HB4081

LRB10332146BMS61211b

103RD GENERAL ASSEMBLY

State of Illinois

2023 and 2024

HB4081

Introduced 5/10/2023, by Rep. Brad Stephens

SYNOPSIS AS INTRODUCED:

New Act

Creates the Cybersecurity Compliance Act. Creates an affirmative defense for every covered entity that creates, maintains, and complies with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of either personal information or both personal information and restricted information and that reasonably conforms to an industry-recognized cybersecurity framework. Prescribes requirements for the cybersecurity program.

LRB103 32146 BMS 61211 b

A BILL FOR

AN ACT concerning business.

Be it enacted by the People of the State of Illinois, represented in the General Assembly:

Section 1. Short title. This Act may be cited as the Cybersecurity Compliance Act.

Section 5. Definitions. As used in this Act:

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

"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 of this State.

"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:

(1) the good faith acquisition of personal information or restricted information by the covered entity's employee or agent for the purposes of the covered entity so long as the personal information or restricted information is not used for an unlawful purpose or subject to further unauthorized disclosure; or

(2) the acquisition of personal information or restricted information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory State agency.

"Personal information" has the same meaning as provided in the Personal Information Protection Act.

"Restricted information" means any information about an individual, other than personal information, that, alone or in combination with other information, including personal information, can be used to distinguish or trace the individual's identity or that is linked or linkable to an individual, if the information is not encrypted, redacted, or altered by any method or technology in such a manner that the information is unreadable, and the breach of which is likely to result in a material risk of identity theft or other fraud to a person or property.

Section 10. Safe harbor requirements.

(a) A covered entity seeking an affirmative defense under this Act shall:

(1) create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information and that reasonably conforms to an industry-recognized cybersecurity framework, as described in Section 15; or

(2) create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of both personal information and restricted information and that reasonably conforms to an industry-recognized cybersecurity framework, as described in Section 15.

(b) A covered entity's cybersecurity program shall be designed to do all of the following:

(1) protect the security and confidentiality of information;

(2) protect against any anticipated threats or hazards to the security or integrity of information; and

(3) protect against unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.

(c) The scale and scope of a covered entity's cybersecurity program under subsection (a), as applicable, is appropriate if it is based on all of the following factors:

(1) the size and complexity of the covered entity;

(2) the nature and scope of the activities of the covered entity;

(3) the sensitivity of the information to be protected;

(4) the cost and availability of tools to improve information security and reduce vulnerabilities; and

(5) the resources available to the covered entity.

(d) A covered entity under this Section is entitled to an affirmative defense as follows:

(1) A covered entity that satisfies paragraph (1) of subsection (a) and also subsections (b) and (c) 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.

(2) A covered entity that satisfies paragraph (2) of subsection (a) and also subsections (b) and (c) 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.

Section 15. Reasonable conformance.

(a) A covered entity's cybersecurity program reasonably conforms to an industry-recognized cybersecurity framework for purposes of this Act if the requirements of subsection (b), (c), or (d) are satisfied.

(b)(1) The cybersecurity program reasonably conforms to an industry-recognized cybersecurity framework for purposes of this Act if the cybersecurity program reasonably conforms to the current version of any of the following or any combination of the following, subject to paragraph (2) and subsection (e):

(A) The "framework for improving critical infrastructure cyber security" developed by the National Institute of Standards and Technology (NIST);

(B) NIST special publication 800-171;

(C) NIST special publications 800-53 and 800-53a;

(D) The Federal Risk And Authorization Management Program (FedRAMP) Security Assessment Framework;

(E) The Center for Internet Security Critical Security Controls for Effective Cyber Defense; or

(F) The International Organization for Standardization/International Electrotechnical Commission 27000 Family - Information Security Management Systems.

(2) When a final revision to a framework listed in paragraph (1) is published, a covered entity whose cybersecurity program reasonably conforms to that framework shall reasonably conform to the revised framework not later than one year after the publication date stated in the revision.

(c)(1) The covered entity's cybersecurity program reasonably conforms to an industry-recognized cybersecurity framework for purposes of this Act if 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 (2):

(A) The security requirements of the Health Insurance Portability and Accountability Act of 1996, as set forth in 45 CFR Part 164, Subpart C;

(B) Title V of the Gramm-Leach-Bliley Act of 1999, Public Law 106-102, as amended;

(C) The Federal Information Security Modernization Act of 2014, Public Law 113-283;

(D) The Health Information Technology for Economic and Clinical Health Act, as set forth in 45 CFR Part 162.

(2) When a framework listed in paragraph (1) is amended, a covered entity whose cybersecurity program reasonably conforms to that framework shall reasonably conform to the amended

framework not later than one year after the effective date of the amended framework.

(d)(1) The cybersecurity program reasonably conforms to an industry-recognized cybersecurity framework for purposes of this Act if the cybersecurity program reasonably complies with both the current version of the payment card industry (PCI) data security standard and conforms to the current version of another applicable industry-recognized cybersecurity framework listed in subsection (b), subject to paragraph (2) of subsection (b) and subsection (e).

(2) When a final revision to the PCI data security standard is published, a covered entity whose cybersecurity program reasonably complies with that standard shall reasonably comply with the revised standard not later than one year after the publication date stated in the revision.

(e) If a covered entity's cybersecurity program reasonably conforms to a combination of industry-recognized cybersecurity frameworks, or complies with a standard, as in the case of the PCI data security standard, as described in subsection (b) or (d), and 2 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 to or comply with, as applicable, all of the revised frameworks not later than one year after the latest publication date stated in the revisions.

Section 20. No private right of action. This Act shall not be construed to provide a private right of action, including a class action, with respect to any act or practice regulated under it.

Section 97. Severability. The provisions of this Act are severable under Section 1.31 of the Statute on Statutes.