information system;

7 2. Protect against any threats or hazards to the security or
8 integrity of nonpublic information and the information system;

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

11 and

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

15 C. The licensee shall:

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

19 2. Identify reasonably foreseeable internal or external threats
20 that could result in unauthorized access, transmission, disclosure,
21 misuse, alteration or destruction of nonpublic information including
22 the security of information systems and nonpublic information that
23 are accessible to, or held by, third-party service providers;

24

1 3. Assess the likelihood and potential damage of these threats,
2 taking into consideration the sensitivity of the nonpublic
3 information;

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

- 8 a. employee training and management,
- 9 b. information systems, including network and software
10 design, as well as information classification,
11 governance, processing, storage, transmission and
12 disposal, and
- 13 c. detecting, preventing and responding to attacks,
14 intrusions or other systems failures; and

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

19 D. Based on the results of the risk assessment, the licensee
20 shall:

21 1. Design its information security program to mitigate the
22 identified risks, commensurate with the size and complexity of the
23 licensee, the nature and scope of the activities of the licensee
24 including its use of third-party service providers, and the

1 sensitivity of the nonpublic information used by the licensee or in
2 the possession, custody or control of the licensee;

3 2. Determine which security measures listed below are
4 appropriate and implement such security measures:

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

- 1 g. utilize effective controls, which may include multi-
- 2 factor authentication procedures for accessing
- 3 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 shall, at a minimum:

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

9 2. Require the executive management of the licensee or its
10 delegates to report in writing, annually, the following information:

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

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

21 3. If executive management delegates any of its
22 responsibilities, it shall oversee the development, implementation
23 and maintenance of the information security program of the licensee
24 prepared by the delegate or delegates and shall receive a report

1 from the delegate or delegates complying with the requirements of
2 the report to the board.

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

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

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

23 The incident response plan shall address the following areas:

24 1. The internal process for responding to a cybersecurity event;

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

12 I. Annually, each insurer domiciled in this state shall submit
13 to the Insurance Commissioner a written statement by February 15,
14 certifying that the insurer complies with the requirements set forth
15 in Section 663 of Title 36 of the Oklahoma Statutes. Each insurer
16 shall maintain, for examination by the Insurance Department, all
17 records, schedules and data supporting this certificate for a period
18 of five (5) years. To the extent an insurer has identified areas,
19 systems or processes that require material improvement, updating or
20 redesign, the insurer shall document the identification and the
21 remedial efforts planned and underway to address such areas, systems
22 or processes. The documentation shall be available for inspection by
23 the Commissioner upon request.

24

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

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

8 B. During the investigation, the licensee, or an outside
9 vendor or service provider designated to act on behalf of the
10 licensee, shall, at a minimum determine as much of the following
11 information as possible:

- 12 1. Whether a cybersecurity event has occurred;
- 13 2. The nature and scope of the cybersecurity event;
- 14 3. Any nonpublic information that may have been involved in the
15 cybersecurity event; and
- 16 4. Reasonable measures to restore the security of the
17 information systems compromised in the cybersecurity event in order
18 to prevent further unauthorized acquisition, release or use of
19 nonpublic information in the possession, custody or control of the
20 licensee.

21 C. The licensee shall maintain records concerning all
22 cybersecurity events for a period of at least five (5) years from
23 the date of the cybersecurity event and shall produce those records
24 upon request by the Insurance Commissioner.

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

4 A. Every licensee shall notify the Insurance Commissioner
5 without unreasonable delay, but not later than three (3) business
6 days, from a determination that a cybersecurity event involving
7 nonpublic information that is in the possession of a licensee has
8 occurred when either of the following criteria has been met:

9 1. This state is the state of domicile of the licensee, in
10 the case of an insurer, or this state is the home state of the
11 licensee, in the case of a producer, as those terms are defined in
12 the Oklahoma Producer Licensing Act, Sections 1435.1 through 1435.41
13 of Title 36 of the Oklahoma Statutes, and the cybersecurity event
14 has a reasonable likelihood of substantially harming a material part
15 of the normal operations of the licensee or any consumer residing in
16 this state; or

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

20 a. a cybersecurity event impacting the licensee of which
21 notice is required to be provided to any government
22 body, self-regulatory agency or any other supervisory
23 body pursuant to any state or federal law, or
24

1 b. a cybersecurity event that has a reasonable likelihood
2 of materially harming:

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

4 (2) any material part of the normal operation or
5 operations of the licensee.

