WEST VIRGINIA LEGISLATURE

2024 REGULAR SESSION

Committee Substitute

for

House Bill 5338

By Delegates Linville, Cannon, Young, W.

Clark, Butler, Ward, Hillenbrand, Brooks,

Adkins, Hanshaw (Mr. Speaker), and Chiarelli

[Originating in the Committee on Finance;

Reported on February 23, 2024]

A BILL to amend the Code of West Virginia, 1931, as amended, by adding thereto a new article, designated §31A-8H-1, §31A-8H-2, §31A-8H-3, §31A-8H-4, and §31A-8H-5, all relating to providing an affirmative legal defense to certain types of businesses against certain types of lawsuits claiming that the business failed to implement reasonable cybersecurity protections and that as a result, a data breach of personal information or restricted information occurred if the business creates, maintains, and complies with a written cybersecurity program that contains administrative, technical, operational, and physical safeguards for the protection of personal information as set forth in this act; describing the requirements of the cybersecurity program; construction of article; and providing immunity in certain circumstances to certain institutions of higher education in this state that offer a cybersecurity assessment program as part of an undergraduate or graduate program relating to cybersecurity to any business in the state.

Be it enacted by the Legislature of West Virginia:

ARTICLE 8H. SAFE HARBOR FOR CYBERSECURITY PROGRAMS.

§31A-8H-1. Definitions.

As used in this article:

(1) "Business" means any limited liability company, limited liability partnership, corporation, sole proprietorship, association, or other group, however organized and whether operating for profit or not for profit, including a financial institution or bank holding company organized, chartered, or holding a license authorizing operation under the laws of this state, any other state, the United States, or any other country, or the parent or subsidiary of any of the foregoing.

"Business" does not include any body, authority, board, bureau, commission, district, or agency of the state or of any political subdivision of the state.

(2) "Contract" means the total legal obligation resulting from the parties' agreement as affected by this article and other applicable law.

(3) "Covered entity" means a business that accesses, maintains, communicates, or processes personal information or restricted information in or through one or more systems, networks, or services located in or outside this state.

(4) "Data breach" means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information or restricted information owned by or licensed to a covered entity and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to person or property. "Data breach" does not include either of the following:

(A) Good faith acquisition of personal information or restricted information by the covered entity's employee or agent for the purposes of the covered entity provided that the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure;

(B) Acquisition of personal information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory state agency.

(5) "Distributed ledger technology" means an electronic ledger or other record of transactions or other data to which all of the following apply:

(A) The electronic ledger is uniformly ordered.

(B) The electronic ledger is redundantly maintained or processed by more than one computer or machine to guarantee the consistency or nonrepudiation of the recorded transactions or other data.

(6) "Electronic record" means a record created, generated, sent, communicated, received, or stored by electronic means.

(7) "Encryption" means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

(8) "Individual" means a natural person.

(9)(A) "Personal information" means any information relating to an individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, social security number, driver's license number or state identification card number, passport number, account number, or credit or debit card number, precise location data, biometric data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that individual.

(B) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or any of the following media that are widely distributed:

(i) Any news, editorial, or advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio, television, or the internet.

(ii) Any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to news media identified in this paragraph.

(iii) Any publication designed for and distributed to members of any bona fide association or charitable or fraternal nonprofit business.

(iv) Any type of media similar in nature to any item, entity, or activity identified in this paragraph.

(10) "Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

(11) "Redacted" means altered or truncated so that no more than the last four digits of a social security number, driver's license number, state identification card number,

passport number, account number, or credit or debit card number is accessible as part of the data.

(12) "Smart contract" means an electronic record that is an event-driven program or computerized transaction protocol that runs on a distributed, decentralized, shared, and replicated ledger that executes the term of a contract, including but not limited to, taking custody over and instructing the transfer of assets.

(13) "Transaction" means a sale, trade, exchange, transfer, payment, or conversion of virtual currency or other digital asset or any other property or any other action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

§31A-8H-2. Affirmative defenses.

(a) A covered entity seeking an affirmative defense under this chapter shall create, maintain, and comply with a written cybersecurity program that contains administrative, technical, operational, and physical safeguards for the protection of personal information.

(b) A covered entity's cybersecurity program shall include:

(1) An evaluation of and a description of mitigation efforts for any reasonably anticipated internal or external threats or hazards that could lead to a data breach.

(2) A process for communicating to affected parties in the event of a known material data breach.

(c) The scale and scope of a covered entity's cybersecurity program shall be tailored to the nature, complexity, and size of the business, including the industry in which they operate and the risks posed to it.

