As Introduced

132nd General Assembly Regular Session 2017-2018

S. B. No. 220

Senators Hackett, Bacon

A BILL

То	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
or nonprofit corporation or unincorporated nonprofit association	12
that operates in Ohio.	13
(B) "Covered entity" means a business that accesses,	14
maintains, communicates, or handles personal information.	15
(C) "Data breach" has the same meaning as "breach of the	16
security of the system" in section 1349.19 of the Revised Code.	17
(D) "Individual" means a natural person.	18

(E) "NIST cybersecurity framework" means the framework for	19
improving critical infrastructure cybersecurity developed by the	20
national institute of standards and technology, as updated from	21
time to time.	
(F) "Person" means an individual, corporation, business	23
trust, estate, trust, partnership, association, or other legal	24
entity that conducts business in this state.	
(G) "Personal information" has the same meaning as in	26
section 1349.19 of the Revised Code.	27
Sec. 1354.02. (A) Each covered entity seeking a safe	28
harbor under sections 1354.01 to 1354.05 of the Revised Code	29
shall create, maintain, and comply with a written cybersecurity	30
program that contains administrative, technical, and physical	31
safeguards for the protection of personal information that	32
complies with the NIST cybersecurity framework or other industry	33
cybersecurity framework as described in section 1354.03 of the	34
Revised Code.	35
(B) A covered entity's cybersecurity program shall be	36
designed to do all of the following:	37
(1) Protect the security and confidentiality of personal	38
information;	39
(2) Protect against any anticipated threats or hazards to	40
the security or integrity of personal information;	41
(3) Protect against unauthorized access to and acquisition	42
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.	45
(C) The scale and scope of a covered entity's	46

cybersecurity program under division (A) of this section shall	
be appropriate if it is based on all of the following factors:	48
(1) The size and complexity of the covered entity;	49
(2) The nature and scope of the activities of the covered	50
<pre>entity;</pre>	51
(3) The sensitivity of the personal information to be	52
<pre>protected;</pre>	53
(4) The cost and availability of tools to improve	54
information security and reduce vulnerabilities;	55
(5) The resources available to the covered entity.	56
(D) A covered entity that implements and maintains a	57
cybersecurity program that complies with the NIST cybersecurity	58
framework, or other industry cybersecurity framework as	59
described in section 1354.03 of the Revised Code, shall be	60
deemed to be in compliance with this section. Compliance with	61
this section shall constitute an affirmative defense to any	62
cause of action sounding in tort that alleges the failure to	63
implement reasonable information security controls resulted in a	64
data breach. Following any update to the NIST cybersecurity	65
framework, or other industry recognized data security framework,	66
the covered entity shall have a period of one year from the	67
stated effective date as prescribed in the framework to comply	68
with the update. If a covered entity complies with the update	69
within one year of the stated effective date found in the	70
framework as updated, the entity shall still be deemed to be in	71
compliance with this section.	72
Sec. 1354.03. A covered entity shall be deemed to be in	73
compliance with section 1354.02 of the Revised Code if either of	74
the following apply:	75

(A) The covered entity is in substantial compliance with	76
any of the following:	77
(1) NIST special publication 800-171;	78
(2) NIST special publications 800-53 and 800-53a;	79
(3) The federal risk and authorization management program;	80
(4) Center for internet security critical security	81
controls;	82
(5) International organization for	83
standardization/international electrotechnical commission 27000	84
family - information security management systems.	85
(B) The covered entity is regulated by the state and the	86
federal government and is in substantial compliance with the	87
entirety of any of the following:	88
(1) The security requirements of the "Health Insurance	89
Portability and Accountability Act of 1996," as set forth in 45	
CFR Part 164 Subpart C;	91
(2) Title V of the "Gramm-Leach-Bliley Act of 1999,"	92
Public Law 106-102, as amended;	93
(3) The "Federal Information Security Modernization Act of	94
2014," Public Law 113-283.	95
Sec. 1354.04. Sections 1354.01 to 1354.05 of the Revised	96
Code shall not be construed to provide a private right of	97
action, including a class action, with respect to any act or	98
practice regulated under those sections.	99
Sec. 1354.05. If any provision of sections 1354.01 to	100
1354.05 of the Revised Code or the application thereof to a	101
covered entity is for any reason held to be invalid, the	102

remainder of the provisions under those sections and the	
application of such provisions to other covered entities shall	104
not be thereby affected.	
Section 2. (A) The purpose of this act is to establish a	106
legal safe harbor to be pled as an affirmative defense to a	107
cause of action sounding in tort that alleges the failure to	108
implement reasonable information security controls resulted in a	109
data breach. The safe harbor shall apply to all covered entities	110
that implement a cybersecurity program that complies with the	111
Framework for Improving Critical Infrastructure Cybersecurity	112
developed by the National Institute of Standards and Technology,	113
or other industry recognized data security framework.	114
(B) This act is intended to be an incentive and to	115
encourage businesses to achieve a higher level of cybersecurity	116
through voluntary action. The bill does not, and is not intended	117
to, create a minimum cybersecurity standard that must be	118
achieved, nor shall it be read to impose liability upon	119
businesses that do not obtain or maintain practices in	120
compliance with the frameworks referenced in this section	121