6 B. The licensee making the notification required in subsection
7 A of this section shall provide as much of the following information
8 as possible, in a form to be prescribed by the Commissioner:

9 1. Date of the cybersecurity event;

10 2. Description of how the information was exposed, lost, stolen
11 or breached including the specific roles and responsibilities of
12 third-party service providers, if any;

13 3. How the cybersecurity event was discovered;

14 4. Whether any lost, stolen or breached information has been
15 recovered and, if so, how this was done;

16 5. The identity of the source of the cybersecurity event;

17 6. Whether the licensee has filed a police report or has
18 notified any regulatory, government or law enforcement agencies and,
19 if so, when such notification was provided;

20 7. Description of the specific types of information acquired
21 without authorization. Specific types of information means
22 particular data elements including, but not limited to, types of
23 medical information, financial information or information allowing
24 identification of the consumer;

1 8. The period during which the information system was
2 compromised by the cybersecurity event;

3 9. The number of total consumers in this state affected by the
4 cybersecurity event. The licensee shall provide the best estimate
5 in the initial report to the Commissioner and update this estimate
6 with each subsequent report to the Commissioner pursuant to this
7 section;

8 10. The results of any internal review identifying a lapse in
9 either automated controls or internal procedures, or confirming that
10 all automated controls or internal procedures were followed;

11 11. Description of efforts being undertaken to remediate the
12 situation which permitted the cybersecurity event to occur;

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

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

18 The licensee shall have a continuing obligation to update and
19 supplement initial and subsequent notifications to the Commissioner
20 regarding material changes to previously provided information
21 relating to the cybersecurity event.

22 C. A licensee shall comply with the procedures of the Security
23 Breach Notification Act, Section 161 et seq. of Title 24 of the
24 Oklahoma Statutes, to notify affected consumers and provide a copy

1 of the notice sent to consumers under that statute to the
2 Commissioner, when a licensee is required to notify the Commissioner
3 under subsection A of this section.

4 D. 1. In the case of a cybersecurity event in a system
5 maintained by a third-party service provider, of which the licensee
6 has become aware, the licensee shall treat the event as it would
7 under subsection A of this section unless the third-party service
8 provider provides the notice required under subsection A of this
9 section to the Commissioner and the licensee.

10 2. The computation of deadlines of the licensee shall begin on
11 the day after the third-party service provider notifies the licensee
12 of the cybersecurity event or the licensee otherwise has actual
13 knowledge of the cybersecurity event, whichever is sooner.

14 3. Nothing in this subsection shall prevent or abrogate an
15 agreement between a licensee and another licensee, a third-party
16 service provider or any other party to fulfill any of the
17 investigation requirements imposed or notice requirements imposed
18 under this act.

19 E. 1. In the case of a cybersecurity event involving nonpublic
20 information that is used by the licensee that is acting as an
21 assuming insurer, or in the possession, custody or control of a
22 licensee, that is acting as an assuming insurer and that does not
23 have a direct contractual relationship with the affected consumers,
24 the assuming insurer shall notify its affected ceding insurers and

1 the Commissioner of its state of domicile within three (3) business
2 days of making the determination that a cybersecurity event has
3 occurred. The ceding insurers that have a direct contractual
4 relationship with affected consumers shall fulfill the consumer
5 notification requirements imposed under the Security Breach
6 Notification Act, Section 161 et seq. of Title 24 of the Oklahoma
7 Statutes and any other notification requirements relating to a
8 cybersecurity event imposed under this section.

9 2. In the case of a cybersecurity event involving nonpublic
10 information that is in the possession, custody or control of a
11 third-party service provider of a licensee that is an assuming
12 insurer, the assuming insurer shall notify its affected ceding
13 insurers and the Commissioner of its state of domicile within three
14 (3) business days of receiving notice from its third-party service
15 provider that a cybersecurity event has occurred. The ceding
16 insurers that have a direct contractual relationship with affected
17 consumers shall fulfill the consumer notification requirements
18 imposed under Security Breach Notification Act, Section 161 et seq.
19 of Title 24 of the Oklahoma Statutes and any other notification
20 requirements relating to a cybersecurity event imposed under this
21 section.

22 F. In the case of a cybersecurity event involving nonpublic
23 information that is in the possession, custody or control of a
24 licensee that is an insurer or its third-party service provider for

1 which a consumer accessed the services of the insurer through an
2 independent insurance producer, and for which consumer notice is
3 required by this act or the Security Breach Notification Act,
4 Section 161 et seq. of Title 24 of the Oklahoma Statutes, the
5 insurer shall notify the producers of record of all affected
6 consumers of the cybersecurity event no later than the time at which
7 notice is provided to the affected consumers.

8 The insurer is excused from this obligation for any producers
9 who are not authorized by law or contract to sell, solicit or
10 negotiate on behalf of the insurer, and in those instances in which
11 the insurer does not have the current producer of record information
12 for an individual consumer. Any licensee acting as an assuming
13 insurer shall have no other notice obligations relating to a
14 cybersecurity event or other data breach under this section or any
15 other law of this state.

