

1 AN ACT relating to insurance data security.

2 *Be it enacted by the General Assembly of the Commonwealth of Kentucky:*

3 ➔SECTION 1. A NEW SECTION OF SUBTITLE 3 OF KRS CHAPTER 304 IS
4 CREATED TO READ AS FOLLOWS:

5 *As used in Sections 1 to 10 of this Act:*

6 *(1) "Consumer" means an individual, including but not limited to an applicant,*
7 *policyholder, insured, beneficiary, claimant, and certificate holder:*

8 *(a) Who is a resident of this Commonwealth; and*

9 *(b) Whose nonpublic information is in a licensee's possession, custody, or*
10 *control;*

11 *(2) "Cybersecurity event":*

12 *(a) Means an event resulting in unauthorized access to, disruption of, or*
13 *misuse of an information system or nonpublic information stored on an*
14 *information system; and*

15 *(b) Shall not include:*

16 *1. Unauthorized acquisition of encrypted nonpublic information if the*
17 *encryption, process, or key is not also acquired, released, or used*
18 *without authorization; or*

19 *2. An event with regard to which the licensee has determined that the*
20 *nonpublic information accessed by an unauthorized person:*

21 *a. Has not been used or released; and*

22 *b. Has been returned or destroyed;*

23 *(3) "Encrypted" means the transformation of data into a form that results in a low*
24 *probability of assigning meaning without the use of a protective process or key;*

25 *(4) "Information security program" means the administrative, technical, and*
26 *physical safeguards that a licensee uses to access, collect, distribute, process,*
27 *protect, store, use, transmit, dispose of, or otherwise handle nonpublic*

1 information;

2 (5) "Information system":

3 (a) Means a discrete set of electronic nonpublic information resources
4 organized for the collection, processing, maintenance, use, sharing,
5 dissemination, or disposition of electronic information; and

6 (b) Shall include any specialized system such as industrial or process controls
7 systems, telephone switching and private branch exchange systems, and
8 environmental control systems;

9 (6) "Licensee":

10 (a) Means any person who is, or is required to be, licensed, authorized to
11 operate, or registered pursuant to the insurance laws of this state; and

12 (b) Shall not include:

13 1. A purchasing group or a risk retention group chartered and licensed
14 in a state other than this state; or

15 2. A licensee that is acting as an assuming insurer that is domiciled in
16 another state or jurisdiction;

17 (7) "Nonpublic information":

18 (a) Means electronic information that is not publicly available information;
19 and

20 (b) Shall include:

21 1. Business-related information of a licensee that if tampered with, or
22 disclosed, accessed, or used without authorization, would cause a
23 material adverse impact to the business, operations, or security of the
24 licensee;

25 2. Any confidential personal identifying information of a consumer,
26 including:

27 a. Social Security number;

- 1 **b. Operator's license number or personal identification card**
 2 **number;**
- 3 **c. Financial account number;**
- 4 **d. Credit or debit card number;**
- 5 **e. Any security code, access code, or password that would permit**
 6 **access to a consumer's financial account; or**
- 7 **f. Biometric records; and**
- 8 **3. Any information or data, except age or gender, in any form or**
 9 **medium created by or derived from a health care provider or a**
 10 **consumer that relates to:**
- 11 **a. The past, present, or future physical, mental, or behavioral**
 12 **health or condition of any consumer or member of the**
 13 **consumer's family;**
- 14 **b. The provision of health care to any consumer; or**
- 15 **c. Payment for the provision of health care to any consumer;**
- 16 **(8) "Person" means any individual or nongovernmental entity, including but not**
 17 **limited to any nongovernmental partnership, corporation, branch, agency, or**
 18 **association;**
- 19 **(9) (a) "Publicly available information" means any information that a licensee has**
 20 **a reasonable basis to believe is lawfully made available to the general public**
 21 **from:**
- 22 **1. Federal, state, or local government records;**
- 23 **2. Widely distributed media; or**
- 24 **3. Disclosures to the general public that are required to be made by**
 25 **federal, state, or local law.**
- 26 **(b) For purposes of this definition, a licensee has a reasonable basis to believe**
 27 **that information is lawfully made available to the general public if the**

1 licensee has taken steps to determine:

2 1. That the information is of the type that is available to the general
3 public; and

4 2. Whether the consumer can direct that information not be made
5 available to the general public, and if so, that the consumer has not
6 done so; and

7 (10) "Third-party service provider" means a person, other than a licensee, that:

8 (a) Contracts with a licensee to maintain, process, or store nonpublic
9 information; or

10 (b) Is otherwise permitted access to nonpublic information through its
11 provision of services to a licensee.

