

1 SB54
2 194392-7
3 By Senator Shelnutt
4 RFD: Banking and Insurance
5 First Read: 05-MAR-19

2
3
4 ENGROSSED

5
6
7 A BILL
8 TO BE ENTITLED
9 AN ACT

10
11 Relating to insurance; to require insurers and other
12 entities licensed by the Department of Insurance to develop,
13 implement, and maintain an information security program; to
14 provide for reporting to the Commissioner of Insurance,
15 including the reporting of cybersecurity events; to provide
16 that information provided to the commissioner pursuant to this
17 act would be confidential and privileged under certain
18 conditions; to provide for civil penalties under certain
19 conditions; and for this purpose to amend Sections
20 10A-20-6.16, as corrected by Act 2018-406, the Codification
21 Act, relating to certain nonprofit corporations, and
22 27-21A-23, Code of Alabama 1975, relating to health
23 maintenance organizations.

24 BE IT ENACTED BY THE LEGISLATURE OF ALABAMA:

25 Section 1. Short title.

26 This act shall be known and may be cited as the
27 Insurance Data Security Law.

1 Section 2. Purpose and intent.

2 (a) Notwithstanding any other provision of law, this
3 act establishes the exclusive state standards applicable to
4 licensees for data security, the investigation of a
5 cybersecurity event as defined in Section 3, and notification
6 to the Commissioner of Insurance of a cybersecurity event as
7 provided by this act.

8 (b) This act may not be construed to create or imply
9 a private cause of action for a violation of this act nor may
10 it be construed to curtail a private cause of action which
11 would otherwise exist in the absence of this act.

12 Section 3. Definitions.

13 For purposes of this act, the following words have
14 the following meanings:

15 (1) AUTHORIZED INDIVIDUAL. An individual known to
16 and screened by the licensee and determined to be necessary
17 and appropriate to have access to the nonpublic information
18 held by the licensee and its information systems.

19 (2) COMMISSIONER. The Commissioner of Insurance.

20 (3) CONSUMER. An individual, including, but not
21 limited to, an applicant, policyholder, insured, beneficiary,
22 claimant, or certificate holder, who is a resident of this
23 state and whose nonpublic information is in the possession,
24 custody, or control of a licensee.

25 (4)a. CYBERSECURITY EVENT. An event resulting in
26 unauthorized access to, disruption, or misuse of an

1 information system or nonpublic information stored on an
2 information system.

3 b. The term cybersecurity event does not include the
4 unauthorized acquisition of encrypted nonpublic information if
5 the encryption, process, or key is not also acquired,
6 released, or used without authorization.

7 c. Cybersecurity event does not include an event
8 with regard to which the licensee has determined that the
9 nonpublic information accessed by an unauthorized person has
10 not been used or released and has been returned or destroyed.

11 (5) DEPARTMENT. The Department of Insurance.

12 (6) ENCRYPTED. The transformation of data into a
13 form which results in a low probability of assigning meaning
14 without the use of a protective process or key.

15 (7) INFORMATION SECURITY PROGRAM. The
16 administrative, technical, and physical safeguards that a
17 licensee uses to access, collect, distribute, process,
18 protect, store, use, transmit, dispose of, or otherwise handle
19 nonpublic information.

20 (8) INFORMATION SYSTEM. A discrete set of electronic
21 information resources organized for the collection,
22 processing, maintenance, use, sharing, dissemination, or
23 disposition of electronic nonpublic information, as well as
24 any specialized system such as industrial/process controls
25 systems, telephone switching and private branch exchange
26 systems, and environmental control systems.

1 (9) LICENSEE. Any person licensed, authorized to
2 operate, or registered, or required to be licensed,
3 authorized, or registered pursuant to the insurance laws of
4 this state but shall not include a purchasing group or a risk
5 retention group chartered and licensed in a state other than
6 this state or a licensee that is acting as an assuming insurer
7 that is domiciled in another state or jurisdiction.

8 (10) MULTI-FACTOR AUTHENTICATION. Authentication
9 through verification of at least two of the following types of
10 authentication factors:

- 11 a. Knowledge factors, such as a password.
- 12 b. Possession factors, such as a token or text
13 message on a mobile phone.
- 14 c. Inherence factors, such as a biometric
15 characteristic.

