COMMONWEALTH OF VIRGINIA

STATE CORPORATION COMMISSION

AT RICHMOND, AUGUST 13, 2020

COMMONWEALTH OF VIRGINIA, *ex rel.*

STATE CORPORATION COMMISSION

CASE NO. INS-2020-00168

Ex Parte: In the matter of Adopting
Rules to Implement the Requirements
of the Insurance Data Security Act

ORDER TO TAKE NOTICE

Section 12.1-13 of the Code of Virginia ("Code") provides that the State Corporation Commission ("Commission") shall have the power to promulgate rules and regulations in the enforcement and administration of all laws within its jurisdiction, and § 38.2-223 of the Code provides that the Commission may issue any rules and regulations necessary or appropriate for the administration and enforcement of Title 38.2 of the Code.

The rules and regulations issued by the Commission pursuant to § 38.2-223 of the Code are set forth in Title 14 of the Virginia Administrative Code. The Bureau of Insurance ("Bureau") has submitted to the Commission proposed additions to the rules set forth in Title 14 of the Virginia Administrative Code, by adding Chapter 430, entitled Rules Governing Insurance Data Security Risk Assessment and Reporting, 14 VAC 5-430-10 *et seq.* ("Rules"). A copy of this order may also be found at the Commission's website: https://scc.virginia.gov/pages/Case-Information.

The addition of Chapter 430 to Title 14 of the Virginia Administrative Code is necessary to implement the provisions of Title 38.2, Chapter 6, Article 2, known as the Insurance Data Security Act, § 38.2-621, *et seq.* of the Code which was added during the 2020 General Assembly (Chapter 0264 of the 2020 Acts of Assembly), which requires that certain cybersecurity initiatives and notification procedures be implemented by insurers, insurance agencies and licensees or third-party providers defined or governed by Title 38.2 of the Code.

The proposed revisions as contained in Chapter 430 of the Virginia Administrative Code include the following:

- Requirements for implementing a periodic Information Security Program Risk Assessment, which will, among other things, identify internal or external cybersecurity threats and address safeguards to manage the potential threats.

- Requirements for implementing Information Security Program Security Measures to manage, protect against and respond to cybersecurity threats.

- Requirements and obligations of the Bureau's licensees who engage third-party providers to ensure compliance with the Code and the Rules.

- Requirements for reporting cybersecurity events to the Commissioner of Insurance and maintaining related records.

NOW THE COMMISSION, is of the opinion that the proposed revisions submitted by the Bureau to revise Title 14 of the Virginia Administrative Code by adding Chapter 430, Rules 14 VAC 5-430-10 through 14 VAC 5-430-70, should be considered for adoption with a proposed effective date of December 1, 2020.

Accordingly, IT IS ORDERED THAT:

(1) The proposal to add Rules 14 VAC 5-430-10 through 14 VAC 5-430-70 is attached hereto and made a part hereof.

(2) All interested persons who desire to comment in support of or in opposition to, or request a hearing to oppose the revisions to the Rules, shall file such comments or hearing request on or before October 26, 2020, with the Clerk of the Commission, State Corporation Commission, c/o Document Control Center, P.O. Box 2118, Richmond, Virginia 23218 and shall refer to Case No. INS-2020-00168. Interested persons desiring to submit comments electronically may do so by following the instructions at the Commission's website: https://scc.virginia.gov/casecomments/Submit-Public-Comments. All comments shall reference Case No. INS-2020-00168.

(3) If no written request for a hearing on the proposal to revise the Rules, as outlined in this Order, is received on or before October 26, 2020, the Commission, upon consideration of any comments submitted in support of or in opposition to the proposal, may adopt the Rules as submitted by the Bureau.

(4) The Bureau shall provide notice of the proposal to revise the Rules to all insurers, burial societies, fraternal benefit societies, health services plans, risk retention groups, joint underwriting associations, group self-insurance pools, and group self-insurance associations licensed by the Commission, to qualified reinsurers in Virginia, and to all interested persons.

(5) The Commission's Division of Information Resources shall cause a copy of this Order, together with the proposal to revise the Rules, to be forwarded to the Virginia Registrar of Regulations for appropriate publication in the *Virginia Register of Regulations*.

(6) The Commission's Division of Information Resources shall make available this Order and the attached proposed revisions to the Rules on the Commission's website: https://scc.virginia.gov/pages/Case-Information.

(7) The Bureau shall file with the Clerk of the Commission an affidavit of compliance with the notice requirements of Ordering Paragraph (4) above.

(8) This matter is continued.

A copy of this Order shall be sent by the Clerk of the Commission to:

C. Meade Browder, Jr., Senior Assistant Attorney General, Office of the Attorney General, Division of Consumer Counsel, by electronic mail at MBrowder@oag.state.va.us, and by first class mail, postage prepaid to 202 N. 9th Street, 8th Floor, Richmond, Virginia 23219-3424; and a copy hereof shall be delivered to the Commission's Office of General Counsel and the Bureau of Insurance in care of Deputy Commissioner Donald C. Beatty.