12 ➔SECTION 2. A NEW SECTION OF SUBTITLE 3 OF KRS CHAPTER 304 IS
13 CREATED TO READ AS FOLLOWS:

14 A licensee with fewer than fifty (50) employees, including independent contractors,
15 shall be exempt from the requirements of Sections 1 to 10 of this Act.

16 ➔SECTION 3. A NEW SECTION OF SUBTITLE 3 OF KRS CHAPTER 304 IS
17 CREATED TO READ AS FOLLOWS:

18 Notwithstanding any other law, Sections 1 to 10 of this Act establish the exclusive
19 requirements applicable to licensees, except licensees exempt under Section 2 of this
20 Act, under the laws of the Commonwealth of Kentucky for:

21 (1) Data security;

22 (2) The investigation of a cybersecurity event; and

23 (3) Notification to the commissioner regarding the occurrence of a cybersecurity
24 event.

25 ➔SECTION 4. A NEW SECTION OF SUBTITLE 3 OF KRS CHAPTER 304 IS
26 CREATED TO READ AS FOLLOWS:

27 (1) As used in this section:

- 1 (a) "Authorized individual" means an individual:
- 2 1. Known to, and screened by, the licensee; and
- 3 2. Determined to be necessary and appropriate to have access to the
- 4 nonpublic information held by the licensee and its information
- 5 systems;
- 6 (b) "Multi-factor authentication" means authentication through verification of
- 7 at least two (2) of the following methods of authentication factors:
- 8 1. Knowledge factors, such as a password;
- 9 2. Possession factors, such as a token or text message on a mobile
- 10 phone; or
- 11 3. Inherence factors, such as a biometric characteristic; and
- 12 (c) "Risk assessment" means the risk assessment that each licensee is required
- 13 to conduct under subsection (3) of this section.
- 14 (2) (a) Each licensee shall develop, implement, and maintain a comprehensive
- 15 written information security program based on the licensee's risk
- 16 assessment that contains administrative, technical, and physical safeguards
- 17 for the protection of nonpublic information and the licensee's information
- 18 system.
- 19 (b) The information security program required under this subsection shall be:
- 20 1. Commensurate with the:
- 21 a. Size and complexity of the licensee;
- 22 b. Nature and scope of the licensee's activities, including its use of
- 23 third-party service providers; and
- 24 c. Sensitivity of the nonpublic information used by the licensee or
- 25 in the licensee's possession, custody, or control; and
- 26 2. Designed to:
- 27 a. Protect the security and confidentiality of nonpublic information

- 1 and the security of the information system;
- 2 b. Protect against any threats or hazards to the security or integrity
- 3 of nonpublic information and the information system;
- 4 c. Protect against unauthorized access to or use of nonpublic
- 5 information and minimize the likelihood of harm to any
- 6 consumer; and
- 7 d. Define, and periodically reevaluate:
- 8 i. A schedule for retention of nonpublic information; and
- 9 ii. A mechanism for the destruction of nonpublic information
- 10 when no longer needed, which shall comply with KRS
- 11 365.725.

12 (3) Each licensee shall:

- 13 (a) Designate one (1) or more employees, an affiliate, or an outside vendor
- 14 designated to act on behalf of the licensee who is responsible for the
- 15 information security program;
- 16 (b) Identify reasonably foreseeable internal or external threats that could result
- 17 in unauthorized access, transmission, disclosure, misuse, alteration, or
- 18 destruction of nonpublic information, including the security of information
- 19 systems and nonpublic information that are accessible to, or held by, third-
- 20 party service providers;
- 21 (c) Assess the likelihood and potential damage of the threats identified under
- 22 paragraph (b) of this subsection, taking into consideration the sensitivity of
- 23 the nonpublic information;
- 24 (d) Assess the sufficiency of policies, procedures, information systems, and
- 25 other safeguards in place to manage the threats identified under paragraph
- 26 (b) of this subsection, including consideration of threats in each relevant
- 27 area of the licensee's operations, including:

