Client Alert: Ohio Bill Would Create Cybersecurity Safe Harbor

Related Attorneys

John L. Landolfi

Related Services

Data Strategy, Privacy and Security

Litigation

CLIENT ALERT | 12.5.2017

Senate Bill 220, also known as the Data Protection Act, was recently introduced in the Ohio legislature. If passed, the Data Protection Act will create a safe harbor from certain liability as a result of a data breach where the organization has complied with the National Institute of Standards and Technology (NIST) Cybersecurity Framework or certain other cybersecurity frameworks. The NIST Cybersecurity Framework is voluntary guidance, based on existing standards, guidelines and practices, for organizations to better manage and reduce cybersecurity risk. The Data Protection Act was introduced as a way to help Ohio businesses with cybersecurity issues and manage cybersecurity risks.

The Data Protection Act provides that, if covered businesses implement and maintain a cybersecurity program that complies with certain cybersecurity frameworks, then the organization will have an affirmative defense to a tort claim alleging that a failure to implement reasonable security controls resulted in a data breach. In order to qualify for this safe harbor, the entity must implement a cybersecurity program 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 personal information, (3) protect against unauthorized access to and acquisition of personal information. The scale of the cybersecurity program should be appropriate to the organization based on its 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.

Additionally, the organization's cybersecurity program must be in "substantial compliance" with one of the following cybersecurity frameworks:

- NIST special publication 800-171, or 800-53 and 800-53a;
- The federal risk and authorization management program;
- Center for Internet Security critical security controls;
- International Organization for Standardization (ISO)/international electrotechnical commission (IEC) 27000 family – information

security management systems standards.

For entities regulated by the state and federal government, cybersecurity programs in substantial compliance with the security requirements of the Health Insurance Portability and Accountability Act (HIPAA), Title V of the Gramm-Leach-Bliley Act (GLBA) or the Federal Information Security Modernization Act also qualify for the safe harbor.

The Data Protection 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." Rather, it seeks "to be an incentive and to encourage businesses to achieve a higher level of cybersecurity through voluntary action."

Ohio Attorney General Mike DeWine has endorsed the legislation, stating "The Data Protection Act is an effort to encourage businesses to take the necessary steps to protect their customer data and avoid costly data breaches. As businesses beef up their cybersecurity, consumers will benefit from the additional protection as well."

Notably, for businesses that accept payment cards, the Payment Card Industry's Data Security Standard (PCI DSS) is not one of the cybersecurity frameworks eligible for the safe harbor. So, businesses that currently comply with PCI DSS must also comply with one of the above industry frameworks in order to qualify for the safe harbor. Another potential challenge for covered organizations is that many of the industry frameworks, like NIST, do not have a standard certification process, so proving compliance with the applicable framework may prove challenging. However, given the increasing risk that cybersecurity presents for many organizations, the Data Protection Act if passed may grant some relief. For questions about this legislation or cybersecurity, please contact your Vorys attorney.