

As Passed by the Senate

132nd General Assembly

Regular Session

2017-2018

Sub. S. B. No. 220

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 19
restricted information in or through one or more systems, 20
networks, or services located in or outside this state. 21

(C) "Data breach" means unauthorized access to and 22
acquisition of computerized data that compromises the security 23
or confidentiality of personal information or restricted 24
information owned or licensed by a person and that causes, 25
reasonably is believed to have caused, or reasonably is believed 26
will cause a material risk of identity theft or other fraud to 27
person or property. "Data breach" does not include either of the 28
following: 29

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

(2) Acquisition of personal information or restricted 35
information pursuant to a search warrant, subpoena, or other 36
court order, or pursuant to a subpoena, order, or duty of a 37
regulatory state agency. 38

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

(E) "Restricted information" means any information about 41
an individual, other than personal information, that can be used 42
to distinguish or trace the individual's identity or that is 43
linked or linkable to an individual, if the information is not 44
encrypted, redacted, or altered by any method or technology in 45
such a manner that the information is unreadable. 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

<u>(C) The scale and scope of a covered entity's</u>	76
<u>cybersecurity program under division (A) (1) or (2) of this</u>	77
<u>section, as applicable, is appropriate if it is based on all of</u>	78
<u>the following factors:</u>	79
<u>(1) The size and complexity of the covered entity;</u>	80
<u>(2) The nature and scope of the activities of the covered</u>	81
<u>entity;</u>	82
<u>(3) The sensitivity of the information to be protected;</u>	83
<u>(4) The cost and availability of tools to improve</u>	84
<u>information security and reduce vulnerabilities;</u>	85
<u>(5) The resources available to the covered entity.</u>	86
<u>(D) (1) A covered entity that complies with divisions (A)</u>	87
<u>(1), (B), and (C) of this section is entitled to assert an</u>	88
<u>affirmative defense to any cause of action sounding in tort that</u>	89
<u>is brought under the laws of this state or in the courts of this</u>	90
<u>state and that alleges that the failure to implement reasonable</u>	91
<u>information security controls resulted in a data breach</u>	92
<u>concerning personal information.</u>	93
<u>(2) A covered entity that complies with divisions (A) (2),</u>	94
<u>(B), and (C) of this section is entitled to assert an</u>	95
<u>affirmative defense to any cause of action sounding in tort that</u>	96
<u>is brought under the laws of this state or in the courts of this</u>	97
<u>state and that alleges that the failure to implement reasonable</u>	98
<u>information security controls resulted in a data breach</u>	99
<u>concerning personal information or restricted information.</u>	100
<u>Sec. 1354.03. A covered entity's cybersecurity program, as</u>	101
<u>described in section 1354.02 of the Revised Code, reasonably</u>	102
<u>complies with an industry recognized cybersecurity framework for</u>	103

purposes of that section if any of the following apply: 104

(A) (1) The cybersecurity program reasonably complies with 105
the current version of any of the following or any combination 106
of the following, subject to divisions (A) (2) and (D) of this 107
section: 108

(a) The "framework for improving critical infrastructure 109
cybersecurity" developed by the "national institute of standards 110
and technology" (NIST); 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 114
(FedRAMP) security assessment framework"; 115

(e) The "center for internet security critical security 116
controls for effective cyber defense"; 117

(f) The "international organization for 118
standardization/international electrotechnical commission 27000 119
family - information security management systems." 120

(2) When a final revision to a framework listed in 121
division (A) (1) of this section is published, a covered entity 122
whose cybersecurity program reasonably complies with that 123
framework shall reasonably comply with the revised framework not 124
later than one year after the publication date stated in the 125
revision. 126

(B) (1) The covered entity is regulated by the state, by 127
the federal government, or both, and the cybersecurity program 128
reasonably complies with the entirety of the current version of 129
any of the following, subject to division (B) (2) of this 130
section: 131

<u>(a) The security requirements of the "Health Insurance</u>	132
<u>Portability and Accountability Act of 1996," as set forth in 45</u>	133
<u>CFR Part 164 Subpart C;</u>	134
<u>(b) Title V of the "Gramm-Leach-Bliley Act of 1999,"</u>	135
<u>Public Law 106-102, as amended;</u>	136
<u>(c) The "Federal Information Security Modernization Act of</u>	137
<u>2014," Public Law 113-283.</u>	138
<u>(2) When a framework listed in division (B)(1) of this</u>	139
<u>section is amended, a covered entity whose cybersecurity program</u>	140
<u>reasonably complies with that framework shall reasonably comply</u>	141
<u>with the amended framework not later than one year after the</u>	142
<u>effective date of the amended framework.</u>	143
<u>(C)(1) The cybersecurity program reasonably complies with</u>	144
<u>both the current version of the "payment card industry (PCI)</u>	145
<u>data security standard" and the current version of another</u>	146
<u>applicable industry recognized cybersecurity framework listed in</u>	147
<u>division (A) of this section, subject to divisions (C)(2) and</u>	148
<u>(D) of this section.</u>	149
<u>(2) When a final revision to the "PCI data security</u>	150
<u>standard" is published, a covered entity whose cybersecurity</u>	151
<u>program reasonably complies with that standard shall reasonably</u>	152
<u>comply with the revised standard not later than one year after</u>	153
<u>the publication date stated in the revision.</u>	154
<u>(D) If a covered entity's cybersecurity program reasonably</u>	155
<u>complies with a combination of industry recognized cybersecurity</u>	156
<u>frameworks, as described in division (A) or (C) of this section,</u>	157
<u>and two or more of those frameworks are revised, the covered</u>	158
<u>entity whose cybersecurity program reasonably complies with</u>	159
<u>those frameworks shall reasonably comply with all of the revised</u>	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