- 1 1. Employee training and management;
- 2 2. Information systems, including network and software design,
- 3 information classification, governance, processing, storage,
- 4 transmission, and disposal; and
- 5 3. Detection, prevention, and response to attacks, intrusions, or other
- 6 system failures;
- 7 (e) Implement information safeguards to manage the threats identified in the
- 8 licensee's ongoing assessment; and
- 9 (f) No less than annually, assess the effectiveness of the key controls, systems,
- 10 and procedures of the safeguards implemented under paragraph (e) of this
- 11 subsection.
- 12 (4) Based on its risk assessment, each licensee shall:
- 13 (a) Design its information security program to mitigate the identified risks
- 14 commensurate with the:
- 15 1. Size and complexity of the licensee; and
- 16 2. Nature and scope of the licensee's activities, including its use of third-
- 17 party service providers;
- 18 (b) Implement the following security measures, as appropriate:
- 19 1. Place access controls on information systems, including controls to
- 20 authenticate and permit access only to authorized individuals to
- 21 protect against the unauthorized acquisition of nonpublic
- 22 information;
- 23 2. Identify and manage the data, personnel, devices, systems, and
- 24 facilities that enable the organization to achieve business purposes in
- 25 accordance with their relative importance to business objectives and
- 26 the organization's risk strategy;
- 27 3. Restrict physical access to nonpublic information to authorized

- 1 individuals only;
- 2 4. Protect, by encryption or other appropriate means, all nonpublic
- 3 information;
- 4 a. While being transmitted over an external network; and
- 5 b. Stored on a laptop computer or other portable computing or
- 6 storage device or media;
- 7 5. Adopt:
- 8 a. Secure development practices for in-house developed
- 9 applications utilized by the licensee; and
- 10 b. Procedures for evaluating, assessing, or testing the security of
- 11 externally developed applications utilized by the licensee;
- 12 6. Modify the information system in accordance with the licensee's
- 13 information security program;
- 14 7. Utilize effective controls, which may include multi-factor
- 15 authentication procedures for any individual accessing nonpublic
- 16 information;
- 17 8. Regularly test and monitor systems and procedures to detect actual
- 18 and attempted attacks on, or intrusions into, information systems;
- 19 9. Include audit trails within the information security program designed
- 20 to:
- 21 a. Detect and respond to cybersecurity events; and
- 22 b. Reconstruct material financial transactions sufficient to support
- 23 normal operations and obligations of the licensee;
- 24 10. Implement measures to protect against destruction, loss, or damage of
- 25 nonpublic information due to environmental hazards, such as fire and
- 26 water damage, or other catastrophes or technological failures; and
- 27 11. Develop, implement, and maintain procedures for the secure disposal

- 1 of nonpublic information in any format;
- 2 (c) Include cybersecurity risks in the licensee's enterprise risk management
- 3 process;
- 4 (d) Stay informed regarding emerging threats or vulnerabilities;
- 5 (e) Utilize reasonable security measures when sharing information
- 6 commensurate with the character of the sharing and the type of information
- 7 shared; and
- 8 (f) Provide its personnel with cybersecurity awareness training that is updated
- 9 as necessary to reflect risks identified by the licensee in its risk assessment.
- 10 (5) (a) A licensee's executive management or its delegates shall, at a minimum:
- 11 1. Develop, implement, and maintain the licensee's information security
- 12 program; and
- 13 2. If the licensee has a board of directors or other appropriate committee,
- 14 report at least annually, in writing, to the board or committee the
- 15 following information:
- 16 a. The overall status of the information security program and the
- 17 licensee's compliance with Sections 1 to 10 of this Act; and
- 18 b. Material matters related to the information security program,
- 19 addressing issues including risk assessment, risk management
- 20 and control decisions, third-party service provider arrangements,
- 21 results of testing, cybersecurity events or violations and
- 22 management's response to the events or violations, and
- 23 recommendations for changes in the information security
- 24 program.
- 25 (b) If a licensee's executive management delegates any of its responsibilities
- 26 under this subsection, executive management shall:
- 27 1. Oversee the development, implementation, and maintenance of the

1 licensee's information security program prepared by the delegate or
2 delegates; and

3 2. Receive a report from the delegate or delegates that complies with the
4 requirements of paragraph (a)2. of this subsection.

5 (6) Each licensee that uses a third-party service provider shall:

6 (a) Exercise due diligence in selecting the third-party service provider; and

7 (b) Require the third-party service provider to implement appropriate
8 administrative, technical, and physical measures to protect and secure the
9 information systems and nonpublic information that are accessible to, or
10 held by, the third-party service provider.

