Tucker Ellis LLP

CLIENT ALERT

CYBERSECURITY SAFE HARBOR AGAINST DATA BREACH LAWSUITS BECOMES OHIO LAW

AUGUST 2018

On August 3, Ohio Governor John Kasich signed the Data Protection Act, which provides a safe harbor against data breach suits to businesses maintaining recognized cybersecurity programs. The Act will go into effect on November 2, 2018. Ohio businesses of all sizes and industries should be aware of this new law given the significant legal and reputational risks and costs associated with data breaches.

Businesses taking reasonable cybersecurity precautions that meet certain industry-recognized frameworks will now be afforded a "safe harbor" against tort claims alleging that a failure to implement reasonable cybersecurity measures resulted in a data breach concerning personal or restricted information. *See* Ohio R.C. 1354.02(D)(2) (effective November 2, 2018). While the safe harbor does not immunize an entity from liability, it does aid businesses that adopt recognized frameworks to protect personal information. It is step forward for both businesses and consumers whose personal information is at risk.

The Data Protection Act, which creates R.C. 1354.01 to 1354.05, is the first piece of legislation introduced as a result of Ohio Attorney General Mike DeWine's CyberOhio Initiative. The Act was introduced as an effort to encourage businesses to take steps to protect their customer data and minimize costly data breaches by maintaining a cybersecurity program that reasonably conforms with enumerated industry-recommended frameworks. *See* Ohio Senate Bill 220 (S.B. 220), Section 3(A); R.C. 1354.01 to 1354.05.

SAFE HARBOR DETAILS

In order to trigger this safe harbor, an entity must adopt cybersecurity measures designed to: (1) protect the security and confidentiality of personal information; (2) protect against any anticipated threats or hazards to the security or integrity of the personal information; and (3) protect against unauthorized access to and acquisition of information that is likely to result in a material risk of identity theft or other fraud. R.C. 1354.02(B). But it is not a one-size-fits-all approach. Instead, the scale of the cybersecurity program should be based on the organization's size and complexity, the nature and scope of its activities, the sensitivity of the personal information protected under the program, the cost and availability of tools to improve its information security, and the resources available to the organization. R.C. 1354.02(C).

The entity's cybersecurity measures must also "reasonably conform" to one of the industry-recognized frameworks listed in R.C. 1354.03. 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. R.C. 1354.03.

The Data Protection Act requires businesses to assert this safe harbor as an affirmative defense and establish that its cybersecurity program reasonably conforms with an applicable framework. Although the burden of proof remains with the entity asserting the defense, the Act expressly states that it does not create a minimum cybersecurity standard or impose liability upon businesses maintaining cybersecurity practices that are not in compliance. *See* S.B. 220, Section 3(B).

LEGAL RECOGNITION OF BLOCKCHAIN TRANSACTIONS

The version of S.B. 220 signed by Governor Kasich also includes certain terms of Ohio Senate Bill No. 300, known as the Uniform Electronic Transactions Act. The amendment gives legal effect to transactions, signatures, or contracts secured by blockchain technology by defining

these transactions as "electronic records." Blockchain technology refers to a digital ledger where information, or "blocks," are connected to each other through written code known as "chains." The information is held on a decentralized register that is regularly updated and is considered incorruptible. With this amendment, Ohio is one of the most recent states to pass legislation recognizing signatures and smart contracts secured by blockchain technology as legal documents.

NO CHANGES TO BREACH-REPORTING OBLIGATIONS IN OHIO

The Data Protection Act does not affect Ohio's current notification laws. Entities adopting one of the safe harbor's cybersecurity frameworks must still provide notification of data breaches involving Ohio residents. *See* R.C. 1349.19. The specific notification requirements can be found at R.C. 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 CAN OHIO COMPANIES DO TO TAKE ADVANTAGE OF THE DATA PROTECTION ACT?

No business is immune from the threat of a data breach. Time alone will test the effectiveness of the Act at protecting consumer data and minimizing data breach costs, but the new safe harbor defense reflects a step in the right direction for Ohio businesses and consumers alike. This new defense provides Ohio businesses the opportunity to evaluate the personal information they create, receive, maintain, and transmit, as well as the program they have in place to protect that information. Businesses should first consult their latest data-mapping and system inventories to understand how information is flowing through the organization and then decide how it should be secured. Businesses should also examine the administrative, physical, and technical security controls they currently have in place and to what extent their overall security program conforms with the cybersecurity frameworks listed in R.C. 1354.03. In doing so, a business may take into account what is reasonable given the organization's size, revenues, the resources available to it, and the sensitivity of the information it maintains. Because data breaches can happen even if a business adopts strong cybersecurity measures, all businesses should also have a tested incident response plan in place so it is ready in the unfortunate event of a breach.

ADDITIONAL INFORMATION

For additional information, please contact:

- **Rob Hanna** | 216.696.3463 | robert.hanna@tuckerellis.com
- **Bill Berglund** | 216.696.2698 | william.berglund@tuckerellis.com
- **Emily Knight** | 216.696.4893 | emily.knight@tuckerellis.com