16 (11) NONPUBLIC INFORMATION. Electronic information
17 that is not publicly available information and is any of the
18 following:

- 19 a. Any information concerning a consumer which
20 because of name, number, personal mark, or other identifier
21 can be used to identify the consumer, in combination with any
22 one or more of the following data elements:
 - 23 1. The Social Security number.
 - 24 2. The driver's license number or nondriver
25 identification card number.
 - 26 3. Any financial account number or a credit or debit
27 card number.

1 4. Any security code, access code, or password that
2 would permit access to a consumer's financial account.

3 5. Biometric records.

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

8 1. The past, present, or future physical, mental, or
9 behavioral health or condition of a consumer or a member of
10 the consumer's family.

11 2. The provision of health care to any consumer.

12 3. Payment for the provision of health care to any
13 consumer.

14 (12) PERSON. Any individual or any nongovernmental
15 entity, including, but not limited to, any nongovernmental
16 partnership, corporation, branch, agency, or association.

17 (13)a. PUBLICLY AVAILABLE INFORMATION. Any
18 information that a licensee has a reasonable basis to believe
19 is lawfully made available to the general public from federal,
20 state, or local government records; widely distributed media;
21 or disclosures to the general public that are required to be
22 made by federal, state, or local law.

23 b. For the purposes of this definition, a licensee
24 has a reasonable basis to believe that information is lawfully
25 made available to the general public if the licensee has taken
26 steps to determine both of the following:

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

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

6 (14) RISK ASSESSMENT. The risk assessment that each
7 licensee is required to conduct under subsection (c) of
8 Section 4.

9 (15) STATE. The State of Alabama.

10 (16) THIRD-PARTY SERVICE PROVIDER. A person, not
11 defined as a licensee, who contracts with a licensee to
12 maintain, process, store, or access nonpublic information
13 through the provision of services to the licensee.

14 Section 4. Information Security Program.

15 (a) Commensurate with the size and complexity of the
16 licensee, the nature and scope of the activities of the
17 licensee, including its use of third-party service providers,
18 and the sensitivity of the nonpublic information used by the
19 licensee or in the possession, custody, or control of the
20 licensee, each licensee shall develop, implement, and maintain
21 a comprehensive written information security program based on
22 the risk assessment of the licensee that contains
23 administrative, technical, and physical safeguards for the
24 protection of nonpublic information and the information system
25 of the licensee.

26 (b) The information security program of a licensee
27 shall be designed to do all of the following:

1 (1) Protect the security and confidentiality of
2 nonpublic information and the security of the information
3 system.

4 (2) Protect against any threats or hazards to the
5 security or integrity of nonpublic information and the
6 information system.

7 (3) Protect against unauthorized access to or use of
8 nonpublic information and minimize the likelihood of harm to
9 any consumer.

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

13 (c) The licensee shall do all of the following:

14 (1) Designate one or more employees, an affiliate,
15 or an outside vendor to act on behalf of the licensee who is
16 responsible for the information security program.

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

23 (3) Assess the likelihood and potential damage of
24 these threats, taking into consideration the sensitivity of
25 the nonpublic information.

26 (4) Assess the sufficiency of policies, procedures,
27 information systems, and other safeguards in place to manage

1 these threats, including consideration of threats in each
2 relevant area of the operations of the licensee, including all
3 of the following:

4 a. Employee training and management.

5 b. Information systems, including network and
6 software design, as well as information classification,
7 governance, processing, storage, transmission, and disposal.

8 c. Detecting, preventing, and responding to attacks,
9 intrusions, or other systems failures.

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

14 (d) Based on its risk assessment, the licensee shall
15 do all of the following:

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

23 (2) Determine which security measures listed below
24 are appropriate and, if appropriate, do the following to
25 implement the security measures:

26 a. Place access controls on information systems,
27 including controls to authenticate and permit access only to

1 authorized individuals to protect against the unauthorized
2 acquisition of nonpublic information.

3 b. Identify and manage the data, personnel, devices,
4 systems, and facilities that enable the organization to
5 achieve business purposes in accordance with their relative
6 importance to business objectives and the risk strategy of the
7 licensee.