STATE CORPORATION COMMISSION, BUREAU OF INSURANCE

CH 430 Insurance Data Security Risk Assessment and Reporting

CHAPTER 430

INSURANCE DATA SECURITY RISK ASSESSMENT AND REPORTING

14VAC5-430-10. Applicability and scope.

This chapter sets forth rules to carry out the provisions of the Insurance Data Security Act, Article 2 (§ 38.2-621, et seq.) of Chapter 6 of Title 38.2 of the Code of Virginia, and sets minimum standards for risk assessment and security standards required of all licensees. However, as outlined, the specific requirements for licensees may differ in certain circumstances, depending on the size and complexity of the licensee. This chapter applies to and protects physical and electronic data, including nonpublic information, stored, transmitted, and processed across various information systems or any other media used by licensees.

14VAC5-430-20. Severability.

If any provision of this chapter or its application to any person or circumstance is for any reason held to be invalid by a court or the Commission, the remainder of this chapter and the application of the provisions to other persons or circumstances shall not be affected.

14VAC5-430-30. Definitions.

"Authorized person" means a person known to and authorized by the licensee and determined to be necessary and appropriate to have access to the nonpublic information held by the licensee and its information systems.

"Bureau" means the Bureau of Insurance.

"Code" means the Code of Virginia.

"Commissioner" means the Commissioner of Insurance.

"Consumer" means an individual, including any applicant, policyholder, former policyholder, insured, beneficiary, claimant, and certificate holder, who is a resident of Virginia and whose nonpublic information is in the possession, custody, or control of a licensee or an authorized person.

"Cybersecurity event" means an event resulting in unauthorized access to, disruption of, or misuse of an information system or nonpublic information in the possession, custody, or control of a licensee or an authorized person. "Cybersecurity event" does not include (i) the unauthorized acquisition of encrypted nonpublic information if the encryption, process, or key is not also acquired, released, or used without authorization or (ii) an event in which the licensee has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed.

"Encrypted" means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key.

"Home state" means the jurisdiction in which the producer maintains its principal place of residence or principal place of business and is licensed by that jurisdiction to act as a resident insurance producer.

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

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

"Level one licensee" means any licensee with more than 10 employees and authorized persons.

"Level two licensee" means any licensee with 10 or fewer employees and authorized persons. A level two licensee may choose to comply with the requirements for a level one licensee. If a licensee ceases to qualify as a level two licensee, the licensee shall have 180 days from the date it ceases to qualify to comply with the requirements of a level one licensee.

"Licensee" means any person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of Virginia. "Licensee" does not include a purchasing group or a risk retention group chartered and licensed in a state other than Virginia or a person that is acting as an assuming insurer that is domiciled in another state or jurisdiction.

"Multi-factor authentication" means authentication through verification of at least two of the following types of authentication factors:

1. Knowledge factors, such as a password; or

2. Possession factors, such as a token or text message on a mobile device; or

3. Inherence factors, such as a biometric characteristic.

"Nonpublic information" means information that is not publicly available information and is:

1. Business-related information of a licensee the tampering with which, or the unauthorized disclosure, access, or use of which, would cause a material adverse impact to the business, operations, or security of the licensee;

2. Any information concerning a consumer that because of name, number, personal mark, or other identifier can be used to identify such consumer, in any combination with a consumer's (i) social security number; (ii) driver's license number or nondriver

identification card number; (iii) financial account, credit card, or debit card number; (iv) security code, access code, or password that would permit access to a consumer's financial account; (v) passport number; (vi) military identification number; or (vii) biometric records; or

3. Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or a consumer that can be used to identify a particular consumer, and that relates to (i) the past, present, or future physical, mental, or behavioral health or condition of any consumer or a member of the consumer's family; (ii) the provision of health care to any consumer; or (iii) payment for the provision of health care to any consumer.

"Third-party service provider" means a person, not otherwise defined as a licensee, that contracts with a licensee to maintain, process, or store nonpublic information, or otherwise is permitted access to nonpublic information through its provision of services to the licensee, or an insurance-support organization.

14VAC5-430-40. Information security program risk assessment.

A.1. In addition to the requirements of § 38.2-623 of the Code, each level one licensee shall conduct periodic risk assessments consistent with the objectives of the most current revision of NIST SP 800-30, NIST SP 800-39, or other substantially similar standard, taking into consideration the level one licensee's size and complexity.

2. Each level one licensee shall consider cybersecurity risks in its enterprise risk management process.

3. Compliance with the provisions of this subsection is required for all level one licensees on or before (insert the effective date which will be one year from the effective date of this chapter).

