COMMONWEALTH OF VIRGINIA

STATE CORPORATION COMMISSION

AT RICHMOND, MAY 24, 2021

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 ADOPTING REGULATIONS

On August 13, 2020, the State Corporation Commission ("Commission") entered an Order to Take Notice of a proposal by the Bureau of Insurance ("Bureau") to adopt new rules at Title 14, Chapter 430 of the Virginia Administrative Code (14VAC5-430-10 *et seq.*), entitled Insurance Data Security Risk Assessment and Reporting ("Rules").

The Bureau's proposed Rules were drafted to comply with the requirements of the Insurance Data Security Act, §§ 38.2-621 *et seq.* of the Code of Virginia ("IDSA"). The IDSA was enacted by the 2020 Virginia General Assembly and establishes standards that Bureau licensees must meet regarding data security, cybersecurity investigations, and notification to the Commissioner of Insurance and consumers of cybersecurity events. The IDSA also directed the Commission to adopt regulations to implement the requirements of the IDSA.[1] A detailed summary of these proposed amendments was set forth in the Order to Take Notice.

The Order to Take Notice and proposed regulations were published in the *Virginia Register of Regulations* on September 14, 2020, posted on the Commission's website, and sent to all to all insurers, burial societies, fraternal benefit societies, health services plans, risk retention

[1] *See* § 38.2-627 D of the IDSA.

groups, joint underwriting associations, group self-insurance pools, and group self-insurance associations licensed by the Commission, qualified reinsurers in Virginia (collectively, potential "Licensees"), the Virginia Attorney General's Division of Consumer Counsel ("Consumer Counsel") and to all interested persons. Licensees, Consumer Counsel and other interested parties were afforded the opportunity to file written comments or request a hearing on or before October 26, 2020.

Comments to the Rules were filed by Wesley Bissett, Independent Agents and Brokers of America ("IIABA"); Robert Bradshaw, on behalf of Independent Insurance Agents of Virginia, as well as on behalf of Christine E. Miller,, Kevin Kowar, Professional Insurance Agents of Virginia/DC, Kathie Naylor, Virginia Association of Health Underwriters; Nancy Egan, American Property Casualty Insurance Association; Marc Follmer, Virginia Farm Bureau Mutual Insurance Company ("VFB"); Michelle Caroll Foster, American Council of Life Insurers; Leigh Hubbard, Virginia Land Title Association; Andrew Kirkner, National Association of Mutual Insurance Companies; and John Morris, UnitedHealthcare ("UHC").[2]

The Bureau considered the comments filed and responded to them in its Response to Comments ("Response"),[3] which the Bureau filed with the Clerk of the Commission on April 5, 2021. In its Response, the Bureau addressed the comments and either recommended that various sections of the proposed Rules be amended or indicated why it did not believe other suggested revisions were authorized or warranted.

[2] Comments submitted by NAIMIC, IIABA and UHC were filed on October 27, 2020, after the deadline imposed by the Order to Take Notice. However, as the Bureau indicated it considered and responded to all comments received, the Commission has considered all comments filed as well.

[3] The only commenter requesting a hearing, withdrew the request based upon the Bureau's proposed modifications to the Rules as outlined in the Response.

NOW THE COMMISSION, having considered the proposed regulations, the comments filed, the Bureau's Statement of Position, the record herein, and applicable law, concludes that the proposed regulations should be adopted by the Commission, as recommended and modified and attached hereto. The Commission further concludes that the proposed regulations, as modified, should be adopted with an effective date of June 1, 2021.

Accordingly, IT IS ORDERED THAT:

(1) The proposed regulations, as modified herein and attached hereto, are adopted effective June 1, 2021.

(2) This Order and the attached regulations shall be made available on the Commission's website: scc.virginia.gov/pages/Case-Information.

(3) The Commission's Division of Information Resources shall provide a copy of this Order and the regulations to the Virginia Registrar of Regulations for publication in the *Virginia Register of Regulations*.

(4) This case is dismissed, and the papers filed herein shall be placed in the Commission's file for ended causes.

A COPY of this Order and the attached regulations shall be sent by the Clerk of the Commission to the Commission's Office of General Counsel, to the Attorney General's Division of Consumer Counsel and to the Commissioner of the Bureau of Insurance, who shall email an electronic link to this Order and attached regulations 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, qualified reinsurers in Virginia and such other interested persons as he may designate.