11 (7) Each licensee shall monitor, evaluate, and adjust, as appropriate, the information
12 security program consistent with:

13 (a) Any relevant changes in technology;

14 (b) The sensitivity of its nonpublic information;

15 (c) Internal or external threats to information; and

16 (d) The licensee's own changing business arrangements, including mergers
17 and acquisitions, alliances and joint ventures, outsourcing arrangements,
18 and changes to information systems.

19 (8) (a) As part of its information security program, each licensee shall establish a
20 written incident response plan designed to promptly respond to, and recover
21 from, any cybersecurity event that compromises:

22 1. The confidentiality, integrity, or availability of nonpublic information
23 in its possession;

24 2. The licensee's information systems; or

25 3. The continuing functionality of any aspect of the licensee's business
26 or operations.

27 (b) The incident response plan established under this subsection shall address

1 the following:

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

3 2. The goals of the incident response plan;

4 3. The definition of clear roles, responsibilities, and levels of decision-
5 making authority;

6 4. External and internal communications and information sharing;

7 5. Identification of requirements for the remediation of any identified
8 weaknesses in information systems and associated controls;

9 6. Documentation and reporting regarding cybersecurity events and
10 related incident response activities; and

11 7. The evaluation and revision, as necessary, of the incident response
12 plan following a cybersecurity event.

13 (9) (a) Each insurer domiciled in this state shall:

14 1. By February 15 of each year, submit to the commissioner a written
15 statement certifying that the insurer is in compliance with this section;

16 and

17 2. Maintain, for examination by the department, all records, schedules,
18 and data supporting the certification submitted under subparagraph 1.
19 of this paragraph for a period of five (5) years.

20 (b) 1. To the extent an insurer has identified areas, systems, or processes
21 that require material improvement, updating, or redesign, the insurer
22 shall document the identification and remedial efforts planned and
23 underway to address the areas, systems, or processes identified.

24 2. The documentation required under this paragraph shall be available
25 for inspection by the commissioner for a period of five (5) years.

26 (10) (a) An employee, agent, representative, or designee of a licensee, who is also a
27 licensee, shall be exempt from the requirements of this section and shall not

1 be required to develop its own information security program to the extent
2 that the employee, agent, representative, or designee is covered by the
3 information security program of the other licensee.

4 (b) In the event that a licensee ceases to qualify for an exception under
5 paragraph (a) of this subsection, the licensee shall have one hundred eighty
6 (180) days to comply with this section.

7 ➔SECTION 5. A NEW SECTION OF SUBTITLE 3 OF KRS CHAPTER 304 IS
8 CREATED TO READ AS FOLLOWS:

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

12 (b) During an investigation required under this subsection, the licensee, or
13 outside vendor or service provider designated to act on behalf of the
14 licensee, shall, at a minimum:

15 1. Determine whether a cybersecurity event has occurred;

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

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

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

24 (2) If a licensee learns that a cybersecurity event has or may have occurred in a
25 system maintained by a third-party service provider, the licensee shall complete,
26 or confirm and document that the third-party service provider has completed, the
27 steps listed in subsection (1)(b) of this section.

1 (3) Each licensee shall maintain, and produce upon demand of the commissioner,
 2 records concerning all cybersecurity events for a period of at least five (5) years
 3 from the date of the cybersecurity event.

4 ➔SECTION 6. A NEW SECTION OF SUBTITLE 3 OF KRS CHAPTER 304 IS
 5 CREATED TO READ AS FOLLOWS:

6 (1) Each licensee shall notify the commissioner of a cybersecurity event involving
 7 nonpublic information that is in the possession of the licensee as promptly as
 8 possible, but in no event later than three (3) business days from a determination
 9 that a cybersecurity event has occurred, if:

10 (a) In the case of an insurer, this state is the licensee's state of domicile and the
 11 cybersecurity event has a reasonable likelihood of harming any material
 12 part of normal operations of the licensee;

13 (b) In the case of an insurance producer, this state is the licensee's home state,
 14 as those terms are defined in KRS 304.9-020; or

15 (c) The licensee reasonably believes that:

16 1. The nonpublic information involved in the cybersecurity event is
 17 related to two hundred fifty (250) or more consumers residing in this
 18 state; and

19 2. The cybersecurity event is either of the following:

20 a. A cybersecurity event requiring the licensee to provide notice to
 21 any governmental body, self-regulatory agency, or any other
 22 supervisory body pursuant to any state or federal law; or

23 b. A cybersecurity event that has a reasonable likelihood of
 24 materially harming any:

25 i. Consumer residing in this state; or

26 ii. Material part of the normal operations of the licensee.