8 c. Restrict physical access to nonpublic information
9 to authorized individuals only.

10 d. Protect by encryption or other appropriate means,
11 all nonpublic information while being transmitted over an
12 external network and all nonpublic information stored on any
13 laptop computer or other portable computing or storage device
14 or media.

15 e. Adopt secure development practices for in-house
16 developed applications utilized by the licensee.

17 f. Modify the information system in accordance with
18 the information security program of the licensee.

19 g. Utilize effective controls, which may include
20 multi-factor authentication procedures for employees accessing
21 nonpublic information.

22 h. Regularly test and monitor systems and procedures
23 to detect actual and attempted attacks on, or intrusions into,
24 information systems.

25 i. Include audit trails within the information
26 security program designed to detect and respond to
27 cybersecurity events and designed to reconstruct material

1 financial transactions sufficient to support normal operations
2 and obligations of the licensee.

3 j. Implement measures to protect against
4 destruction, loss, or damage of nonpublic information due to
5 environmental hazards, such as fire and water damage or other
6 catastrophes or technological failures.

7 k. Develop, implement, and maintain procedures for
8 the secure disposal of nonpublic information in any format.

9 (3) Include cybersecurity risks in the enterprise
10 risk management process of the licensee.

11 (4) Stay informed regarding emerging threats or
12 vulnerabilities and utilize reasonable security measures when
13 sharing information relative to the character of the sharing
14 and the type of information shared.

15 (5) Provide its personnel with cybersecurity
16 awareness training that is updated as necessary to reflect
17 risks identified by the licensee in the risk assessment.

18 (e) If the licensee has a board of directors, the
19 board or an appropriate committee of the board, at a minimum,
20 shall do all of the following:

21 (1) Require the executive management of the licensee
22 or its delegates to develop, implement, and maintain the
23 information security program of the licensee.

24 (2) Require the executive management of the licensee
25 or its delegates to report in writing at least annually, all
26 of the following:

1 a. The overall status of the information security
2 program of the licensee and the compliance of the licensee
3 with this act.

4 b. Material matters related to the information
5 security program, addressing issues such as risk assessment,
6 risk management and control decisions, third-party service
7 provider arrangements, results of testing, cybersecurity
8 events or violations and the responses of management thereto,
9 and recommendations for changes in the information security
10 program.

11 (3) If executive management delegates any of its
12 responsibilities under this section, it shall oversee the
13 development, implementation, and maintenance of the
14 information security program of the licensee prepared by the
15 delegate and shall receive a report from the delegate
16 complying with the requirements of the report to the board of
17 directors.

18 (f) (1) A licensee shall exercise due diligence in
19 selecting a third-party service provider.

20 (2) A licensee shall require a third-party service
21 provider to implement appropriate administrative, technical,
22 and physical measures to protect and secure the information
23 systems and nonpublic information that are accessible to, or
24 held by, the third-party service provider.

25 (g) The licensee shall monitor, evaluate, and
26 adjust, as appropriate, the information security program
27 consistent with any relevant changes in technology, the

1 sensitivity of its nonpublic information, internal or external
2 threats to information, and the changing business arrangements
3 of the licensee, such as mergers and acquisitions, alliances
4 and joint ventures, outsourcing arrangements, and changes to
5 information systems.

6 (h) (1) As part of its information security program,
7 each licensee shall establish a written incident response plan
8 designed to promptly respond to, and recover from, any
9 cybersecurity event that compromises the confidentiality,
10 integrity, or availability of nonpublic information in its
11 possession, the information systems of the licensee, or the
12 continuing functionality of any aspect of the business or
13 operations of the licensee.

14 (2) The incident response plan shall address all of
15 the following areas:

16 a. The internal process for responding to a
17 cybersecurity event.

18 b. The goals of the incident response plan.

19 c. The definition of clear roles, responsibilities,
20 and levels of decision-making authority.

21 d. External and internal communications and
22 information sharing.

23 e. Identification of requirements for the
24 remediation of any identified weaknesses in information
25 systems and associated controls.

26 f. Documentation and reporting regarding
27 cybersecurity events and related incident response activities.

