



July 11, 2018

OHIO LEGISLATURE PASSES CYBERSECURITY PROGRAM SAFE HARBOR BILL

The Ohio General Assembly passed Ohio S.B. No. 220 that provides a legal safe harbor to covered entities that implement a cybersecurity program that meets the requirements outlined in the law. The law gives a covered entity a safe harbor if it does one of the following:

- (1) Creates, maintains and complies 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 provided in the law; or
- (2) Creates, maintains and complies 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 provided in the law.

Under the new law a cybersecurity program reasonably conforms to an "industry recognized cybersecurity framework" if, among other methods, 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:

- (1) The security requirements of the Health Insurance Portability and Accountability Act of 1996;
- (2) Title V of the Gramm-Leach-Bliley Act of 1999, as amended;
- (3) The Federal Information Security Modernization Act of 2014;
- (4) The Health Information Technology for Economic and Clinical Health Act.

If a covered entity satisfies these requirements, the entity is entitled to an affirmative defense to any cause of action sounding in tort that is brought under the laws of Ohio or in the courts of Ohio and that alleges that failure to implement reasonable information security controls resulted in a data breach concerning personal information or

restricted information.

The bill defines a "covered entity" as 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 of Ohio. "Personal information" generally means an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted or altered by any method or technology in such a manner that the data elements are unreadable: (i) social security number; (ii) driver's license number or state identification card number; (iii) account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account. "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.

Ohio S.B. No. 220 will be sent to the governor for his signature and be effective 90 days after the bill is filed with the Ohio Secretary of State.

Please contact us with questions or for more information. ☐

✧ *Elizabeth Anstaett and Lindsay Valentine*

Darrell L. Dreher
ddreher@dtlaw.com

Elizabeth L. Anstaett
eanstaett@dtlaw.com

Emily C. Cellier
ecellier@dtlaw.com

Susan L. Ostrander
sostrander@dtlaw.com

2750 HUNTINGTON CENTER
41 S. HIGH STREET
COLUMBUS, OHIO 43215
TELEPHONE: (614) 628-8000 FACSIMILE: (614) 628-1600
WWW.DTLAW.COM

To see previously sent ALERTS, visit our website at www.dtlaw.com

To decline future ALERTS, please contact us at ALERTS@DLT.LAW.COM. This ALERT has been prepared for informational purposes only. It does not constitute legal advice and does not create an attorney-client relationship.

Michael C. Tomkies
mtomkies@dtlaw.com

Susan M. Seaman
sseaman@dtlaw.com

Lindsay P. Valentine
lvalentine@dtlaw.com

Judith M. Scheiderer
jscheiderer@dtlaw.com

Robin R. De Leo
robin@deher-la.com