WEBSTER, CHAMBERLAIN & BEAN, LLP | NONPROFIT ALERT

February 25, 2020

NEW YORK'S SHIELD ACT – IT'S COMPLIANCE TIME

The New York Stop Hacks and Improve Electronic Security Act[1] ("SHIELD Act") aims to reduce the likelihood of data breaches by requiring robust data security programs. To reduce the risk of a data breach, by **March 21, 2020**, any person or business (including nonprofit organizations) that owns or licenses private information of a resident of New York shall develop a data security program.[2]

The SHEILD Act provides details about a data security program. The SHIELD Act identifies reasonable safeguards such as: designating one or more employees to coordinate the security program, training and managing employees in the security program practices and procedures, selecting service providers capable of maintaining safeguards, protecting against unauthorized access to or use of private information and disposing of private information within a reasonable amount of time by erasing electronic media.[3]

What are some other key provisions? As noted by the New York Attorney General,[4] the SHIELD Act:

- Expands the scope of information subject to the current data breach notification law to include biometric information, email addresses, and corresponding passwords or security questions and answers;
- Broadens the definition of a data breach to include unauthorized "access" to private information from the current "acquired" standard;
- Applies the notification requirement to any person or entity with private information of a New York resident, not just to those that conduct business in New York State;
- Updates the notification procedures companies and state entities must follow when there has been a breach of private information; and
- Creates reasonable data security requirements tailored to the size of a business.

What does this mean for nonprofits? To start, consider whether your organization possesses "private information" of a New York resident. Next, assess your data security programs, including your policies, procedures, and staffing decisions, in consideration of the SHIELD Act and any other applicable laws, such as the European Union General Data Protection Regulation and the California Consumer Privacy Act. In developing and implementing a SHIELD Act compliant data security program, it must incorporate "reasonable safeguards" in three separate ways: administratively, technically, and physically.

Are there any exceptions to applicability? Small businesses, such as those with fewer than 50 employees, still must comply with the SHIELD Act. However, they have some flexibility regarding data security measures, but not breach notification. Note that an exception to breach notification exists under some circumstances for inadvertent exposure.

What if you do not comply with the SHIELD Act? If the above applies to you, you need to comply! Although the SHIELD Act does not confer a private right of action, the New York Attorney General is authorized to impose significant fines.

* * *

Lauren L. Dockter | ldockter@wc-b.com | 202-785-9500

David S. Lieberman | dlieberman@wc-b.com | 202-785-9500

---

[1] Senate Bill S5575B, available at https://www.nysenate.gov/legislation/bills/2019/s5575.
[2] N.Y. Gen. Bus. L. § 899-BB Data Security Protections, available at https://www.nysenate.gov/legislation/laws/GBS/899-BB.
[3] For additional information on reasonable security measures see the California Data Breach Report dated February 2016, available at https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.
[4] Attorney General James Applauds Passage Of The Shield Act, available at https://ag.ny.gov/press-release/2019/attorney-general-james-applauds-passage-shield-act.