1 g. The evaluation and revision as necessary of the
2 incident response plan following a cybersecurity event.

3 (i) Each insurer domiciled in this state, annually
4 on or before February 15, shall submit to the commissioner a
5 written statement certifying that the insurer is in compliance
6 with the requirements set forth in this act. Each insurer
7 shall maintain for examination by the department all records,
8 schedules, and data supporting this certificate for a period
9 of five years. To the extent an insurer has identified areas,
10 systems, or processes that require material improvement,
11 updating, or redesign, the insurer shall document the
12 identification and the remedial efforts planned and underway
13 to address the areas, systems, or processes. The documentation
14 shall be available for inspection by the commissioner.

15 Section 5. Investigation of a Cybersecurity Event.

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

20 (b) During the investigation, the licensee, or an
21 outside vendor or service provider designated to act on behalf
22 of the licensee, at a minimum, shall determine as much of the
23 following information as possible:

24 (1) If a cybersecurity event has occurred.

25 (2) The nature and scope of the cybersecurity event.

26 (3) Any nonpublic information that may have been
27 involved in the cybersecurity event.

1 (c) The licensee shall perform or oversee reasonable
2 measures to restore the security of the information systems
3 compromised in the cybersecurity event in order to prevent
4 further unauthorized acquisition, release, or use of nonpublic
5 information in the possession, custody, or control of the
6 licensee.

7 (d) If the licensee learns that a cybersecurity
8 event has or may have occurred in a system maintained by a
9 third-party service provider, the licensee shall complete the
10 steps listed in subsection (b) or confirm and document that
11 the third-party service provider has completed those steps.

12 (e) The licensee shall maintain records concerning
13 all cybersecurity events for a period of at least five years
14 from the date of the cybersecurity event and shall produce
15 those records upon demand of the commissioner.

16 Section 6. Notification of a Cybersecurity Event.

17 (a) Each licensee shall notify the commissioner as
18 promptly as possible, but in no event later than three
19 business days from a determination that a cybersecurity event
20 involving nonpublic information that is in the possession of a
21 licensee has occurred when either of the following criteria
22 has been met:

23 (1) This state is the state of domicile of the
24 licensee, in the case of an insurer, or this state is the home
25 state of the licensee, in the case of a producer, as those
26 terms are defined in Section 27-7-1, Code of Alabama 1975, and
27 the cybersecurity event has a reasonable likelihood of

1 materially harming a consumer residing in this state or
2 reasonable likelihood of materially harming any material part
3 of the normal operation of the licensee.

4 (2) The licensee reasonably believes that the
5 nonpublic information involves 250 or more consumers residing
6 in this state and the cybersecurity event is either of the
7 following:

8 a. A cybersecurity event impacting the licensee that
9 the licensee is required to notify any government body,
10 self-regulatory agency, or any other supervisory body about
11 pursuant to any state or federal law.

12 b. A cybersecurity event that has a reasonable
13 likelihood of materially harming either of the following:

14 1. Any consumer residing in this state.

15 2. Any material part of the normal operation of the
16 licensee.

17 (b) The licensee shall provide as much of the
18 following information as possible in electronic form as
19 directed by the commissioner:

20 (1) The date of the cybersecurity event.

21 (2) A description of how the information was
22 exposed, lost, stolen, or breached, including the specific
23 roles and responsibilities of any third-party service
24 providers.

25 (3) How the cybersecurity event was discovered.

26 (4) Whether any lost, stolen, or breached
27 information has been recovered and if so, how this was done.

1 (5) The identity of the source of the cybersecurity
2 event.

3 (6) Whether the licensee has filed a police report
4 or has notified any regulatory, government, or law enforcement
5 agencies and, if so, when the notification was provided.

6 (7) A description of the specific types of
7 information acquired without authorization. Specific types of
8 information means particular data elements including, for
9 example, types of medical information, types of financial
10 information, or types of information allowing identification
11 of the consumer.

12 (8) The period during which the information system
13 was compromised by the cybersecurity event.

14 (9) The number of total consumers in this state
15 affected by the cybersecurity event. The licensee shall
16 provide the best estimate in the initial report to the
17 commissioner and update this estimate with each subsequent
18 report to the commissioner pursuant to this section.

