Ohio Data Breach Safe Harbor Law Now Effective

PROFESSIONALS

Melissa A. Kern
mkern@fbtlaw.com
513.651.6898

Michael E. Nitardy
mnitardy@fbtlaw.com
859.817.5914

PRACTICES

Privacy and Data Security Law

INDUSTRIES

Technology (fbtTECH)

NOVEMBER 2, 2018

Legal Update

Ohio's data breach safe harbor law goes into effect today. By choosing to provide incentive for companies to implement written cybersecurity programs the Ohio legislature has chosen to use a "carrot" approach to encourage businesses to adopt cybersecurity programs instead of a more traditional "stick" approach of imposing fines and penalties for failing to do so. Although the adoption of written cybersecurity programs remains optional under the new law, implementing one can greatly reduce businesses' exposure to lawsuits and claims alleging that lax security practices led to a data breach or identity theft.

What the Law Does

As we reported in a previous update, the law creates an affirmative defense (referred to as a "safe harbor") to tort actions brought against eligible businesses alleging that a business' failure to implement reasonable information security controls resulted in a data breach concerning personal information or restricted information. "Personal information" has the same definition as Ohio's data breach notification statute. The law defines "restricted information" as

> any information about an individual, other than personal information, that, alone or in combination with other information, including personal information, can be used to distinguish or trace the individual's identity or that is linked or linkable to an individual, if the information is not encrypted, redacted, or altered by any method or technology in such a manner that the information is unreadable, and the breach of which is likely to result in a material risk of identity theft or other fraud to person or property.

In adopting this definition, Ohio follows the European Union in recognizing that information about an individual that was once not considered to lead directly to identity theft or other criminal activity can nonetheless be used to track and trace individuals when combined with other information, including "personal information."

Ohio Data Breach Safe Harbor Law Now Effective

How the Safe Harbor Works

A business can become eligible for the safe harbor by "creating, maintaining, and complying with" a written cybersecurity program that "contains administrative, technical, and physical safeguards" to protect (1) personal information or (2) both personal information and restricted information. Businesses that take the latter approach and tailor their written cybersecurity program to protect both personal information and restricted information will see the greatest protection under the law.

Importantly, to be eligible for the law's safe harbors, any written cybersecurity program must be designed to the do the following:

1. Protect the security and confidentiality of the information.
2. Protect against any anticipated threats or hazards to the security or integrity of the information.
3. Protect against unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.

The law identifies specific cybersecurity frameworks through which businesses can qualify for the safe harbor, essentially dividing such frameworks into three categories:

1. Industry recognized cybersecurity frameworks, (i.e., those recommended by administrative bodies, like the National Institute of Standards and Technology.
2. Frameworks required by federal or state law under a relevant federal or state law or regulation (i.e., HIPAA, Gramm-Leach-Bliley).
3. A framework that combines the payment card industry (PCI) data security standard with a current version of an applicable industry recognized cybersecurity framework.

After a business adopts one of these frameworks (or a combination of these frameworks) and the framework is updated or amended by the applicable administrative or governing body, the business must likewise update its cybersecurity program to be in compliance with such changes within one-year of the administrative or governing body's adoption of such changes.

While identifying the frameworks through which businesses can qualify for the safe harbor, the law also recognizes that one size does not fit all when it comes to effective and reasonable cybersecurity programs. As a result, the law explicitly allows for programs that take the following into account:

1. The size and complexity of the covered entity.
2. The nature and scope of the activities of the covered entity.
3. The sensitivity of the information to be protected.
4. The cost and availability of tools to improve information security and reduce vulnerabilities.
5. The resources available to the covered entity.

In addition, the law makes clear that it provides no new private right of action for the failure of a business to comply with the law's provisions.

Takeaways

A written cybersecurity program is a necessity to doing business in today's world. Ohio's law encourages businesses to do what they should be doing anyway—implementing cybersecurity programs that protect sensitive information (i.e., "personal information" and "restricted information"). Businesses that fail to do so risk having fewer defenses to assert in the event of litigation involving claims related to their security practices.

For more information, please contact Melissa Kern, Mike Nitardy, Jane Shea or any Attorney in Frost Brown Todd's Privacy and Information Security group.