27 (2) (a) In its notification to the commissioner under subsection (1) of this section,

1 the licensee shall provide, in an electronic form prescribed by the
2 commissioner, the following information:

3 1. The date of the cybersecurity event;

4 2. A description of how the information was exposed, lost, stolen, or
5 breached, including the specific roles and responsibilities of third-
6 party service providers, if any;

7 3. How the cybersecurity event was discovered;

8 4. Whether any lost, stolen, or breached information has been recovered,
9 and if so, how the information was recovered;

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

11 6. Whether the licensee has filed a police report or has notified any
12 regulatory, government, or law enforcement agencies, and if so, when
13 the notification was provided;

14 7. A description of the specific types of information acquired without
15 authorization, including but not limited to types of medical
16 information, financial information, or information allowing
17 identification of the consumer;

18 8. The period during which the information system was compromised by
19 the cybersecurity event;

20 9. The licensee's best estimate of the number of total consumers in this
21 state affected by the cybersecurity event, which shall be updated with
22 each subsequent report to the commissioner pursuant to this section;

23 10. The results of any internal review:

24 a. Identifying a lapse in automated controls or internal procedures;

25 or

26 b. Confirming that all automated controls or internal procedures
27 were followed;

- 1 11. A description of the efforts being undertaken to remediate the
2 situation that permitted the cybersecurity event to occur;
- 3 12. A copy of the licensee's privacy policy and a statement outlining the
4 steps the licensee will take to investigate and notify consumers affected
5 by the cybersecurity event;
- 6 13. A copy of the notice sent to consumers under KRS 365.732, if
7 applicable; and
- 8 14. The name of a contact person who is familiar with the cybersecurity
9 event and authorized to act for the licensee.
- 10 (b) The licensee shall have a continuing obligation under subsection (1) of this
11 section to update and supplement initial and subsequent notifications to the
12 commissioner concerning the cybersecurity event.
- 13 (3) Each licensee shall comply with KRS 365.732, as applicable.
- 14 (4) In the case of a cybersecurity event in a system maintained by a third-party
15 service provider of which the licensee has become aware:
- 16 (a) Except as provided under subsection (5) of this section, the licensee shall
17 treat the cybersecurity event as it would under subsection (1) of this section;
18 and
- 19 (b) The computation of the licensee's deadlines under this subsection shall
20 begin on the earlier of the day after:
- 21 1. The third-party service provider notifies the licensee of the
22 cybersecurity event; or
- 23 2. The licensee otherwise has actual knowledge of the cybersecurity
24 event.
- 25 (5) Nothing in Sections 1 to 10 of this Act shall prevent or abrogate an agreement
26 between a licensee and another licensee, a third-party service provider, or any
27 other party to fulfill the obligations of or obligations similar to:

1 (a) Investigation requirements under Section 5 of this Act; or

2 (b) Notice requirements under this section.

3 (6) (a) In the case of a cybersecurity event involving nonpublic information that is
4 used by a licensee acting as an assuming insurer, or that is in the
5 possession, custody, or control of a licensee that is acting as an assuming
6 insurer, and the assuming insurer does not have a direct contractual
7 relationship with the affected consumers, the assuming insurer shall notify
8 its affected ceding insurers and the commissioner of its state of domicile
9 within three (3) business days of making the determination that a
10 cybersecurity event has occurred.

11 (b) In the case of a cybersecurity event involving nonpublic information that is
12 in the possession, custody, or control of a third-party service provider of a
13 licensee that is an assuming insurer, the assuming insurer shall notify its
14 affected ceding insurers and the commissioner of its state of domicile within
15 three (3) business days of receiving notice from its third-party service
16 provider that a cybersecurity event has occurred.

17 (c) A ceding insurer under paragraphs (a) or (b) of this subsection that has a
18 direct contractual relationship with affected consumers shall fulfill:

19 1. The consumer notification requirements imposed under KRS 365.732;

20 and

21 2. Any other notification requirements relating to a cybersecurity event
22 under this section.

