Vermont markup to ACLI Comments 1/21/2022

Section 4728. INSURANCE DATA SECURITY

(a) Title. This section shall be known and may be cited as the "Vermont Insurance Data Security Law."

(b) Construction.

(1) Notwithstanding any other provision of law, t~~T~~his section establishes the exclusive state standards applicable to licensees for data security and for the investigation of a cybersecurity event ~~applicable to licensees~~.

(2) This section shall not be construed to change any aspect of the Security Breach Notice Act, 9 V.S.A. Section 2435.

(3) This section may not be construed to create or imply a private cause of action for violation of its provisions, nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this section.

(4) A licensee in compliance with N.Y. Comp. Codes R. & Regs. Title 23, section 500, Cybersecurity Requirements for Financial Services Companies, effective March 1, 2017, shall be considered to meet the requirements of this section, provided that the licensee submits a written statement to the Commissioner certifying such compliance.

(c) Definitions. As used in this section:

(1) "Authorized person" means a person known to and screened 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.

(2) "Consumer" means an individual, including but not limited to an applicant, policyholder, insured, beneficiary, claimant, or certificate holder, who is a resident of this State and whose nonpublic information is in a licensee's possession, custody, or control.

(3) "Cybersecurity event" means an event resulting in unauthorized access to or disruption or misuse of~~:~~

~~(A)~~ an information system~~;~~ or

~~(B)~~ nonpublic information stored on such information system~~in the possession, custody, or control of a licensee or authorized person~~.

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

The term “cybersecurity event” also does not include an event with regard to 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.

(4) "Encrypted" means the transformation of data into a form which results in a low probability of assigning meaning the use of a protective process or key.

(5) "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.

(6) "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 an industrial/process controls system, telephone switching and private branch exchange system, or environmental control system.

Commented [KEG1]: DFR doesn't support this addition

(7) "Licensee" means a person licensed, authorized to operate, or registered or required to be licensed, authorized, or registered pursuant to the insurance laws of this State, but shall not include:

(A) a captive insurance company;

(B) a purchasing group or risk retention group chartered; or

(C) a licensee domiciled in a jurisdiction other than this State or a person that is acting as an assuming insurer for a licensee domiciled in this State.

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

(A) a knowledge factor, such as a password;

(B) a possession factor, such as a token or text message on a mobile phone; or

(C) an inherence factor, such as a biometric characteristic.

(9) "Nonpublic information" means information that is not publicly available information and is:

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

Commented [KEG3]: DFR doesn't support deletion of this language

(B) information concerning a consumer that, because of name, number, personal mark, or other identifier, can be used to identify such consumer, in combination with any one or more of the following data elements:

(i) Social Security number;

(ii) driver's license number or nondriver identification card number;

(iii) individual taxpayer identification number;

(iv) passport number;

(v) military identification card number;

(vii) financial account number or credit or debit card number;

(viii) security code, access code, or password that would permit access to a consumer's financial account; or

(ix) biometric record;

(B) 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 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.

(xx) “Person” means any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association.

(10)(A) "Publicly available information" means 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.

(B) As used in this subdivision, 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 the consumer has not done so.

(11) "Risk assessment" means the risk assessment that each licensee is required to conduct under subdivision (d)(3) of this section.

(12) "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 is otherwise permitted access to nonpublic information through its provision of services to the licensee.

(d) Information Security Program.

(1) Commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control, each licensee shall develop, implement, and maintain a comprehensive written information security program that is based on the licensee's risk assessment and contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system.

(2) A licensee's information security program shall be designed to:

(A) protect the security and confidentiality of nonpublic information and the security of the information system;

(B) protect against any threats or hazards to the security or integrity of nonpublic information and the information system;

(C) protect against unauthorized access to or use of nonpublic information and minimize the likelihood of harm to any consumer; and

(D) define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction when no longer needed.

(3) The licensee shall:

(A) designate one or more employees, an affiliate, or an outside vendor designated to act on behalf of the licensee to be responsible for the information security program;

(B) identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration, or destruction of nonpublic information, including the security of information systems and nonpublic information that are accessible to or held by third-party service providers;

(C) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the nonpublic information;

(D) 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, including:

(i) employee training and management;

(ii) information systems, including network and software design, as well as information classification, governance, processing, storage, transmission, and disposal; and

(iii) detecting, preventing, and responding to attacks, intrusions, or other systems failures; and

(E) implement information safeguards to manage the threats identified in its ongoing assessment and, no less than annually, assess the effectiveness of the safeguards' key controls, systems, and procedures.

