COWAN LIEBOWITZ & LATMAN

Privacy Law Alert – New York State Enacts a New Electronic Data Privacy Protection Law

October 8, 2019

By Danielle J. Siegel

In July 2019, New York State passed the *Stop Hacks and Improve Electronic Data Security Act*, N.Y. G.B.L. § 899 *et seq.* (the "SHIELD Act"), which goes into effect on March 21, 2020.

The SHIELD Act is meant to improve consumer data security by expanding the definition of protected data, increasing notification requirements, and requiring substantive data security controls. The SHIELD Act will make New York's data protection laws consistent with those of other states, including Massachusetts and Florida.

Who is Covered?

The SHIELD Act expands New York's electronic data protection to cover any person or business that owns, licenses, trades in, or otherwise affects the private information of any New York resident, regardless of whether the business is located in New York.

However, small businesses with fewer than 50 employees and less than three million dollars in gross revenues in each of last three fiscal years, *or* less than five million dollars in total year-end assets, may choose to create their own data security programs that may be less burdensome than the program mandated by the statute as long as their programs use safeguards that are reasonable based on the size, complexity, type, and scope of the business. For example, a small restaurant could create a much simpler data protection and notification program, while a technology-based startup that deals in information gathering, even if small, would need a more complicated program. Larger companies must comply strictly with all of the Act's safeguards and requirements.

What is Protected?

The current definition of private information is

- personal information ("any information concerning a natural person which, because of name, number, personal mark or other identifier, can be used to identify such natural person") that is

- used in conjunction with a person's social security number, driver's license number or other account number in combination with security codes, access codes or passwords which would allow access to a person's account.

Under the SHIELD Act, this definition of private information is expanded to include financial account numbers that can be used by themselves to access accounts, including credit card numbers; usernames or email addresses and either passwords or security questions and answers that would allow access to an online account; biometric information used to authenticate someone's identity; and unsecured HIPAA-protected health information.

What Security is Required?

Compliance with HIPAA, the Gramm-Leach-Bliley Act (also known as the Financial Security Modernization Act), and/or the New York State Department of Financial Services Cybersecurity Regulation that became fully effective on March 1, 2019, is sufficient to meet the requirements of the SHIELD Act. Entities that comply with these statutory requirements are considered "Compliant Regulated Entities" under the SHIELD Act, which means, in part, that they do not need to comply with additional notification requirements, although they still need to inform the New York State Attorney General and any other relevant government agencies when a breach has occurred.

A company covered by the SHIELD Act must either be a "Compliant Regulated Entity," or it may implement a data security program including reasonable administrative, technical, and physical safeguards, as identified in the statute. These safeguards may include designating employees to coordinate the data protection program, identifying reasonably foreseeable internal and external risks to the entity, and updating its company security programs as needed to ensure it remains effective and compliant.

Breach Notification Requirements

Additionally, breach notifications will have to include contact information for state and federal agencies and breached companies will have to ensure that people whose data was impacted, the New York State Attorney General, and any other required party or government agency receives proper notice of the breach.

Penalties

Although the SHIELD Act does not allow private citizens to sue for the loss of their data, the New York Attorney General can bring enforcement actions that can result in potentially substantial civil penalties. Courts may award actual damages for failure to comply with the Act's data breach notification requirements. Additionally, if those violations are knowing and reckless, courts may impose penalties of either $5,000 or up to $20 per instance with a limit of $250,000, whichever is higher. For violations of the reasonable safeguard requirements, courts may impose penalties of not more than $5,000 per violation.

Takeaway

The SHIELD Act goes into effect in less than five months, so covered entities should start now to take steps to comply.