132nd General Assembly

Regular Session   **Sub. S. B. No. 220**

2017-2018

Senators Hackett, Bacon

Cosponsors: Senators Coley, Burke, Dolan, Hoagland

————

A BILL

To enact sections 1354.01, 1354.02, 1354.03,	1
1354.04, and 1354.05 of the Revised Code to	2
provide a legal safe harbor to covered entities	3
that implement a specified cybersecurity	4
program.	5

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

Section 1. That sections 1354.01, 1354.02, 1354.03,	6
1354.04, and 1354.05 of the Revised Code be enacted to read as	7
follows:	8
Sec. 1354.01. As used in this chapter:	9
(A) "Business" means any limited liability company,	10
limited liability partnership, corporation, sole proprietorship,	11
association, or other group, however organized and whether	12
operating for profit or not for profit, including a financial	13
institution organized, chartered, or holding a license	14
authorizing operation under the laws of this state, any other	15
state, the United States, or any other country, or the parent or	16
subsidiary of a financial institution.	17
(B) "Covered entity" means a business that accesses,	18

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. 19 20 21

(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 or licensed by a person 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: 22 23 24 25 26 27 28 29

(1) Good faith acquisition of personal information or restricted information by the person's employee or agent for the purposes of the person, provided that the personal information or restricted information is not used for an unlawful purpose or subject to further unauthorized disclosure; 30 31 32 33 34

(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. 35 36 37 38

(D) "Personal information" has the same meaning as in section 1349.19 of the Revised Code. 39 40

(E) "Restricted information" means any information about an individual, other than personal information, that 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. 41 42 43 44 45 46

As used in this division, "encrypted" and "redacted" have 47

the same meanings as in section 1349.19 of the Revised Code. 48

Sec. 1354.02. (A) A covered entity seeking an affirmative 49
defense under sections 1354.01 to 1354.05 of the Revised Code 50
shall do one of the following: 51

(1) Create, maintain, and comply with a written 52
cybersecurity program that contains administrative, technical, 53
and physical safeguards for the protection of personal 54
information and that reasonably complies with an industry 55
recognized cybersecurity framework, as described in section 56
1354.03 of the Revised Code; 57

(2) Create, maintain, and comply with a written 58
cybersecurity program that contains administrative, technical, 59
and physical safeguards for the protection of both personal 60
information and restricted information and that reasonably 61
complies with an industry recognized cybersecurity framework, as 62
described in section 1354.03 of the Revised Code. 63

(B) A covered entity's cybersecurity program shall be 64
designed to do all of the following with respect to the 65
information described in division (A)(1) or (2) of this section, 66
as applicable: 67

(1) Protect the security and confidentiality of the 68
information; 69

(2) Protect against any anticipated threats or hazards to 70
the security or integrity of the information; 71

(3) Protect against unauthorized access to and acquisition 72
of the information that is likely to result in a material risk 73
of identity theft or other fraud to the individual to whom the 74
information relates. 75

(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 complies with divisions (A)
(1), (B), and (C) of this section is entitled to assert 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 complies with divisions (A)(2),
(B), and (C) of this section is entitled to assert 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
complies with an industry recognized cybersecurity framework for

76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103

purposes of that section if any of the following apply:

104

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

105
106
107
108

(a) The "framework for improving critical infrastructure cybersecurity" developed by the "national institute of standards and technology" (NIST);

109
110
111

(b) "NIST special publication 800-171";

112

(c) "NIST special publications 800-53 and 800-53a";

113

(d) The "federal risk and authorization management program (FedRAMP) security assessment framework";

114
115

(e) The "center for internet security critical security controls for effective cyber defense";

116
117

(f) The "international organization for standardization/international electrotechnical commission 27000 family - information security management systems."

118
119
120

(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 complies with that framework shall reasonably comply with the revised framework not later than one year after the publication date stated in the revision.

121
122
123
124
125
126

(B)(1) The covered entity is regulated by the state, by the federal government, or both, and the cybersecurity program reasonably complies with the entirety of the current version of any of the following, subject to division (B)(2) of this section:

127
128
129
130
131

(a) The security requirements of the "Health Insurance   132
Portability and Accountability Act of 1996," as set forth in 45 133
CFR Part 164 Subpart C;   134

(b) Title V of the "Gramm-Leach-Bliley Act of 1999,"   135
Public Law 106-102, as amended;   136

(c) The "Federal Information Security Modernization Act of   137
2014," Public Law 113-283.   138

(2) When a framework listed in division (B)(1) of this   139
section is amended, a covered entity whose cybersecurity program 140
reasonably complies with that framework shall reasonably comply 141
with the amended framework not later than one year after the   142
effective date of the amended framework.   143

(C)(1) The cybersecurity program reasonably complies with   144
both the current version of the "payment card industry (PCI)   145
data security standard" and the current version of another   146
applicable industry recognized cybersecurity framework listed in 147
division (A) of this section, subject to divisions (C)(2) and   148
(D) of this section.   149

(2) When a final revision to the "PCI data security   150
standard" is published, a covered entity whose cybersecurity   151
program reasonably complies with that standard shall reasonably 152
comply with the revised standard not later than one year after   153
the publication date stated in the revision.   154

(D) If a covered entity's cybersecurity program reasonably   155
complies with a combination of industry recognized cybersecurity 156
frameworks, as described in division (A) or (C) of this section, 157
and two or more of those frameworks are revised, the covered   158
entity whose cybersecurity program reasonably complies with   159
those frameworks shall reasonably comply with all of the revised 160

frameworks not later than one year after the latest publication   161
date stated in the revisions.   162

    Sec. 1354.04. Sections 1354.01 to 1354.05 of the Revised   163
Code shall not be construed to provide a private right of   164
action, including a class action, with respect to any act or   165
practice regulated under those sections.   166

    Sec. 1354.05. If any provision of sections 1354.01 to   167
1354.05 of the Revised Code or the application thereof to a   168
covered entity is for any reason held to be invalid, the   169
remainder of the provisions under those sections and the   170
application of such provisions to other covered entities shall   171
not be thereby affected.   172

    Section 2. (A) The purpose of this act is to establish a   173
legal safe harbor to be pled as an affirmative defense to a   174
cause of action sounding in tort that alleges or relates to the   175
failure to implement reasonable information security controls,   176
resulting in a data breach. The safe harbor shall apply to all   177
covered entities that implement a cybersecurity program that   178
meets the requirements of the act.   179

    (B) This act is intended to be an incentive and to   180
encourage businesses to achieve a higher level of cybersecurity   181
through voluntary action. The act does not, and is not intended   182
to, create a minimum cybersecurity standard that must be   183
achieved, nor shall it be read to impose liability upon   184
businesses that do not obtain or maintain practices in   185
compliance with the act.   186