(4) Based on its risk assessment, the licensee shall:

(A) Design its information security program to mitigate the identified risks, commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control.

(B) Determine which security measures listed below are appropriate and implement such security measures:

(i) place access controls on information systems, including controls to authenticate and permit access only to authorized persons to protect against the unauthorized acquisition of nonpublic information;

(ii) identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy;

(iii) restrict physical access to nonpublic information to authorized persons only;

(iv) protect by encryption or other appropriate means all nonpublic information while being transmitted over an external network and all nonpublic information stored on a laptop computer or other portable computing or storage device or media;

(v) adopt secure development practices for in-house developed applications utilized by the licensee and procedures for evaluating, assessing, or testing the security of externally developed applications utilized by the licensee;

Commented [KEG5]: DFR doesn't support deletion of this language

(vi) modify the information system in accordance with the licensee's information security program;

(vii) utilize effective controls, which may include multi-factor authentication procedures, for any individual accessing nonpublic information;

(viii) regularly test and monitor systems and procedures to detect actual and attempted attacks on or intrusions into information systems;

(ix) include audit trails within the information security program designed to detect and respond to cybersecurity events and reconstruct material financial transactions sufficient to support normal operations and obligations of the licensee;

(x) implement measures to protect against destruction, loss, or damage of nonpublic information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures; and

(xi) develop, implement, and maintain procedures for the secure disposal of nonpublic information in any format.

(C) Include cybersecurity risks in the licensee's enterprise risk management process.

(D) Stay informed regarding emerging threats and vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared.

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

(5)(A) If the licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum:

(i) require the licensee's executive management or its delegates to develop, implement, and maintain the licensee's information security program;

(ii) require the licensee's executive management or its delegates to report in writing at least annually the following information:

(I) the overall status of the information security program and the licensee's compliance with this section; and

(II) material matters related to the information security program, addressing issues such as risk assessment; risk management and control decisions; third-party service provider arrangements; results of testing, cybersecurity events, or violations and management's responses thereto; and recommendations for changes in the information security program.

(B) If executive management delegates any of its responsibilities under subsection (d) of this section, it shall oversee the development, implementation, and maintenance of the licensee's information security program prepared by the delegate or delegates and shall receive a report from the delegate or delegates complying with the requirements of the report to the board of directors.

(6) (A) A licensee shall exercise due diligence in selecting its third-party service provider.

(B) A licensee shall require a 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.

(7) A licensee shall monitor, evaluate, and adjust, as appropriate, the information security program consistent with any relevant changes in technology, the sensitivity of its nonpublic information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

(8) (A) As part of its information security program, a licensee shall establish a written incident response plan designed to promptly respond to and recover from any cybersecurity event that compromises the confidentiality, integrity, or availability of nonpublic information in its possession; the licensee's information systems; or the continuing functionality of any aspect of the licensee's business or operations.

(B) The incident response plan shall address the following areas:

(i) the internal process for responding to a cybersecurity event;

(ii) the goals of the incident response plan;

(iii) the definition of clear roles, responsibilities, and levels of decision-making authority;

(iv) external and internal communications and information sharing;

(v) identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

(vi) documentation and reporting regarding cybersecurity events and related incident response activities; and

(vii) the evaluation and revision as necessary of the incident response plan following a cybersecurity event.

(9) Annually, each insurer domiciled in this State shall submit to the Commissioner a written statement on or before April 15, certifying that the insurer is compliant with the requirements established in subsection (d) of this section. Each insurer shall maintain for examination by the Commissioner all records, schedules, and data supporting this certificate for a period of five years. To the extent an insurer has identified areas, systems, or processes that require material improvement, updating, or redesign, the insurer shall document the identification and the remedial efforts planned and underway to address such areas, systems, or processes. Such documentation shall be available for inspection by the Commissioner.

(e) Investigation of a Cybersecurity Event.

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

(2) During the investigation, the licensee or an outside vendor or service provider, or both, designated to act on behalf of the licensee shall, at a minimum, make the best effort to:

Commented [KEG7]: DFR suggests this language as an alternative to ACLI's language

(A) determine whether a cybersecurity event has occurred;

(B) assess the nature and scope of the cybersecurity event;

(C) identify any nonpublic information that may have been involved in the cybersecurity event; and

(D) perform or oversee reasonable measures to restore the security of the information systems compromised in the cybersecurity event in order to prevent further unauthorized acquisition, release, or use of nonpublic information in the licensee's possession, custody, or control.

