LEGAL Insights

Summer 2019

Nicola, Gudbranson & Cooper LLC

New cybersecurity defenses for data breach violations

Data breaches and cybersecurity violations continue to dominate media headlines. The inadvertent disclosure of Personally Identifiable Information (PII) by well-known corporate entities including Equifax Inc., Anthem Inc., Marriott Corp., Uber, Saks Fifth Avenue, Facebook, T-Mobile and Target Corp., have spurred lawmakers to develop legislation that addresses mounting consumer privacy risks.

A corporate entity that breaches its duty of care in the maintenance, protection, distribution, exchange and overall handling of sensitive consumer data, can be saddled with paying for actual and even in some instances, anticipated future damages to entire classes of plaintiffs. Corporate defendants in data-breach cases face exorbitant litigation costs, multi-million-dollar judgments and the potential for declining profits due to negative publicity. Even settlements are costly. For example, the Target settlement in 2017 required payment of $18.5 million to 47 states and the District of Columbia, in addition to the $202 million expenditures on legal fees and other costs associated with the breach.

THE OHIO DATA PROTECTION ACT

Ohio recently became the first state in the U.S. to provide corporate defendants with an affirmative defense to data-breach claims involving personal information. On November 2, 2018, the Ohio Data Protection Act went into effect—and with it, a "safe harbor" for corporate defendants that demonstrate responsible data protection efforts. Ohio corporations now have an affirmative defense against liability for alleged consumer damages if they can demonstrate their concrete efforts to design and implement a cybersecurity program that reasonably conforms to recognized identity standards. While compliance with these standards is not entirely dispositive, corporate defendants are better positioned to avoid liability through compliance.

The new law enumerates nine industry standards by which a company's cybersecurity program is reviewed to determine safe harbor applicability, including:

- National Institute of Standards and Technology (NIST).
- Federal Risk and Authorization Management Program (FedRAMP) (Security Assessment Framework).
- Center for Internet Security Critical Security Controls (CIS CSC).
- International Organization for Standardization (ISO) / International Electrotechnical Commission's (IEC) 27000 Family.
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Security Rule Subpart C).
- Health Information Technology for Economic and Clinical Health Act (HITECH).
- Title 5 of the Gramm-Leach-Bliley Act of 1999 (GLBA).
- Federal Information Security Modernization Act of 2014 (FISMA).
- Payment Card Industry standard (PCI).

SAFE HARBORS

Ohio's move to establish safe harbor standards by which corporations can model their cybersecurity program efforts, offers three key benefits:

- **Reduces the risk of breach.** The intent of Ohio's Data Protection Act is to encourage companies to proactively reduce the risk of a data breach, by implementing stronger and more reliable security programs, regardless of the likely increased upfront costs. The nine industry standards identified in the safe harbor law provide clear recommendations on the features and protections companies can use to develop their cybersecurity programs. These guidelines will help corporations develop systems that reduce the risk of a breach incident.
- **Allows mitigation of damages.** While implementing a cybersecurity program in accordance with recommended standards may not completely eliminate the risk of breach, doing so may reduce or eliminate damages in the event of a claim. The safe harbor helps corporations understand the types of considerations that are key to determining liability in advance, enabling organizations to proactively manage the potential costs and damages associated with data breaches.
- **Establishes a model for other state legislatures to develop corporate defenses.** The enactment of this safe harbor law provides a framework for other state lawmakers to define the scope of responsibility for and defenses to data breach events.

While data security will likely remain an ongoing priority for corporations for the foreseeable future, it is helpful to see that risk avoidance may have its own rewards as legislatures begin to address the interests of corporate America.

If your company is interested in discussing your current cybersecurity risks or potential liability exposure, please contact Jim Grove at Nicola, Gudbranson, & Cooper.

—James H. Grove
grove@nicola.com

Starlyn Priest, a law clerk at Nicola, Gudbranson & Cooper, assisted with this article.

Nicola, Gudbranson & Cooper LLC
25 West Prospect Avenue, Suite 1400
Cleveland, Ohio 44115

Tel: (216) 621-7227
Fax: (216) 621-3999

www.nicola.com