VORYS

Publications

Client Alert: Ohio Enacts Cybersecurity Safe Harbor Law for Data Breach Litigation

Related Professionals

John L. Landolfi

Christopher L. Ingram

Related Services

Data Strategy, Privacy and Security

Litigation and Appeals

CLIENT ALERT | 8.6.2018

On August 3, 2018, Governor John Kasich signed Senate Bill 220, also known as the Ohio Data Protection Act. Under the Act, eligible organizations may rely on their conformance to certain cybersecurity frameworks as an affirmative defense against tort claims in data breach litigation. The Act is intended to provide organizations with a legal incentive to implement written cybersecurity programs.

In order to qualify for this new defense, the organization must implement a written 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 that is likely to result in a material risk of identity theft or fraud. 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 "reasonably conform" to one of the following cybersecurity frameworks:

- National Institute of Standards and Technology's (NIST) Cybersecurity Framework;
- NIST special publication 800-171, or 800-53 and 800-53a;
- Federal Risk and Authorization Management Program's Security Assessment Framework;
- Center for Internet Security's Critical Security Controls for Effective Cyber Defense;
- International Organization for Standardization (ISO)/International Electrotechnical Commission's (IEC) 27000 Family – Information Security Management Systems Standards.

For organizations that accept payment cards, their cybersecurity programs must also comply with the Payment Card Industry's Data Security Standards (PCI-DSS) to qualify for the affirmative defense. Similarly, organizations subject to certain state or federally mandated security requirements may also qualify, such as the security requirements in the Health Insurance Portability and Accountability Act (HIPAA), Title V of the Gramm-Leach-Bliley Act (GLBA), the Federal Information Security Modernization Act (FISMA), or the Health Information Technology for Economic and Clinical Health Act (HITECH).

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

This law will be the first in the nation which incentivizes businesses to implement certain cybersecurity controls by providing them with an affirmative defense. States like New York require certain businesses to meet specific cybersecurity compliance standards, without providing a specific affirmative defense as an incentive to do so.

Qualification for this new safe harbor will not be automatic and may be challenging to establish. Many of the specified frameworks, like NIST, do not have a standard certification process, so proving that a security program conforms to the applicable framework may prove difficult. However, given the increasing risk that cybersecurity presents for many organizations, the Ohio Data Protection Act may grant some relief. For questions about this legislation or other cybersecurity issues, please contact John Landolfi, Chris Ingram, or your Vorys attorney.