19 (10) The results of any internal review identifying
20 a lapse in either automated controls or internal procedures,
21 or confirming that all automated controls or internal
22 procedures were followed.

23 (11) A description of efforts being undertaken to
24 remediate the situation which permitted the cybersecurity
25 event to occur.

26 (12) A copy of the privacy policy of the licensee
27 and a statement outlining the steps the licensee will take to

1 investigate and notify consumers affected by the cybersecurity
2 event.

3 (13) The name of a contact person who is both
4 familiar with the cybersecurity event and authorized to act
5 for the licensee.

6 (c) The licensee shall have a continuing obligation
7 to update and supplement initial and subsequent notifications
8 regarding material changes to previously provided information
9 relating to the cybersecurity event.

10 (d) The licensee shall comply with Act 2018-396 of
11 the 2018 Regular Session as applicable and provide a copy of
12 the notice sent to consumers under the law to the
13 commissioner.

14 (e) (1) If the licensee becomes aware of a
15 cybersecurity event in a system maintained by a third-party
16 service provider, the licensee shall treat the event in the
17 same manner as provided under subsection (a) unless the
18 third-party service provider provides the notice required
19 under subsection (a) to the commissioner.

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

25 (3) Nothing in this act shall prevent or abrogate an
26 agreement between a licensee and another licensee, a
27 third-party service provider, or any other party to fulfill

1 any of the investigation requirements of Section 5 or the
2 notice requirements of this section.

3 (f)(1) a. In the case of a cybersecurity event
4 involving nonpublic information that is used by the licensee
5 that is acting as an assuming insurer or in the possession,
6 custody, or control of a licensee that is acting as an
7 assuming insurer and that does not have a direct contractual
8 relationship with the affected consumers, the assuming insurer
9 shall notify its affected ceding insurers and the commissioner
10 of its state of domicile within three business days of making
11 the determination that a cybersecurity event has occurred.

12 b. The ceding insurers that have a direct
13 contractual relationship with affected consumers shall fulfill
14 the consumer notification requirements under Act 2018-396,
15 2018 Regular Session, and any other notification requirements
16 relating to a cybersecurity event under this section.

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

25 b. The ceding insurers that have a direct
26 contractual relationship with affected consumers shall fulfill
27 the consumer notification requirements under Act 2018-396,

1 2018 Regular Session, and any other notification requirements
2 relating to a cybersecurity event under this section.

3 (3) Any licensee acting as assuming insurer shall
4 have no other notice obligations relating to a cybersecurity
5 event or other data breach under this section or any other law
6 of this state.

7 (g) (1) In the case of a cybersecurity event
8 involving nonpublic information that is in the possession,
9 custody, or control of a licensee that is an insurer or its
10 third-party service provider for which a consumer accessed the
11 services of the insurer through an independent insurance
12 producer, and for which consumer notice is required by Act
13 2018-396, 2018 Regular Session, the insurer shall notify the
14 producers of record of all affected consumers of the
15 cybersecurity event no later than the time at which notice is
16 provided to the affected consumers.

17 (2) The insurer is excused from this obligation for
18 any producers who are not authorized by law or contract to
19 sell, solicit, or negotiate on behalf of the insurer, and in
20 those instances in which the insurer does not have the current
21 producer of record information for an individual consumer.

22 Section 7. Power of Commissioner.

23 (a) The commissioner may examine and investigate
24 into the affairs of any licensee to determine whether the
25 licensee has been or is engaged in any conduct in violation of
26 this act. This power is in addition to the powers which the
27 commissioner has under Section 27-2-21, Code of Alabama 1975.

1 The investigation or examination shall be conducted pursuant
2 to Sections 27-2-22, et seq., Code of Alabama 1975.

3 (b) If the commissioner has reason to believe that a
4 licensee has been or is engaged in conduct in this state which
5 violates this act, the commissioner may take action that is
6 necessary or appropriate to enforce this act.

