DATA PRIVACY AND CYBERSECURITY

AN OUNCE OF PREVENTION IS WORTH A POUND OF CURE: OHIO'S DATA PROTECTION ACT BECOMES EFFECTIVE NOVEMBER 1, 2018

by Sara H. Jodka, CIPP-US

Introduction

The Ohio Data Protection Act comes into effect November 1, 2018. The law is important for business data holders because it grants them a defense if a data breach occurs and the company can prove it had a CyberSecurity program in place that meets industry-recognized security frameworks.

The Law and Its Affirmative Defense

Unlike most laws, this one is a voluntary law that grants vigilant companies an incentive to meet a "higher level of security" through a number of measures, including: (1) having a written CyberSecurity Program; and (2) implementing strong technical privacy controls in place to protect data. It applies to any business that "accesses, maintains, communicates, or processes personal information [as defined in Ohio Revised Code 1349.19] or restricted information", which is defined as unencrypted information about an individual that can be "used to distinguish or trace the individual's identity."

Specifically, businesses who seek to take advantage of the defense available through the law, must implement a CyberSecurity program that:

- Is designed to protect the confidentiality and security of personal information;
- Protects against the unauthorized access to and acquisition of personal information that is likely to result in a material risk of fraud or identity theft; and
- Reasonably conforms to one of the following information security, cybersecurity or security assessment frameworks: CIS Critical Security Controls, ISO, IEC, NIST, FedRAMP, and some others.

If the business accepts credit/debit cards, the CyberSecurity programs must also comply with the Payment Card Industry's Data Security Standards (PCI-DSS).

And for businesses that are subject to other industry-specific privacy laws, such as healthcare business that have to comply with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH); and financial institutions that have to comply with the Gramm-Leach-Bliley Act (GLBA); and others, those businesses will have to comply with those laws to use the affirmative defense.

While law requires "reasonable" compliance with one of the listed frameworks, covered entities can tailor the scale and scope of their CyberSecurity to fit their own business needs as what would be appropriate, taking into account the following:

- The size and complexity of the business;
- The activities of the business;
- The sensitivity of personal information;
- The cost and availability of tools to improve cybersecurity; and
- The resources available to the business.

The Limits

The law, however, does have its limits. Most notably, it is only applicable to any "tort that alleges or relates to the failure to implement reasonable information security controls, resulting in a data breach", such as negligence and invasion of privacy. This means that the law does not apply to statutory or contract claims. Second, the affirmative defense is only available to claims brought under Ohio law or in Ohio courts.

On September 14, 2018, *Yujian Wang v. Daniel J. Lim, et al.*, was filed in the Franklin County Court of Common Pleas as Case Number 18CV007748 in the State of Ohio. The suit alleges that, during a home buying transaction, the title company never received $55,614.98 that the buyer had allegedly wired from his personal savings to his real estate agent. The lawsuit alleges that a hacker, posing as an escrow officer, sent a fraudulent email to the real estate agent asking for the plaintiff's email contact information. After receiving the email information, the hacker, posing as the real estate agent, sent wire instructions for the closing. The plaintiff wired the closing money to the hacker account pursuant to the fraudulent instructions and the money was lost and unavailable for the closing. Plaintiff sued the real estate agent and the real estate agency for negligence.

The case is in the initial stages so there has been no determination on liability, but it demonstrates the type of case that the affirmative defense would be relevant after the November 1, 2018 effective date of the law. Unfortunately, the affirmative defense is not available to the defendant real estate agency or agency.

The glaring issue then is that businesses that seek to take advantage of the new law will still have to prove their compliance via the appropriate standard of proof to trigger the affirmative defense. This sounds easier said than done, especially when you consider that most of the frameworks identified in the law don't have a standardized process of compliance or come with a certificate or gold star noting that the business is compliant. As such, compliance will be a litigated issue that will impact the cost of litigation defense.

Benefits

Overall, and with anything that encourages business to be more vigilant about their data privacy and cybersecurity, the law is a good start. While the actual ability of a business to use the affirmative defense may remain quite low and costly, the benefits of businesses taking stock in their data privacy and cybersecurity to meet the terms of the law is a very good thing. It is definitely a step in the right direction as data breaches can be, and have been, devastating for so many companies with the economic, brand, reputational, and other losses that come along with them.

Differences

The Ohio law is different than the consumer privacy initiatives that have been passed in California and Colorado in that those laws are punitive in nature and penalize businesses for failing to meet specific minimum data security requirements.

Takeaways

The law is far from perfect but it is a step in the right direction. For businesses, it creates an incentive to data privacy vigilance and preparedness. For data subjects, it may add another layer of protection over their personal information. For privacy in general, it keeps it on the forefront and, hopefully, puts the privacy initiatives identified in the law on the top of every Ohio companies' task list and budget conversations.

There are a number of sayings every privacy professional uses over and over again.

- "It's not *if* a data breach will happen, it's *when* a data breach will happen."
- "Think before you click".
- "Protect personal information. The identity saved could be your own."
- "If you suspect deceit, hit DELETE".

These are just a few. The Ohio law reminds me of another, and that is, "an ounce of prevention is worth a pound of cure." In this case, that pound of cure could amount to a lot of saved dollars and reputational harm a company would face if hit with a data breach.

This client alert is published by Dickinson Wright PLLC to inform our clients and friends of important developments in the field of Data Privacy and Cybersecurity law. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright attorney if you have specific questions or concerns relating to any of the topics covered in here.

FOR MORE INFORMATION CONTACT:

Sara H. Jodka, CIPP-US is Of Counsel in Dickinson Wright's Columbus office. She can be reached at 614.744.2943 or sjodka@dickinsonwright.com.

For more information about this law, Sara will be presenting on a panel discussion titled "Ohio's New Data Protection Law: Is SB 220 a Get-out-of-jail-free card?" with C Matthew Curtin, CISSP, Founder of Interhack and Gregory A. Tapocsi, Director of CyberOhio/Senior Assistant Attorney General – Consumer Protection, Cyber and Privacy Unit on November 28, 2018. Please refer to Infragard's website to register and for event details.