23 (d) Except as provided in paragraphs (a) or (b) of this subsection, a licensee
24 acting as an assuming insurer shall not be subject to any notice obligations
25 relating to a cybersecurity event or other data breach under this section.

26 (7) (a) Except as provided in paragraph (b) of this subsection, in the case of a
27 cybersecurity event involving nonpublic information that is in the

1 possession, custody, or control of a licensee that is an insurer, or its third-
 2 party service provider, and for which a consumer accessed the insurer's
 3 services through an independent insurance producer, the insurer shall
 4 notify the producers of record at the same time as all affected consumers
 5 when a licensee is required to notify consumers under KRS 365.732.

6 (b) An insurer shall not be required to comply with paragraph (a) of this
 7 subsection when the insurer does not have the current producer of record
 8 information for any individual consumer.

9 ➔SECTION 7. A NEW SECTION OF SUBTITLE 3 OF KRS CHAPTER 304 IS
 10 CREATED TO READ AS FOLLOWS:

11 (1) (a) The commissioner shall have the power to examine and investigate the
 12 affairs of any licensee to determine whether the licensee has been or is
 13 engaged in any conduct in violation of Section 4, 5, or 6 of this Act.

14 (b) The power granted to the commissioner under this subsection shall be in
 15 addition to the powers of the commissioner under KRS 304.2-100.

16 (c) Any investigation or examination conducted under this subsection shall be
 17 conducted pursuant to KRS 304.2-210.

18 (2) If the commissioner has reason to believe that a licensee has been or is engaged
 19 in conduct in this state that violates Section 4, 5, or 6 of this Act, the
 20 commissioner may take action that is necessary or appropriate to enforce the
 21 relevant provisions.

22 ➔SECTION 8. A NEW SECTION OF SUBTITLE 3 OF KRS CHAPTER 304 IS
 23 CREATED TO READ AS FOLLOWS:

24 (1) (a) Subject to paragraph (b) of this subsection and subsections (3) and (6) of
 25 this section, any documents, materials, or other information in the control
 26 or possession of the department that are furnished by a licensee, or an
 27 employee or agent acting on behalf of a licensee, under Section 4, 5, or 6 of

1 this Act or that are obtained by the commissioner in an investigation or
2 examination under Section 7 of this Act shall:

- 3 1. Be confidential by law and privileged;
- 4 2. Not be subject to KRS 61.870 to 61.884;
- 5 3. Not be subject to subpoena; and
- 6 4. Not be subject to discovery or admissible in evidence in any private
7 civil action.

8 (b) The commissioner may use documents, materials, or other information
9 referenced under paragraph (a) of this subsection in furtherance of any
10 regulatory or legal action brought as part of the commissioner's duties, and
11 shall not otherwise make the documents, materials, or other information
12 public without the written consent of the licensee.

13 (2) The commissioner, and any person who received documents, materials, or other
14 information while acting under the authority of the commissioner, shall not be
15 permitted, or required, to testify in any private civil action concerning any
16 confidential documents, materials, or other information subject to subsection
17 (1)(a) of this section.

18 (3) In order to assist in the performance of the commissioner's duties under Sections
19 1 to 10 of this Act, the commissioner:

20 (a) May share documents, materials, and other information, including
21 confidential and privileged documents, materials, or other information
22 subject to subsection (1) of this section, with the following if the recipient
23 agrees, in writing, to maintain the confidentiality and privileged status of
24 the documents, materials, or other information:

- 25 1. State, federal, and international regulatory agencies;
- 26 2. The National Association of Insurance Commissioners, its affiliates,
27 or subsidiaries; and

- 1 3. State, federal, and international law enforcement authorities;
- 2 (b) May receive documents, materials, and other information, including
- 3 confidential and privileged documents, materials, or information, from:
- 4 1. The National Association of Insurance Commissioners, its affiliates,
- 5 or subsidiaries; and
- 6 2. Regulatory and law enforcement officials of other foreign and
- 7 domestic jurisdictions;
- 8 (c) Shall maintain as confidential and privileged any document, material, or
- 9 information received with notice or understanding that it is confidential and
- 10 privileged under the laws of the jurisdiction that is the source of the
- 11 documents, materials, or other information;
- 12 (d) May share documents, materials, and other information subject to
- 13 subsection (1) this section with a third-party consultant or vendor, if the
- 14 consultant or vendor agrees, in writing, to maintain the confidentiality and
- 15 privileged status of the documents, materials, or other information; and
- 16 (e) May enter into agreements governing the sharing and use of information
- 17 consistent with this section.
- 18 (4) No waiver of any applicable privilege or claim of confidentiality shall occur as a
- 19 result of:
- 20 (a) A disclosure to the commissioner of documents, materials, or other
- 21 information under this section; or
- 22 (b) The sharing of the documents, materials, or other information as
- 23 authorized under subsection (3) of this section.
- 24 (5) Documents, materials, and other information in the possession or control of the
- 25 National Association of Insurance Commissioners or a third-party consultant or
- 26 vendor pursuant to Sections 1 to 10 of this Act shall:
- 27 (a) Be confidential by law and privileged;