7 Section 8. Confidentiality.

8 (a) (1) Any documents, materials, or other
9 information in the control or possession of the department
10 that are furnished by a licensee or an employee or agent
11 acting on behalf of a licensee pursuant to subsection (i) of
12 Section 4; subdivisions (2), (3), (4), (5), (8), (10), and
13 (11) of subsection (b) of Section 6; or that are obtained by
14 the commissioner in an investigation or examination pursuant
15 to Section 7 shall be confidential by law and privileged,
16 shall not be subject to any open records, freedom of
17 information, sunshine, or other public record disclosure laws,
18 shall not be subject to subpoena, and shall not be subject to
19 discovery or admissible in evidence in any private civil
20 action. The commissioner shall not otherwise make the
21 documents, materials, or other information public without the
22 prior written consent of the licensee.

23 (2) Notwithstanding subdivision (1), the
24 commissioner may use the documents, materials, or other
25 information in the furtherance of any regulatory or legal
26 action brought as a part of the duties of the commissioner.

1 (b) Neither the commissioner nor any person who
2 received documents, materials, or other information while
3 acting under the authority of the commissioner or with whom
4 the documents, materials, or other information are shared
5 pursuant to this section shall be permitted or required to
6 testify in any private civil action concerning any
7 confidential documents, materials, or information subject to
8 subsection (a).

9 (c) In order to assist in the performance of the
10 duties of the commissioner under this act, the commissioner
11 may do all of the following:

12 (1) Share documents, materials, or other
13 information, including the confidential and privileged
14 documents, materials, or information subject to subsection
15 (a), with other state, federal, and international regulatory
16 agencies, with the National Association of Insurance
17 Commissioners, its affiliates or subsidiaries, and with state,
18 federal, and international law enforcement authorities,
19 provided that the recipient agrees in writing to maintain the
20 confidentiality and privileged status of the documents,
21 materials, or other information.

22 (2) Receive documents, materials, or information,
23 including otherwise confidential and privileged documents,
24 materials, or information, from the National Association of
25 Insurance Commissioners, its affiliates or subsidiaries and
26 from regulatory and law enforcement officials of other foreign
27 or domestic jurisdictions, and shall maintain as confidential

1 or privileged any document, material, or information received
2 with notice or the understanding that it is confidential or
3 privileged under the laws of the jurisdiction that is the
4 source of the document, material, or information.

5 (3) Share documents, materials, or other information
6 subject to subsection (a) with a third-party consultant or
7 vendor provided the consultant agrees in writing to maintain
8 the confidentiality and privileged status of the document,
9 material, or other information.

10 (4) Enter into agreements governing sharing and use
11 of information consistent with this subsection.

12 (d) No waiver of any applicable privilege or claim
13 of confidentiality in the documents, materials, or information
14 shall occur as a result of disclosure to the commissioner
15 under this section or as a result of sharing as authorized in
16 subsection (c).

17 (e) Nothing in this act shall prohibit the
18 commissioner from releasing final adjudicated actions that are
19 open to public inspection to a database or other clearinghouse
20 service maintained by the National Association of Insurance
21 Commissioners, its affiliates or subsidiaries.

22 (f) Documents, materials, or other information in
23 the possession or control of the National Association of
24 Insurance Commissioners or a third-party consultant or vendor
25 pursuant to this act shall be confidential by law and
26 privileged, shall not be subject to open records, freedom of
27 information, sunshine, or other public record disclosure laws,

1 shall not be subject to subpoena, and shall not be subject to
2 discovery or admissible in evidence in any private civil
3 action.

4 Section 9. Exceptions.

5 (a) The following exceptions shall apply to this
6 act:

7 (1) A licensee is exempt from Section 4 of this act
8 if any of the following criteria apply:

9 a. The licensee has fewer than 25 employees.

10 b. The licensee has less than \$5 million in gross
11 annual revenue.

12 c. The license has less than \$10 million in year-end
13 total assets.

14 (2) A licensee subject to Pub.L. 104-191, 110 Stat.
15 1936, enacted August 21, 1996 (Health Insurance Portability
16 and Accountability Act) that has established and maintains an
17 information security program pursuant to the statutes, rules,
18 regulations, procedures, or guidelines established thereunder,
19 shall be considered to meet the requirements of this act,
20 provided that licensee is compliant with and submits a written
21 statement certifying its compliance with Pub. L. 104-191.

