Reviewed As To Form By
Legislative Service Commission

I_132_0943-9

132nd General Assembly
Regular Session
2017-2018

Sub. S. B. No. 220

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, association, or other group, however organized and whether operating for profit or not for profit, including 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, or the parent or subsidiary of any of the foregoing.

(B) "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.

(C) "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:

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

(2) 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.

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

(E) "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 person or property.

As used in this division, "encrypted," "individual," and "redacted" have the same meanings as in section 1349.19 of the Revised Code.

Sec. 1354.02. (A) A covered entity seeking an affirmative defense under sections 1354.01 to 1354.05 of the Revised Code shall do one of the following:

(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 1354.03 of the Revised Code; 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 1354.03 of the Revised Code.

(B) A covered entity's cybersecurity program shall be designed to do all of the following with respect to the information described in division (A)(1) or (2) of this section, as applicable:

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

(2) Protect against any anticipated threats or hazards to

the security or integrity of the information;

(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 division (A)(1) or (2) of this section, 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;

(5) The resources available to the covered entity.

(D)(1) A covered entity that satisfies divisions (A)(1), (B), and (C) 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.

(2) A covered entity that satisfies divisions (A)(2), (B), and (C) 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.

Sec. 1354.03. A covered entity's cybersecurity program, as described in section 1354.02 of the Revised Code, reasonably conforms to an industry recognized cybersecurity framework for purposes of that section if division (A), (B), or (C) of this section is satisfied.

(A)(1) The cybersecurity program reasonably conforms to the current version of any of the following or any combination of the following, subject to divisions (A)(2) and (D) of this section:

(a) The "framework for improving critical infrastructure cybersecurity" 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";

(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 division (A)(1) of this section 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.

(B)(1) 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 division (B)(2) of this section:

(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 division (B)(1) of this section 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.

(C)(1) 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 division (A) of this section, subject to divisions (C)(2) and (D) of this section.

(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.

(D) 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 payment card industry (PCI) data security standard, as described in division (A) or (C) of this section, 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 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.

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 or relates to the failure to implement reasonable information security controls, resulting in a data breach. The safe harbor shall apply to all covered entities that implement a cybersecurity program that

meets the requirements of the act.

(B) This act is intended to be an incentive and to encourage businesses to achieve a higher level of cybersecurity through voluntary action. The act 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 act.