B. In addition to the requirements of § 38.2-623 of the Code, taking into consideration the level two licensee's size and complexity, each level two licensee, shall conduct a periodic risk assessment consistent with the following elements:

1. Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of nonpublic information held by a level two licensee;

2. Assess the likelihood and potential damage of these threats taking into consideration the sensitivity of nonpublic information in the possession, custody, or control of the licensee and its authorized persons;

3. Assess the sufficiency of policies, procedures, information systems, and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the licensee's operations, such as employee training; information classification that includes the processing, storage, transmission, and disposal of information; and the detection, prevention, and response to attacks and intrusions; and

4. Implement information safeguards to manage the threats identified in the licensee's ongoing assessment and, no less than annually, assess the effectiveness of the key controls, systems, and procedures.

5. Compliance with the provisions of this subsection is required of all level two licensees on or before July 1, 2022.

14VAC5-430-50. Information security program security measures.

A.1. Based on its risk assessments, each level one licensee shall implement the appropriate measures consistent with NIST SP 800-53, NIST SP 800-171, or any substantially similar framework based on these standards, taking into consideration its size and complexity.

2. Compliance with the provisions of this subsection is required for all level one licensees on or before (insert the effective date which will be one year from the effective date of this chapter).

B. Based on its risk assessments, each level two licensee shall implement appropriate security measures as follows:

1. Manage the data, personnel, devices, systems, and facilities of the licensee in accordance with its identified risk;

2. Protect, by encryption or other appropriate means, all nonpublic information while being transmitted over an external network;

3. Protect, by encryption or other appropriate means, all nonpublic information stored on portable computing, storage devices, or media;

4. Adopt secure development practices for applications developed in-house and used by the licensee;

5. Adopt procedures for evaluating and assessing the security of externally developed applications utilized by the licensee;

6. Implement effective controls, including multi-factor authentication, for authorized individuals to access nonpublic information; and

7. Use audit trails or audit logs designed to detect and respond to cybersecurity events and to reconstruct material financial transactions.

8. Compliance with the provisions of this subsection is required of all level two licensees on or before July 1, 2022.

C. Effective July 1, 2022, each licensee that utilizes a third-party service provider shall:

1. Exercise due diligence in selecting a third-party service provider; and

2. Require the third-party service provider to implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information that are accessible to, or held by, the third-party service provider.

14VAC5-430-60. Reporting cybersecurity events to the Commissioner.

A.1. Once a licensee has determined that a cybersecurity event has occurred and the licensee has a duty to report it to the Commissioner pursuant to § 38.2-625 of the Code, the licensee shall notify the Commissioner within three business days that it has information to report, using the email address designated by the Bureau. This notification should include the name, telephone number and email address of the individual or individuals who is the licensee's designated contact for the cybersecurity event.

2. Instructions for communicating the information required by § 38.2-625 of the Code to the Commissioner through a secure portal will be provided by the Bureau in response to the email.

3. The licensee shall update the Commissioner on the progress of its investigation as information becomes known to the licensee until the licensee has provided all the information set forth in § 38.2-625 of the Code.

4. a. If also required to notify consumers under §§ 38.2-626 of the Code and 14 VAC 5-430-50, licensees shall provide the Commissioner with a copy of the notice template and any documentation provided to consumers.

b. Licensees shall maintain a list of consumers notified and retain the list for the longer of 5 years or the time frame established by § 38.2-624 D of the Code.

B. Except where nonpublic information has been accessed, once a domestic insurance company has notified the Commissioner of the date, nature, and scope of the cybersecurity event, the company may report all remaining information required by § 38.2-625 of the Code (i) annually

in a separate report, (ii) in the certification described in § 38.2-623 H of the Code or (iii) on a continuing basis through the portal established for the company by the Bureau for this purpose.

C. Unless exempted by § 38.2-629 A 2 of the Code, producers whose home state is Virginia shall report cybersecurity events to the Commissioner in accordance with subsection A of this section.

D. If required to report to the Commissioner, non-domestic insurance companies, and, unless exempted under § 38.2-629 A 2 of the Code, producers whose home state is not Virginia, shall notify the Commissioner of the cybersecurity event pursuant to § 38.2-625 A. 2 of the Code, as set forth in subsection A of this section.

14VAC5-430-70. Consumer notification provisions.

A. Licensees, except those exempted under § 38.2-629 A 2 of the Code, that determine a cybersecurity event has occurred, and has caused or has a reasonable likelihood of causing identity theft or other fraud to consumers whose information was accessed or acquired, shall notify those consumers in accordance with § 38.2-626 of the Code, subject to any applicable numerical threshold.

B. Each licensee required to notify consumers of a cybersecurity event that does not intend to notify consumers based on a belief that the cybersecurity event does not have a reasonable likelihood of causing identity theft or other fraud to the consumers shall notify the Commissioner of its position and provide a detailed explanation supporting the licensee's position.

C. If, upon review of the report, the cybersecurity event does have a reasonable likelihood of causing identity theft or other fraud to the consumer, the Commissioner may require the licensee to notify the affected consumers in accordance with § 38.2-626 of the Code.

DOCUMENTS INCORPORATED BY REFERENCE (14VAC5-430)

Enter document list here

NIST 800-30 (rev. 1)

NIST 800-39

NIST 800-53 (rev. 4)

NIST 800-171 (rev. 2)