(d) A covered entity that satisfies all requirements of this section is entitled to an affirmative defense to any cause of action sounding in tort that is brought under the laws of this state or in the courts of this state and that alleges that the failure to implement

reasonable information security controls resulted in a data breach concerning personal information or restricted information.

(e) A covered entity satisfies all requirements of this section if its cybersecurity program reasonably conforms to an industry-recognized cybersecurity framework, as described in §31A-8H-3 of this code.

§31A-8H-3. Cybersecurity program framework.

(a) A covered entity's cybersecurity program, as described in section §31A-8H-2 of this code, reasonably conforms to an industry-recognized cybersecurity framework for purposes of this article if any of the following are true:

(1)(A) The cybersecurity program reasonably conforms to the current version of any of the following or any combination of the following, subject to paragraph (B) of this subdivision and subsection (b) of this section:

(i) The framework for improving critical infrastructure cybersecurity developed by the national institute of standards and technology.

(ii) National institute of standards and technology special publication 800-171.

(iii) National institute of standards and technology special publications 800-53 and 800-53a.

(iv) National institute of standards and technology special publication 800-76-1.

(v) The federal risk and authorization management program security assessment framework.

(vi) The center for internet security critical security controls for effective cyber defense.

(vii) The international organization for standardization/international electrotechnical commission 27000 family — information security management systems.

(viii) The Cybersecurity Maturity Model Certification at a minimum of Level 2 with external certification.

(B) When a final revision to a framework listed in paragraph (A) is published, a covered entity whose cybersecurity program reasonably conforms to that framework shall reasonably conform the elements of its cybersecurity program to the revised framework within the time frame provided in the relevant framework upon which the covered entity intends to rely to support its affirmative defense, but in no event later than one year after the publication date stated in the revision.

(2)(A) The covered entity is regulated by the state, by the federal government, or both, or is otherwise subject to the requirements of any of the laws or regulations listed below, and the cybersecurity program reasonably conforms to the entirety of the current version of any of the following, subject to paragraph (B) of this subdivision:

(i) The security requirements of the federal Health Insurance Portability and Accountability Act of 1996, as set forth in 45 C.F.R. pt. 164, subpt. C.

(ii) Title V of the federal Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, as amended.

(iii) The federal Information Security Modernization Act of 2014, Pub. L. No. 113-283.

(iv) The federal Health Information Technology for Economic and Clinical Health Act as set forth in 45 C.F.R. pt. 162.

(v) Any applicable rules, regulations, or guidelines for critical infrastructure protection adopted by the federal environmental protection agency, the federal cybersecurity and infrastructure security agency, or the north American reliability corporation.

(B) When a framework listed in paragraph (A) of this subdivision is amended, a covered entity whose cybersecurity program reasonably conforms to that framework shall reasonably conform the elements of its cybersecurity program to the amended framework within the time frame provided in the relevant framework upon which the covered entity

intends to rely to support its affirmative defense, but in no event later than one year after the effective date of the amended framework.

(3)(A) The cybersecurity program reasonably complies with both the current version of the payment card industry data security standard and conforms to the current version of another applicable industry-recognized cybersecurity framework listed in subdivision (a)(1) of this section, subject to paragraph (B) of this subdivision and subsection (b) of this section.

(B) When a final revision to the payment card industry data security standard is published, a covered entity whose cybersecurity program reasonably complies with that standard shall reasonably comply the elements of its cybersecurity program with the revised standard within the time frame provided in the relevant framework upon which the covered entity intends to rely to support its affirmative defense, but not later than the effective date for compliance.

(b) If a covered entity's cybersecurity program reasonably conforms to a combination of industry-recognized cybersecurity frameworks and two or more of those frameworks are revised, the covered entity whose cybersecurity program reasonably conforms to or complies with, as applicable, those frameworks shall reasonably conform the elements of its cybersecurity program to or comply with, as applicable, all of the revised frameworks within the time frames provided in the relevant frameworks but in no event later than one year after the latest publication date stated in the revisions.

§31A-8H-4. Limitation on private right of action.

This article shall not be construed to provide a private right of action, including a class action, with respect to any act or practice regulated therein.

§31A-8H-5. Security assessments; limitation on liability.

(a) Any institution of higher education in this state may offer a cybersecurity assessment program as part of an undergraduate or graduate program relating to cybersecurity to any business in the state.

(b) An institution of higher education in this state, or any employee or student thereof, offering a cybersecurity assessment program shall be immune from civil liability that arises from the failure of a covered entity to conform to the provisions of this article.