(f) Power of Commissioner.

(1) The Commissioner shall have power to examine and investigate into the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of this section. This power is in addition to the powers the Commissioner has under section 4726 of this title and 9 V.S.A. Section 2435(h)(2). Any such investigation or examination shall be conducted pursuant to section 4726 of this title.

(2) Whenever the Commissioner has reason to believe that a licensee has been or is engaged in conduct in this State that violates this section, the Commissioner may take action that is necessary or appropriate to enforce the provisions of this section.

(g) Confidentiality.

(1) Any documents, materials or other information in the control or possession of the Commissioner that are furnished by a licensee or an employee or agent thereof acting on behalf of the licensee pursuant to subdivision (d)(8) of this section, or that are obtained by the Commissioner in an investigation or examination pursuant to subsection (f) of this section, shall be confidential by law and privileged, shall not be subject to 1 V.S.A. Sections 315–320, shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action. However, the Commissioner is authorized to use the documents, materials, or other information in the furtherance of any regulatory or legal action brought as a part of the Commissioner's duties.

(2) Neither the Commissioner nor any person who received documents, materials, or other information while acting under the authority of the Commissioner shall be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to subdivision (g)(1) of this section.

(3) To assist in the performance of the Commissioner's duties under this section, the Commissioner may:

(A) share documents, materials, or other information, including confidential and privileged documents, materials, or information subject to subdivision (g)(1) of this section, with other state, federal, and international regulatory agencies, the National Association of Insurance Commissioners, its affiliates or subsidiaries, and state, federal, and international law enforcement authorities, provided that the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information shared;

(B) receive documents, materials, or information, including otherwise confidential and privileged documents, materials, or information, from the National Association of Insurance Commissioners, its affiliates or subsidiaries, and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and shall maintain as confidential or privileged any document, material, or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material, or information;

(C) share documents, materials, or other information subject to subdivision (g)(1) of this section with a third-party consultant or vendor, provided that the consultant agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information shared; and

(D) enter into agreements governing the sharing and use of information consistent with this subsection.

(4) No waiver of any applicable privilege or claim of confidentiality in any document, material, or information shall occur as a result of its disclosure to the Commissioner under this section or as a result of sharing as authorized in subdivision (g)(3) of this section.

(5) Nothing in this section shall prohibit the Commissioner from releasing final adjudicated actions that are open to public inspection pursuant to 1 V.S.A. Sections 315–320 to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners or its affiliates or subsidiaries.

(h) Exceptions.

(1) The following exceptions apply to this section:

(A) A licensee with fewer than 20 employees, including any independent contractors, is exempt from subsection (d) of this section.

(B) A licensee that is in possession of protected health information subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub.L. 104–191, 110 Stat. 1936, that has established and maintains an information security program pursuant to such statutes and the rules, regulations, procedures, or guidelines established thereunder, is considered to meet the requirements of subsection (d) of this section, provided that the licensee is compliant with, and annually submits a written statement to, the Commissioner certifying its compliance with such program. As used in this section, the definition of "protected health information" is as set forth in HIPAA and the regulations promulgated thereunder and shall be considered to be a subset of nonpublic information.

(C) An employee, agent, representative, or designee of a licensee, who is also a licensee, is exempt from subsection (d) of this section and need not develop its own information security program to the extent that the employee, agent, representative, or designee is covered by the information security program of the other licensee.

(D) A licensee that is affiliated with a financial institution, as defined in subdivision 11101(32) of this title, or a credit union, as defined in subdivision 30101(5) of this title, that has established and maintains an information security program in compliance with the interagency guidelines establishing standards for safeguarding customer information as set forth in section 501(b) of the Gramm-Leach-Bliley Act, 15 U.S.C. section 6801 et seq., is considered to meet the requirements of subsection (d) of this section, provided that the licensee produces, upon request, documentation satisfactory to the Commissioner that independently validates the affiliated financial institution's or credit union's adoption of an information security program that satisfies the interagency guidelines.

(2) In the event that a licensee ceases to qualify for an exception, such licensee shall have 180 days to comply with this section.

(i) Penalties. In the case of a violation of this section, a licensee may be penalized in accordance with section 3661 or 4726 of this title, as appropriate.

(j) Effective date. This section shall take effect on January 1, 2023. A licensee shall have one year from the effective date of this section to implement subsection (d) of this section, other than subdivision (d)(6) of this section. A licensee shall have two years from the effective date of this section to implement subdivision (d)(6) of this section.