22 (3) An employee, agent, representative, or designee
23 of a licensee who is also a licensee is exempt from this act
24 and is not required to develop its own information security
25 program to the extent that the employee, agent,
26 representative, or designee is covered by the information
27 security program of the other licensee.

1 (4) A licensee affiliated with a depository
2 institution that maintains an Information Security Program in
3 compliance with the Interagency Guidelines Establishing
4 Standards for Safeguarding Customer Information as set forth
5 pursuant to Sections 501 and 505 of the Gramm-Leach-Bliley Act
6 (15 U.S.C. 6801 and 6805) shall be considered to meet the
7 requirements of Section 4, provided that the licensee
8 produces, upon request, documentation satisfactory to the
9 commissioner that independently validates the affiliated
10 depository institution's adoption of an Information Security
11 Program that satisfies the Interagency Guidelines.

12 (b) In the event a licensee ceases to qualify for an
13 exemption, the licensee shall have 180 days to comply with
14 this act.

15 Section 10. Penalties.

16 (a) An insurance producer violating this act may be
17 penalized in accordance with Section 27-7-19, Code of Alabama
18 1975.

19 (b) Any other licensee violating this act may be
20 subject to the suspension or revocation of the license or
21 certificate of authority of the licensee or, in lieu thereof
22 and at the discretion of the commissioner, the licensee may be
23 subject to a fine of up to ten thousand dollars (\$10,000) per
24 violation.

25 Section 11. Rules.

26 The commissioner may adopt rules implementing this
27 act pursuant to Chapter 2 of Title 27, Code of Alabama 1975.

1 Section 12. Severability.

2 If any provision of this act or the application
3 thereof to any person or circumstance is for any reason held
4 to be invalid, the remainder of the act and the application of
5 the provision to other persons or circumstances shall not be
6 affected thereby.

7 Section 13. Sections 10A-20-6.16, as corrected by
8 Act 2018-406, the Codification Act, and 27-21A-23, Code of
9 Alabama 1975, are amended to read as follows:

10 "§10A-20-6.16.

11 "(a) No statute of this state applying to insurance
12 companies shall be applicable to any corporation organized
13 under this article and amendments thereto or to any contract
14 made by the corporation; except the corporation shall be
15 subject to the following:

16 "(1) The provisions regarding annual premium tax to
17 be paid by insurers on insurance premiums.

18 "~~(2) Chapter 55 of Title 27, regarding the~~
19 ~~prohibition of unfair discriminatory acts by insurers on the~~
20 ~~basis of an applicant's or insured's abuse status.~~

21 "~~(3) The Medicare Supplement Minimum Standards set~~
22 ~~forth in Article 2 and Article 3 of Chapter 19 of Title 27,~~
23 ~~and Long-Term Care Insurance Policy Minimum Standards set~~
24 ~~forth in Article 3 of Chapter 19 of Title 27.~~

25 "~~(4) Section 27-1-17, requiring insurers and health~~
26 ~~plans to pay health care providers in a timely manner.~~

1 "~~(5) Chapter 56 of Title 27, regarding the Access to~~
2 ~~Eye Care Act.~~

3 "(6) Rules promulgated by the Commissioner of
4 Insurance pursuant to Sections 27-7-43 and 27-7-44.

5 "(7) Chapter 54 of Title 27.

6 "~~(8) Chapter 57 of Title 27, requiring coverage to~~
7 ~~be offered for the payment of colorectal cancer examinations~~
8 ~~for covered persons who are 50 years of age or older, or for~~
9 ~~covered persons who are less than 50 years of age and at high~~
10 ~~risk for colorectal cancer according to current American~~
11 ~~Cancer Society colorectal cancer screening guidelines.~~

12 "~~(9) Chapter 58 of Title 27, requiring that policies~~
13 ~~and contracts including coverage for prostate cancer early~~
14 ~~detection be offered, together with identification of~~
15 ~~associated costs.~~

16 "~~(10) Chapter 59 of Title 27, requiring that~~
17 ~~policies and contracts including coverage for chiropractic be~~
18 ~~offered, together with identification of associated costs.~~

19 "~~(11) Chapter 54A of Title 27, requiring that~~
20 ~~policies and contracts to offer coverage for certain treatment~~
21 ~~for Autism Spectrum Disorder under certain conditions.~~

22 "(12) Chapter 12A of Title 27.

