New data privacy laws continue to change the landscape for compliance

Dominic A. Paluzzi, James J. Giszczak | Friday, September 28, 2018

2018 has seen a whirlwind of states strengthening their data breach notification laws by expanding what qualifies as personal information and shortening time frames for reporting a breach.

Louisiana

Louisiana is one of the latest to jump on the bandwagon. The Louisiana governor signed an amendment to the state's data breach notification law, which took effect on Aug. 1.

Key changes to the Louisiana law are a shortening of the time frame to report a breach to 60 days from discovery of the breach and an expansion of the definition of 'personal information' to include a state identification card number, passport number, and "biometric data," including fingerprints, voiceprints, eye retina or iris, or other unique biological characteristics used to authenticate an individual's identity when accessing a system or account.

But perhaps most notable is Louisiana's new emphasis on reasonable security practices and data destruction. Specifically, Louisiana implemented requirements for businesses in the state to:

- Implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification or disclosure.
- Take all reasonable steps to destroy or arrange for the destruction of the records within its custody or control containing personal information that is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

While it's yet to be seen whether implementing reasonable security practices will help Louisiana companies defend against data breach lawsuits, other states like New

York and Ohio have specifically considered this beneficial arrangement.

Ohio

Ohio recently enacted a liability safe harbor for entities maintaining specific cybersecurity programs. On Aug. 3, the Ohio governor signed Senate Bill No. 220, the "Data Protection Act," which encouraged businesses to voluntarily adopt strong cybersecurity controls to protect customer data. If the businesses are in substantial compliance with contemplated cybersecurity frameworks, they are entitled to a "legal safe harbor" - an affirmative defense to tort claims related to a data breach stemming from alleged failures to adopt reasonable cybersecurity measures. The necessary size and scope of a cybersecurity program required to trigger the legal safe harbor is not one-size-fits-all. Instead, business specific factors will be considered such as (a) the size, complexity and nature of the business, (b) the level of sensitivity of the personal information it possesses, (c) the cost and availability of tools to improve security and reduce vulnerabilities, and (d) the resources the business has at its disposal to spend on cybersecurity.

New York

New York is considering a similar bill to Ohio's. In November 2017, the New York Attorney General introduced the Stop Hacks and Improve Electronic Data Security Act, also known as the SHIELD Act. The bill would require any business holding sensitive data of New Yorkers, whether they do business in New York or not, to adopt "reasonable" administrative, technical and physical safeguard for sensitive data. The bill provides companies with a strong incentive to go beyond the bare minimum and obtain independent certification that their data security measures meet the highest standards, as companies who do so will receive safe harbor from state enforcement actions. The SHIELD Act also expands the types of data that triggers reporting requirements to include username and password combinations, biometric data and HIPAA-covered health data. The bill is currently in committee and has not been voted on in the Senate or Assembly.

Cybersecurity continues to be a focus for states and regulatory bodies across the nation, as evidenced by the rapidly changing patchwork of state data breach notification laws. Are you in a position to take advantage of these safe harbors? Now is the time to update your data security procedures and incident response plans to do so. McDonald Hopkins will continue to monitor this space to provide the most up-to-date information available. For questions or information on data privacy and cybersecurity, or for an assessment of areas of vulnerability, please contact one of the attorneys below.

Dominic A. Paluzzi

James J. Giszczak