Data Protection Act - Ohio

BUCKINGHAM

OHIO'S NEW DATA PROTECTION ACT

Cybersecurity "Safe Harbor" in Ohio for Data Breach Lawsuits

Starting on November 2, 2018, Ohio businesses that take reasonable precautions in cybersecurity meeting certain industry-recognized frameworks will now be afforded a new "safe harbor" defense against tort claims alleging that a failure to implement reasonable cybersecurity measures resulted in a data breach related to personal or restricted information. While the safe harbor does not immunize a business from liability, it does provide additional protection for entities adopting recognized frameworks to protect personal information. The Data Protection Act is an effort by the state to encourage businesses to take sensible steps to protect collected customer data and minimize disastrous data breaches by maintaining a cybersecurity program that reasonably conforms to one of the enumerated industry-recommended frameworks. Ohio businesses should pay attention given the substantial legal and reputational risks and costs associated with data breaches.

Compliance

The rational is to provide Ohio organizations with a legal incentive to achieve a "higher level of cybersecurity" by creating and maintaining a cybersecurity program that substantially complies with an industry-recommended framework. Businesses that substantially comply with any of the frameworks outlined in the Data Protection Act are entitled to a "legal safe harbor" to be pled as an affirmative defense to tort claims alleging that a failure to implement reasonable security controls resulted in a data breach. The listed frameworks include:

- National Institute of Standards and Technology's (NIST) Cybersecurity Framework;
- Federal Risk and Authorization Management Program's Security Assessment Framework;
- Center for Internet Security's Critical Security Controls for Effective Cyber Defense;
- Federal Information Security Modernization Act;
- Gramm-Leach-Bliley Act's Safeguards Rule;
- Health Information Technology for Economic and Clinical Health Act;
- Health Insurance Portability and Accountability Act's (HIPAA) Security Rule;
- International Organization for Standardization (ISO)/ International Electrotechnical Commission's (IEC) 27000 Family – Information Security Management Systems Standards.

Questions? Contact **Paul Filon** (pfilon@bdblaw.com) to discuss today.

The Details

The law does not promote a one-size-fits-all approach to cyber-security. The Act expressly states that it does not "create a minimum cybersecurity standard that must be achieved" or "impose liability upon businesses that do not obtain or maintain practices in compliance with the frameworks." The intent is "to be an incentive and to encourage businesses to achieve a higher level of cybersecurity through voluntary action." To qualify for the safe harbor defense, the entity must implement a cybersecurity program designed to:

(1) protect the security and confidentiality of personal information;

(2) protect against anticipated threats or hazards to the security or integrity of personal information; and

(3) protect against unauthorized access to and acquisition of personal information.

The scale of the cybersecurity program should be appropriate to:

(1) the organization based on its size and complexity;

(2) the nature and scope of its activities;

(3) the sensitivity of the personal information protected under the program;

(4) the cost and availability of tools to improve its information security; and

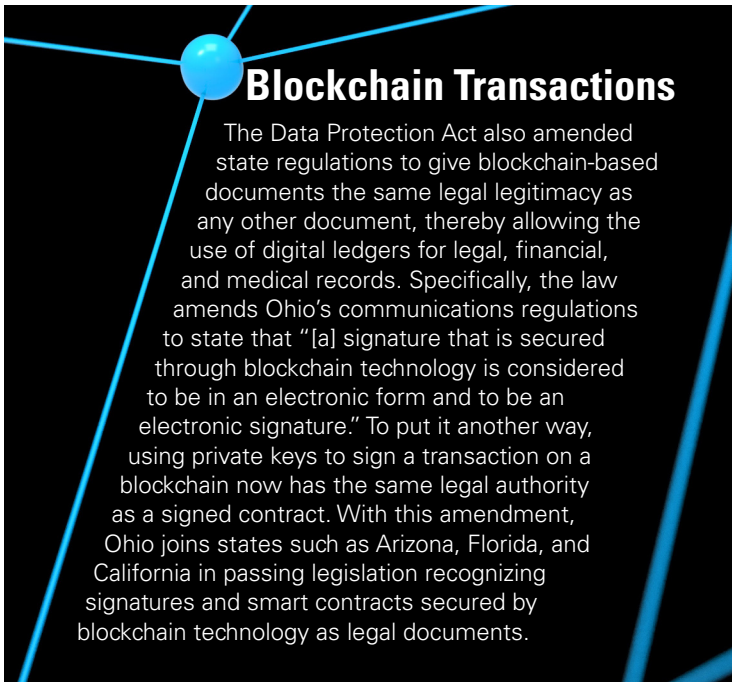
(5) the resources available to the organization.

Critically, for businesses that accept payment cards, the Payment Card Industry's Data Security Standard (PCI DSS) is not a framework eligible for safe harbor. So, businesses that currently comply with PCI DSS must also comply with one of the listed industry frameworks in order to qualify for the safe harbor. Another potential issue for organizations is that many of the enumerated industry frameworks, like NIST, do not have a standard certification process, so proving compliance with the applicable framework may prove challenging.

Protections and Limitations

The Act's "legal safe harbor" does not provide blanket immunity in the event of a data breach lawsuit. Instead, the law creates an affirmative defense to tort actions (such as negligence and invasion of privacy) brought against Ohio businesses that have suffered a data breach involving restricted or personal information. The entity still must establish that its cybersecurity program complied with the law's requirements. Additionally, the safe harbor does not apply to contract-based actions, such as those that arise between a business and its customers where a contractual relationship is alleged or from a business-vendor dispute.

Of additional note, the Data Protection Act does not amend Ohio's current breach notification laws. Any entity that adopts one of the safe harbor's cybersecurity frameworks must still provide notification of data breaches affecting Ohio residents. In Ohio, notification must occur no later than 45 days following the discovery or notification of the breach (subject to specific exceptions for legitimate law enforcement needs and measures necessary to determine scope of the breach). Further, neither the Data Protection Act, nor Ohio's notification law affects breach notification requirements for HIPAA-covered entities and financial institutions that have their own notification requirements under federal law.



Going Forward

No business is immune from the danger of a data breach. Companies should approach data governance as a question of WHEN, and not IF a breach will happen. The Data Protection Act gives Ohio businesses a chance to evaluate the personal information they create, maintain, receive, and share, as well as the safeguards in place to protect that information. Businesses should map and classify the data they collect to understand what information they collect, and how that information is flowing through the organization. Once businesses understand what data they have and where that data is located, they can make informed decisions about appropriate administrative, physical, and technical safeguards to adopt, and create a cybersecurity program that makes sense based on the company's size, revenues, resources, and sensitivity of information maintained. 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. Data breaches are an inevitable part of doing business no matter how robust a company's security program may be. However, following the guidance outlined in the Data Protection Act will set businesses ahead of the curve and provide for a valuable defense in subsequent litigation.

Questions? Contact **Paul Filon** (pfilon@bdblaw.com) to discuss today.