Tucker Ellis LLP

CLIENT ALERT

OHIO BILL PROPOSES SAFE HARBOR AGAINST BREACH SUITS TO BUSINESSES MAINTAINING RECOGNIZED CYBERSECURITY PROGRAMS

DECEMBER 2017

Maintaining robust cybersecurity measures that meet government- and industry-recognized standards will provide businesses operating in Ohio with a legal defense to data breach lawsuits, if a bill recently introduced in the Ohio Senate becomes law.

Ohio Senate Bill No. 220 (S.B. 220), known as the Data Protection Act, was introduced to provide businesses with an incentive to achieve a "higher level of cybersecurity" by maintaining a cybersecurity program that substantially complies with one of eight industry-recommended frameworks. *See* S.B. 220, Section 1, proposed Ohio Rev. Code §§ 1354.01 to 1354.05.

COMPLIANCE STANDARDS TO BE MET

Businesses that are in substantial compliance with one of the eight frameworks outlined in S.B. 220 would be entitled to a "legal safe harbor" to be pled as an affirmative defense to tort claims related to a data breach stemming from alleged failures to adopt reasonable cybersecurity measures. S.B. 220, Section 1, proposed Ohio Rev. Code §§ 1354.02(A) and (C), 1354.03; S.B. 220, Section 2(A). These frameworks include the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, the Security Rule of the Health Insurance Portability and Accountability Act (HIPAA) (45 CFR § 164.302, *et seq.*) for healthcare-industry businesses regulated by HIPAA, and the Safeguards Rule of the Gramm-Leach-Bliley Act (16 CFR § 314.1, *et seq.*) for certain financial institutions. *Id.*, proposed § 1354.03. The other recognized cybersecurity frameworks are listed in proposed § 1354.03.

SAFE HARBOR DETAILS

As drafted, S.B. 220's "legal safe harbor" would not provide a business with blanket immunity to a data breach lawsuit, and applies only to tort claims (*i.e.*, negligence and invasion of privacy claims). It would also not apply to contract-based claims, such as those that could arise from a business-vendor dispute or between a business and its customers where a contractual relationship is alleged. Further, because S.B. 220 requires the safe harbor to be pled as an affirmative defense to a lawsuit, the business would still have the burden of establishing that its cybersecurity program complied with the law's requirements. That said, S.B. 220 provides businesses with a significant incentive to adopt and maintain a compliant cybersecurity program.

S.B. 220 does not take a one-size-fits-all approach to cybersecurity. The necessary scale and scope of a cybersecurity program required to trigger the legal safe harbor is judged by various business-specific factors, including (a) the size, complexity, and nature of the business and its activities, (b) the level of sensitivity of the personal information it possesses, (c) the cost and availability of tools to improve security and reduce vulnerabilities, and (d) the resources the business has at its disposal to expend on cybersecurity. *Id.*, Section 1, proposed § 1354.02(C). The language of S.B. 220 makes clear that the "bill does not, and is not intended to, create a minimum cybersecurity standard that must be achieved," and it is not to "be read to impose liability upon businesses that do not obtain or maintain" a cybersecurity program that is compliant with one of the eight recognized frameworks. *Id.*, Section 2(B).

LEGISLATIVE NEXT STEPS

S.B. 220 was introduced in the Ohio Senate on October 17 and was assigned to the Government Oversight and Reform Committee for consideration on November 29. Tucker Ellis will monitor S.B. 220 and continue to provide updates, including any opportunities for public comment and participation, as the bill winds its way through the legislative process. For additional information, contact bill sponsors Sen. Bob Hackett (R-London) at 614.466.3780 or Sen. Kevin Bacon (R-Minerva

Park) at 614.466.8064. Government Oversight and Reform Committee Chair Sen. Bill Coley (R-Liberty Township) can be reached at 614.466.8072.

REMINDER: DUTY TO REPORT BREACHES IN OHIO

Even if passed, S.B. 220 would not change Ohio's notification laws. In fact, the introduction of S.B. 220 provides a reminder that, since 2006, Ohio law has required most businesses to provide notification of data breaches involving Ohio residents. *See* Ohio Rev. Code § 1349.19. The specific notification requirements can be found at § 1349.19, but they generally require notification to Ohio residents no later than 45 days following the discovery or notification of the breach, subject to certain exceptions for legitimate law enforcement needs and "consistent with measures necessary to determine the scope of the breach." *Id.* § 1349.19(B)(2). Section 1349.19 does not apply to HIPAA covered entities and financial institutions that have their own notification requirements under federal law.

WHAT DOES THIS MEAN FOR COMPANIES IN OHIO?

While S.B. 220 is not yet law, it reflects a step in the right direction in rewarding businesses that adopt and maintain more robust cybersecurity programs. As the calendar turns to 2018, businesses of all shapes, sizes, and industries should take the time to assess the confidential, proprietary, personal, or otherwise sensitive information they possess and examine and evaluate the privacy and security programs in place to protect that information. In doing so, businesses should consider their overall privacy and security culture and ask whether the organization from the board down to its employees is adequately focused on these issues. Businesses should also ensure that they have conducted a thorough risk assessment to identify vulnerabilities and at-risk areas, adopt additional security measures to manage those risks, consider whether they have adequate policies and procedures and a tested incident response plan, and evaluate and update their employee training to make sure that it addresses the latest cyberthreats.

ADDITIONAL INFORMATION

If you have any questions about Ohio Senate Bill No. 220 or data privacy and cybersecurity matters generally, please contact:

- **BILL BERGLUND** | 216.696. 2698 | william.berglund@tuckerellis.com
- **ROB HANNA** | 216.696.3463 | robert.hanna@tuckerellis.com
- **VICKY VANCE** | 216.696.3360 | victoria.vance@tuckerellis.com