- 1 (b) Not be subject to KRS 61.870 to 61.884;
 2 (c) Not be subject to subpoena; and
 3 (d) Not be subject to discovery or admissible in evidence in any private civil
 4 action.

- 5 (6) Nothing in Sections 1 to 10 of this Act shall prohibit the commissioner from
 6 releasing final, adjudicated actions that are open to public inspection under KRS
 7 304.2-150 to a database or other clearinghouse service maintained by the
 8 National Association of Insurance Commissioners, its affiliates, or subsidiaries.

9 ➔SECTION 9. A NEW SECTION OF SUBTITLE 3 OF KRS CHAPTER 304 IS
 10 CREATED TO READ AS FOLLOWS:

- 11 (1) A licensee shall be deemed in compliance with Sections 1 to 10 of this Act if the
 12 licensee:

- 13 (a) 1. Is subject to, governed by, and compliant with the privacy, security,
 14 and breach notifications rules issued by the United States Department
 15 of Health and Human Services, 45 C.F.R. Parts 160 and 164, as
 16 amended, established pursuant to the Health Insurance Portability
 17 and Accountability Act of 1996, Pub. L. No. 104-191, as amended, and
 18 the Health Information Technology for Economic and Clinical Health
 19 Act, Pub. L. No. 111-5, as amended;

- 20 2. Maintains nonpublic information in the same manner as protected
 21 health information; and

- 22 3. Submits to the commissioner:

- 23 a. An annual written statement certifying its compliance with the
 24 applicable provisions referenced under subparagraph 1. of this
 25 paragraph; and

- 26 b. A copy of any individual breach notification required under 45
 27 C.F.R. sec. 164.404, as amended, at the same time as all affected

1 individuals; or

2 (b) 1. Is a financial institution, as defined in KRS 304.9-135, that is subject
 3 to, governed by, and compliant with the privacy, security, and breach
 4 notification standards issued under Section 501 of the Gramm-Leach-
 5 Bliley Act of 1999, 15 U.S.C. sec. 6801, as amended; and

6 2. Submits to the commissioner:

7 a. An annual written statement certifying its compliance with the
 8 applicable provisions referenced under subparagraph 1. of this
 9 paragraph; and

10 b. A copy of any breach notification at the same time and in the
 11 same manner as notifications provided to the financial
 12 institution's federal regulatory authorities.

13 (2) Nothing in subsection (1)(a) of this section shall be construed to restrict the
 14 commissioner's authority to examine and investigate the affairs of any licensee
 15 under Section 7 of this Act to verify the licensee's annual certification under this
 16 section.

17 ➔SECTION 10. A NEW SECTION OF SUBTITLE 3 OF KRS CHAPTER 304
 18 IS CREATED TO READ AS FOLLOWS:

19 Penalties for violations of Sections 1 to 10 of this Act shall be in accordance with KRS
 20 304.99-020.

21 ➔Section 11. Pursuant to KRS 304.2-110, the commissioner may promulgate
 22 administrative regulations necessary for or as an aid to the effectuation of this Act.

23 ➔Section 12. If any provision of this Act or application thereof to any person or
 24 circumstance is for any reason held to be invalid, the invalidity shall not affect the
 25 remainder of the Act or the application of the provision to other persons or circumstances,
 26 and to this end the provisions of this Act are severable.

27 ➔Section 13. (a) Licensees shall have one year from the effective date of this

- 1 Act to implement subsections (1) to (3) and subsections (5) to (7) of Section 4 of this Act.
- 2 (b) Licensees shall have two years from the effective date of this Act to
- 3 implement subsection (4) of Section 4 of this Act.
- 4 ➔Section 14. This Act takes effect January 1, 2023.