As Introduced

132nd General Assembly
Regular Session
2017-2018

S. B. No. 220

Senators Hackett, Bacon

A BILL

To enact sections 1354.01, 1354.02, 1354.03, 1354.04, and 1354.05 of the Revised Code to provide a legal safe harbor to covered entities that implement a specified cybersecurity program.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF OHIO:

Section 1. That sections 1354.01, 1354.02, 1354.03, 1354.04, and 1354.05 of the Revised Code be enacted to read as follows:

Sec. 1354.01. As used in this chapter:

(A) "Business" means any limited liability company, limited liability partnership, corporation, sole proprietorship, or nonprofit corporation or unincorporated nonprofit association that operates in Ohio.

(B) "Covered entity" means a business that accesses, maintains, communicates, or handles personal information.

(C) "Data breach" has the same meaning as "breach of the security of the system" in section 1349.19 of the Revised Code.

(D) "Individual" means a natural person.

(E) "NIST cybersecurity framework" means the framework for improving critical infrastructure cybersecurity developed by the national institute of standards and technology, as updated from time to time.

(F) "Person" means an individual, corporation, business trust, estate, trust, partnership, association, or other legal entity that conducts business in this state.

(G) "Personal information" has the same meaning as in section 1349.19 of the Revised Code.

Sec. 1354.02. (A) Each covered entity seeking a safe harbor under sections 1354.01 to 1354.05 of the Revised Code shall create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information that complies with the NIST cybersecurity framework or other industry cybersecurity framework as described in section 1354.03 of the Revised Code.

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

(1) Protect the security and confidentiality of personal information;

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

(3) Protect against unauthorized access to and acquisition of personal 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 division (A) of this section shall be 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 personal information to be protected;

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

(5) The resources available to the covered entity.

(D) A covered entity that implements and maintains a cybersecurity program that complies with the NIST cybersecurity framework, or other industry cybersecurity framework as described in section 1354.03 of the Revised Code, shall be deemed to be in compliance with this section. Compliance with this section shall constitute an affirmative defense to any cause of action sounding in tort that alleges the failure to implement reasonable information security controls resulted in a data breach. Following any update to the NIST cybersecurity framework, or other industry recognized data security framework, the covered entity shall have a period of one year from the stated effective date as prescribed in the framework to comply with the update. If a covered entity complies with the update within one year of the stated effective date found in the framework as updated, the entity shall still be deemed to be in compliance with this section.

Sec. 1354.03. A covered entity shall be deemed to be in compliance with section 1354.02 of the Revised Code if either of the following apply:

(A) The covered entity is in substantial compliance with any of the following:

(1) NIST special publication 800-171;

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

(3) The federal risk and authorization management program;

(4) Center for internet security critical security controls;

(5) International organization for standardization/international electrotechnical commission 27000 family - information security management systems.

(B) The covered entity is regulated by the state and the federal government and is in substantial compliance with the entirety of any of the following:

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

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

(3) The "Federal Information Security Modernization Act of 2014," Public Law 113-283.

Sec. 1354.04. Sections 1354.01 to 1354.05 of the Revised Code shall not be construed to provide a private right of action, including a class action, with respect to any act or practice regulated under those sections.

Sec. 1354.05. If any provision of sections 1354.01 to 1354.05 of the Revised Code or the application thereof to a covered entity is for any reason held to be invalid, the

remainder of the provisions under those sections and the application of such provisions to other covered entities shall not be thereby affected.

Section 2. (A) The purpose of this act is to establish a legal safe harbor to be pled as an affirmative defense to a cause of action sounding in tort that alleges the failure to implement reasonable information security controls resulted in a data breach. The safe harbor shall apply to all covered entities that implement a cybersecurity program that complies with the Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of Standards and Technology, or other industry recognized data security framework.

(B) This act is intended to be an incentive and to encourage businesses to achieve a higher level of cybersecurity through voluntary action. The bill does not, and is not intended to, create a minimum cybersecurity standard that must be achieved, nor shall it be read to impose liability upon businesses that do not obtain or maintain practices in compliance with the frameworks referenced in this section.