JONES DAY

COMMENTARY

OCTOBER 2018

Ohio Adopts Safe Harbor for Businesses Involved in Data Breach

IN SHORT

The Situation: On August 3, 2018, Ohio Governor John Kasich signed Senate Bill 220, the Ohio Data Protection Act ("Ohio DPA"), which provides a safe harbor against data breach lawsuits for businesses that implement and maintain cybersecurity programs that meet certain industry-recognized standards.

The Result: The Ohio DPA provides businesses with an incentive to implement and maintain an effective cybersecurity program, in contrast to other states that have taken a more punitive approach to cybersecurity, such as California's recently passed Consumer Privacy Act that imposes new obligations and potential liabilities on California businesses.

Looking Ahead: The Ohio DPA goes into effect on November 2, 2018.

The Ohio DPA incentivizes businesses to implement and maintain an effective cybersecurity program by providing an affirmative defense to certain tort actions related to data breaches. The law does not require businesses to comply with the Ohio DPA. Rather, a business that can demonstrate its cybersecurity program meets certain enumerated standards is eligible for the defense to liability for the breach.

Recognizing that different businesses have different needs and resources when it comes to cybersecurity, the Ohio DPA takes into account individualized factors to determine the adequate scale and scope of a business's program under the law. A business has the flexibility to choose from different cybersecurity frameworks as the foundation for a program (as discussed below), allowing a business to tailor its program based on a company's particular industry and circumstances.

Notably, the Ohio DPA is the first law of its kind in the United States and is the first piece of legislation from Ohio Attorney General Mike DeWine's CyberOhio Initiative. While other states require businesses to meet certain cybersecurity compliance standards or punish businesses that suffer a data breach, no other state provides an affirmative defense as an incentive to adopting industry-standard cybersecurity practices like Ohio's new DPA.

The Ohio DPA provides two incentives for businesses: (i) the DPA provides the opportunity for businesses to evaluate and improve their current program, which, as a result, lessens the likelihood of a data breach; and (ii) if such a breach still occurs, the DPA provides a safe-harbor defense against tort claims asserting that the business has inadequate data security measures.

In deciding whether to take advantage of the Ohio DPA's safe-harbor provision, businesses should take into account the ever-increasing number of high-profile data breaches, which often result in substantial monetary and reputational damage.

> The Ohio DPA is the first law of its kind in the United States. No other state provides an affirmative defense as an incentive to adopting industry-standard cybersecurity practices like Ohio's new DPA.

Cybersecurity Program

To take advantage of the safe harbor provision under the Ohio DPA, a business must implement a cybersecurity program that is designed to:

- Protect the security and confidentiality of personal information;
- Protect against any anticipated threats or hazards to the security or integrity of personal information; and
- Protect against unauthorized access to the acquisition of personal information that is likely to result in a material risk of identity theft or other fraud for the associated individuals.

Scale and Scope of the Business are Important Factors Under the Ohio DPA

The Ohio DPA recognizes that there is no "one size fits all" approach to cybersecurity. Thus, the scale and scope of an effective program under the law takes into account:

- The size and complexity of the business;
- The nature and scope of the activities of the business;
- The sensitivity of the information to be protected;
- The cost and availability of tools to improve information security and reduce vulnerabilities; and
- The resources available to the business.

The Ohio DPA reflects the reality that, for example, a local hardware store with six employees should not be expected to maintain the same kind of cybersecurity program as a bank with hundreds of employees and troves of sensitive customer data.

Applicable Cybersecurity Frameworks Under the Ohio DPA

The Ohio DPA seeks to provide companies both certainty and flexibility by establishing an affirmative defense for a business that "reasonably conforms" to one of six industry-recognized cybersecurity frameworks, alone or in combination with the Payment Card Industry Data Security Standard (PCI DSS):

- National Institute of Standards and Technology's ("NIST") Cybersecurity Framework;
- NIST Special Publication 800-171;
- NIST Special Publications 800-53 and 800-53a;
- The Federal Risk and Authorization Management Program (FedRAMP) Security Assessment Framework;
- The Center for Internet Security Critical Security Controls for Effective Cyber Defense; or
- The International Organization for Standardization/International Electrotechnical Commission 27000 Family—Information Security Management Systems.

Businesses regulated by state and/or federal governments must "reasonably conform" to one of the following cybersecurity frameworks, if applicable to that particular business:

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule;
- Title V of the Gramm-Leach-Bliley Act of 1999;
- The Federal Information Security Modernization Act of 2014 (FISMA); or
- The Health Information Technology for Economic and Clinical Health Act (HITECH).

These frameworks are designed to apply to a wide variety of businesses, from the health care industry to the financial sector. Individual businesses are free to choose which framework is most applicable to their operations.

FIVE KEY TAKEAWAYS

1. The Ohio DPA does not establish a minimum standard that all businesses must meet.
2. The Ohio DPA does not modify Ohio's current notification laws, which generally require that businesses provide notice of data breaches as set forth in the Ohio Revised Code. *See* O.R.C. 1349.19.
3. The DPA provides an affirmative defense to tort actions when a plaintiff's claims are based on Ohio law.
4. The Ohio DPA serves as an incentive for businesses to conduct a review of their current cybersecurity program and determine the extent to which they are susceptible to breaches.
5. Some cyber incidents may be unavoidable, so businesses should use the Ohio DPA as an opportunity to implement a qualifying cybersecurity program now so they can take advantage of the statutory affirmative defense to the claims that frequently follow breaches.


Adam Hollingsworth
Cleveland


J. Todd Kennard
Columbus


Vanessa V. Healy
Cleveland


Brandy H. Ranjan
Columbus

YOU MIGHT BE INTERESTED IN: Go To All Recommendations >>

California Adopts Sweeping Consumer Privacy Law

DOJ's Business Email Compromise Takedown Illustrates Pervasiveness of Internet Fraud Schemes

Be Wary of Warranties for Software Design

SUBSCRIBE SUBSCRIBE TO RSS

Jones Day is a global law firm with more than 2,500 lawyers on five continents. We are One Firm Worldwide℠.