D&G | Davis & Gilbert LLP
ATTORNEYS AT LAW

NOVEMBER 2018

DIGITAL MEDIA, TECHNOLOGY & PRIVACY

>> ALERT

NEW LAW CREATES DATA BREACH SAFE HARBOR FOR COMPANIES WITH WRITTEN SECURITY PROGRAMS

A new Ohio law – the Ohio Data Protection Act (the "Act") – has created a legal safe harbor to limit a company's litigation exposure after a data breach if the company maintains and complies with a cybersecurity program with certain controls at the time of breach. All companies – whether located or operating in Ohio or not – should adopt a cybersecurity program that meets the requirements of the Act.

THE BENEFITS

The Act provides covered entities with a legal safe harbor that can be pled as an affirmative defense to tort claims brought in Ohio courts or under Ohio law alleging a company's failure to implement a reasonable cybersecurity program meeting security standards resulting in a breach.

The law does not impose specific security requirements that must be achieved, and does not impose liability on businesses that do not have or maintain practices that comply with the law. The Act states that the purpose of the law is to be an incentive for businesses to voluntarily achieve a higher level of cybersecurity and sets forth minimum cybersecurity standards that need to be met for a covered entity to benefit from the safe harbor provisions of the Act.

THE BASICS

A "covered entity" under the Act is a business that accesses, maintains, communicates, or processes specified personal information or restricted information in or through one or more systems, networks, or services located in or outside of Ohio.

A covered entity that suffers a data breach involving personal or restricted information and is sued for allegedly failing to implement reasonable information security controls is entitled to the Act's safe harbor if it has a written cybersecurity program designed to:

1) Protect the security and confidentiality of the personal or restricted information;

2) Protect against any anticipated threats or hazards to the security or integrity of that information; and

3) Protect against the unauthorized access to and acquisition of that information likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.

Under the Act, the scale and scope of a company's cybersecurity program should be appropriate to its size and complexity and to the nature and scope of its activities. The program must also take into account 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 covered entity.

THE BOTTOM LINE

While there are more laws that require companies to implement reasonable security practices, the Act is the first U.S. law that provides this type of safe harbor to companies that do so. Therefore, every company should implement a comprehensive written information security program, or review and update any existing programs.

>> continues on next page

Critically, the covered entity must reasonably conform with one of the following cybersecurity frameworks:

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

Moreover, a covered entity regulated by a state or federal government can gain the benefit of the affirmative defense by complying with:

- security requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA),
- Title V of the Gramm-Leach-Bliley Act of 1999 (GLB),
- Federal Information Security Modernization Act of 2014, or
- the Health Information Technology for Economic and Clinical Health Act.

Further, a covered entity that processes payment cards must have a program that complies with one of the above cybersecurity frameworks as well as the Payment Card Industry Data Security Standard to be entitled to the safe harbor.

ONGOING OBLIGATIONS

It is important to emphasize that simply creating an appropriate cybersecurity program is not, in and of itself, sufficient to benefit from the affirmative defense. Covered entities also must maintain and comply with their cybersecurity program. In addition, when a cybersecurity program reasonably conforms to a cybersecurity framework as noted above, and that standard or framework is updated or otherwise changed, the covered entity's program also must be amended.

FOR MORE INFORMATION

Gary A. Kibel
Partner
212.468.4918
gkibel@dglaw.com

Vivian W. Byrwa
Associate
212.468.4927
vbyrwa@dglaw.com

Justin H. Lee
Associate
212.468.4894
jlee@dglaw.com

or the D&G attorney with whom you have regular contact.

Davis & Gilbert LLP
212.468.4800
1740 Broadway, New York, NY 10019
www.dglaw.com