23 "(13) Chapter 2B of Title 27.

24 "(14) Chapter 29 of Title 27.

25 "(15) The act adding this amendatory language.

26 "(b) The provisions in subsection (a) that require
27 specific types of coverage to be offered or provided shall not

1 apply when the corporation is administering a self-funded
2 benefit plan or similar plan, fund, or program that it does
3 not insure.

4 "§27-21A-23.

5 "(a) Except as otherwise provided in this chapter,
6 provisions of the insurance law and provisions of health care
7 service plan laws shall not be applicable to any health
8 maintenance organization granted a certificate of authority
9 under this chapter. This provision shall not apply to an
10 insurer or health care service plan licensed and regulated
11 pursuant to the insurance law or the health care service plan
12 laws of this state except with respect to its health
13 maintenance organization activities authorized and regulated
14 pursuant to this chapter.

15 "(b) Solicitation of enrollees by a health
16 maintenance organization granted a certificate of authority
17 shall not be construed to violate any provision of law
18 relating to solicitation or advertising by health
19 professionals.

20 "(c) Any health maintenance organization authorized
21 under this chapter shall not be deemed to be practicing
22 medicine and shall be exempt from the provisions of Section
23 34-24-310, et seq., relating to the practice of medicine.

24 "(d) No person participating in the arrangements of
25 a health maintenance organization other than the actual
26 provider of health care services or supplies directly to
27 enrollees and their families shall be liable for negligence,

1 misfeasance, nonfeasance, or malpractice in connection with
2 the furnishing of such services and supplies.

3 "(e) Nothing in this chapter shall be construed in
4 any way to repeal or conflict with any provision of the
5 certificate of need law.

6 "(f) Notwithstanding the provisions of subsection
7 (a), a health maintenance organization shall be subject to all
8 of the following:

9 "(1) Section 27-1-17.

10 "(2) Chapter 56, ~~regarding the Access to Eye Care~~
11 ~~Act.~~

12 "(3) Chapter 54, ~~regarding mental illness coverage.~~

13 "(4) Chapter 57, ~~requiring coverage to be offered~~
14 ~~for the payment of colorectal cancer examinations for covered~~
15 ~~persons who are 50 years of age or older, or for covered~~
16 ~~persons who are less than 50 years of age and at high risk for~~
17 ~~colorectal cancer according to current American Cancer Society~~
18 ~~colorectal cancer screening guidelines.~~

19 "(5) Chapter 58, ~~requiring that policies and~~
20 ~~contracts including coverage for prostate cancer early~~
21 ~~detection be offered, together with identification of~~
22 ~~associated costs.~~

23 "(6) Chapter 59, ~~requiring that policies and~~
24 ~~contracts including coverage for chiropractic be offered,~~
25 ~~together with identification of associated costs.~~

26 "(7) Rules promulgated by the Commissioner of
27 Insurance pursuant to Sections 27-7-43 and 27-7-44.

1 "(8) Chapter 12A.

2 "~~(9) Chapter 54A, requiring policies and contracts~~
3 ~~to cover certain treatment for Autism Spectrum Disorder under~~
4 ~~certain conditions.~~

5 "~~(10) Chapter 2B, regarding risk-based capital.~~

6 "~~(11) Chapter 29, regarding insurance holding~~
7 ~~company systems.~~

8 "(12) The act adding this amendatory language."

9 Section 14. Licensees shall have two years from the
10 effective date of this act to implement subsection (f) of
11 Section 4 and one year from the effective date of this act to
12 implement the remainder of Section 4.

13 Section 15. This act shall become effective
14 immediately upon its passage and approval by the Governor or
15 its otherwise becoming law.

1
2
3
4
5
6
7
8
9
10

11
12
13
14
15
16
17

Senate

Read for the first time and referred to the Senate
committee on Banking and Insurance..... 05-MAR-19

Read for the second time and placed on the calen-
dar 1 amendment..... 20-MAR-19

Read for the third time and passed as amended 02-APR-19

Yeas 32
Nays 0

Patrick Harris,
Secretary.