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

19 A. The Insurance Commissioner shall have power to examine and
20 investigate the affairs of any licensee to determine whether the
21 licensee has been or is engaged in any conduct in violation of the
22 provisions of this act. This power is in addition to the powers
23 which the Commissioner has under Section 309.1 through 309.6 of
24 Title 36 of the Oklahoma Statutes. Any investigation or examination

1 shall be conducted pursuant to Section 309.1 through 309.6 of Title
2 36 of the Oklahoma Statutes.

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

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

10 A. Any documents, materials or other information in the control
11 or possession of the Insurance Department that are furnished by a
12 licensee or an employee or agent thereof acting on behalf of a
13 licensee pursuant to the provisions of Section 4 and Section 5 of
14 this act or that are obtained by the Insurance Commissioner in an
15 investigation or examination pursuant to Section 6 of this act shall
16 be confidential by law and privileged, shall not be subject to the
17 Oklahoma Open Records Act, shall not be subject to subpoena, and
18 shall not be subject to discovery or admissible in evidence in any
19 private civil action. However, the Commissioner is authorized to
20 use the documents, materials or other information in the furtherance
21 of any regulatory or legal action brought as a part of the
22 Commissioner's duties. The Commissioner shall not otherwise make
23 the documents, materials or other information public without the
24 prior written consent of the licensee.

1 B. Neither the Commissioner nor any person who received
2 documents, materials or other information while acting under the
3 authority of the Commissioner shall be permitted or required to
4 testify in any private civil action concerning any confidential
5 documents, materials or information subject to subsection A of this
6 section.

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

9 1. May share documents, materials or other information,
10 including the confidential and privileged documents, materials or
11 information subject to subsection A of this section, with other
12 state, federal and international regulatory agencies, with the
13 National Association of Insurance Commissioners and its affiliates
14 or subsidiaries and with state, federal and international law
15 enforcement authorities, provided that the recipient agrees in
16 writing to maintain the confidentiality and privileged status of the
17 document, material or other information;

18 2. May receive documents, materials or information, including
19 otherwise confidential and privileged documents, materials or
20 information, from the National Association of Insurance
21 Commissioners, its affiliates or subsidiaries and from regulatory
22 and law enforcement officials of other foreign or domestic
23 jurisdictions, and shall maintain as confidential or privileged any
24 document, material or information received with notice or the

1 understanding that it is confidential or privileged under the laws
2 of the jurisdiction that is the source of the document, material or
3 information;

4 3. May share documents, materials or other information subject
5 to subsection A of this section, with a third-party consultant or
6 vendor, provided the consultant agrees in writing to maintain the
7 confidentiality and privileged status of the document, material or
8 other information; and

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

11 D. No waiver of any applicable privilege or claim of
12 confidentiality in the documents, materials or information shall
13 occur as a result of disclosure to the Commissioner under this
14 section or as a result of sharing as authorized in subsection C of
15 this section.

16 E. Nothing in this act shall prohibit the Commissioner from
17 releasing final, adjudicated actions that are open to public
18 inspection pursuant to the Oklahoma Open Records Act to a database
19 or other clearinghouse service maintained by the National
20 Association of Insurance Commissioners, its affiliates or
21 subsidiaries.

22 F. Documents, materials or other information in the possession
23 or control of the National Association of Insurance Commissioners or
24 a third-party consultant or vendor pursuant to this act shall be

1 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 as evidence in any
4 private civil action.

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

8 A. The Insurance Commissioner shall promulgate rules to
9 implement the provisions of this section.

10 B. The following exceptions shall apply to this act:

11 1. A licensee with fewer than ten (10) employees, including any
12 independent contractors, is exempt from Section 3 of this act;

13 2. A licensee subject to the Health Insurance Portability and
14 Accountability Act, Pub.L. 104-191, 110 Stat. 1936, as amended, that
15 has established and maintains an Information Security Program
16 pursuant to such statutes, rules, regulations, procedures or
17 guidelines established thereunder, will be considered to meet the
18 requirements of Section 3 of this act, provided that the licensee is
19 compliant with, and submits a written statement to the Commissioner
20 certifying its compliance with, the same; and

21 3. An employee, agent, representative or designee of a
22 licensee, who is also a licensee, is exempt from Section 3 of this
23 act and shall not be required to develop its own information
24 security program to the extent that the employee, agent,

1 representative or designee is covered by the information security
2 program of the licensee.

3 C. In the event that a licensee ceases to qualify for an
4 exception, the licensee shall have one hundred eighty (180) days to
5 comply with the provisions of this act.

6 D. In the case of a violation of this act, a licensee may be
7 penalized in accordance with Sections 908 and 1435.26 of Title 36 of
8 the Oklahoma Statutes, or any other provision providing for
9 penalties that the licensee is subject to under the license or
10 permit of the licensee.

11 SECTION 9. This act shall become effective November 1, 2020.

12

13 57-2-3923 CB 2/24/2020 10:55:07 AM

14

15

16

17

18

19

20

21

22

23

24