Ellenoff Grossman & Schole LLP

New Privacy Law Requirements About to Go Live in New York

While New York's Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act") was signed into law on July 25, 2019, its implementation is rolled out in two parts. The first part, involving enhanced requirements related to breach notifications, went into effect on October 23, 2019. The second part, involving enhanced data security requirements, is set to go live on March 21, 2020.

The SHIELD Act modifies and enhances requirements under the earlier New York State Information Security Breach and Notification Act. The SHIELD Act extends the earlier Act to cover any entity, whether located in New York or not, that owns or licenses private information about New York residents. Further, the SHIELD Act extends the definition of private information to include data such as, driver's license and non-driver ID card numbers, financial account information and biometric information (e.g., fingerprints, retina images).

It's also important for clients to note that a breach does not require any data to be actually acquired by a third-party. Unauthorized access alone can be a breach, triggering a potential notification requirement under the SHIELD Act. This would include records accessed by unauthorized individuals, even when no information was actually copied or otherwise retained by the unauthorized individuals.

There is an exception to the notice requirements for inadvertent disclosures by persons authorized to access private information. However, in such cases, the company must reasonably determine that such inadvertent disclosure will not likely result in misuse of such information or financial or emotional harm to the affected person(s). The determination must be made in writing and maintained for at least five years, and if the incident involves over five hundred New York residents, the written determination must be provided to the NY Attorney General within ten days after completed.

There are also exceptions to the notice provisions to residents of New York where the notice is already being given under other state or federal rules or regulations, such as HIPAA, HITECH or Title V of the Gramm-Leach-Bliley Act. However, notice is still required to be given to the Attorney General in most cases, as well as potentially others (e.g., State Police).

With the enhanced data security requirements of the SHIELD Act going into effect as of March 21, 2020, it is important for entities in possession of information pertaining to residents of New York to review and update their data security and compliance programs. Even for entities that have ensured compliance with other privacy and data security laws, such as CCPA, HIPPA, HITECH and GDPR, it is important to make sure that those policies and implementations check all the boxes of the SHIELD Act as well. Most notably, the provisions of the Act related to notifications that need to be sent in relation to breaches may differ from an entities current procedures, and should be addressed to ensure compliance. Review of these policies and implementations should likely be verified by counsel as well to ensure compliance. Our Firm has a longer article on this matter that can be found here - ***New Privacy Law Requirements About to Go Live in New York*.**

James M. Smedley, Esq.

1345 Avenue of the Americas, 11th Fl., New York, NY 10105
Direct Dial (215)-315-3582
jsmedley@egsllp.com | www.egsllp.com