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.

The following word and terms when used in this chapter shall have the following meanings, unless context clearly indicates otherwise:

"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.

"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" or "encryption" 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;

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.

["Nonpublic information" does not include a consumer's personally identifiable information that has been anonymized using a method no less secure than the safe harbor method under HIPAA.

"Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from federal, state, or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state, or local law. A licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine (i) that the information is of the type that is available to the general public and (ii) whether a consumer can direct that the information not be made available to the general public and, if so, that such consumer has not done so.]

"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. [~~In addition to the information security program requirements of § 38.2-623 of the Code of Virginia, 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.~~

~~1. Each level one licensee shall consider cybersecurity risks in its enterprise risk management process.~~

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

~~B.~~] In addition to the information security program requirements of § 38.2-623 of the Code of Virginia, 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~~ processes] :

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 [including the security of information systems and nonpublic information that are accessible to, or held by third-party service providers] ;

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 [and management] ; 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.

[B. An assessment conducted in accordance with the objectives of the most current revision of NIST SP 800-30, NIST SP 800-39, or other substantially similar standard, shall meet the requirements for a periodic assessment in subsection A of this section.

C.] 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. [~~As part of its information security program and 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. Compliance with the provisions of this subsection is required for all level one licensees on or before (insert date one year from the effective date of this chapter).~~

~~B.~~] As part of its information security program and 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~~ which may include] multi-factor authentication, for authorized [~~individuals~~ persons] 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.

[B.] Compliance with the provisions of this [~~subsection~~ section] is required of all [~~level two~~] licensees on or before July 1, 2022.

C. [Security measures implemented in accordance with the objectives of the most current revision of NIST SP 800-30, NIST SP 800-39, or other substantially similar standard, shall meet the requirements for security measures in subsection A of this section.

D.] 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. Reporting cybersecurity events to the commissioner.

1. Once a licensee has determined [both] that a cybersecurity event has occurred and [that] the licensee has a duty to report it to the commissioner pursuant to § 38.2-625 of the Code of Virginia, 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 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 of Virginia 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~~ as much of] the information set forth in § 38.2-625 of the Code of Virginia [as possible] .

4. If also required to notify consumers [~~under § 38.2-626 of the Code of Virginia and 14VAC5-430-70~~] , licensees shall (i) provide the commissioner with a copy of the notice template and any documentation provided to consumers and (ii) maintain a list of consumers notified and retain the list for [~~the longer of five years or~~] the timeframe established by § 38.2-624 D of the Code of Virginia.

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 [insurance] company may report [~~all~~ any] remaining information required by § 38.2-625 of the Code of Virginia [discovered by the licensee pursuant to its investigation] (i) annually in a separate report, (ii) in the certification described in § 38.2-623 H of the Code of Virginia, or (iii) on a continuing basis through the portal established for [~~the company~~ reporting cybersecurity events ~~by~~ to] the bureau [~~for this purpose~~].

C. Unless exempted by § 38.2-629 A 2 of the Code of Virginia, 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, nondomestic insurance companies, and, unless exempted under § 38.2-629 A 2 of the Code of Virginia, 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 of Virginia as set forth in subsection A of this section.

14VAC5-430-70. Consumer notification provisions.

A. Licensees, except those exempted under [subsections A 1 or A 2 of] § 38.2-629 [~~A-2~~] of the Code of Virginia, 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 of Virginia, 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 [, without unreasonable delay,] of its position and provide [~~a detailed~~ an] 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 of Virginia.~~

]

Documents Incorporated by Reference (14VAC5-430)

DOCUMENTS INCORPORATED BY REFERENCE (14VAC5-430)

National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory, 100 Bureau Drive (Mail Stop 8930), Gaithersburg, MD 20899-8930, sec-cert@nist.gov

NIST, Special Publication, Guide for Conducting Risk Assessments, 800-30 (rev. 1, 9/2012)

NIST, Special Publication, Managing Information Security Risk Organization, Mission, and Information System View, 800-39 (eff. 3/2011)

~~[NIST, Special Publication, Security and Privacy Controls for Federal Information Systems and Organizations, 800-53 (rev. 4, 4/2013)~~

~~NIST, Special Publication, Protecting Controlled Unclassified Information, 800-171 (rev. 2, 2/2020)]~~