Published on *The National Law Review* https://natlawreview.com

New York Cybersecurity Upgrades: Are You Ready?

Article By:

Kristin L. Bryan

This spring, New York's cybersecurity landscape shifts dramatically as certain provisions of New York's Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act") take effect. The SHIELD Act, 2019 N.Y. Ch. 117, which was signed into law by Governor Cuomo on July 25, 2019, modifies existing data breach law to expand the definition of "Private Information" and imposes new substantive cybersecurity requirements.

Among other provisions, it requires companies by March 21, 2020, to adopt cybersecurity programs reminiscent of the Written Information Security Program required under Massachusetts law for entities that own or license the personal information of Massachusetts residents. Additionally, with the SHIELD Act's coverage extending to biometric data, New York joins the handful of states that have acted in this area (the others being Illinois, Texas and Washington).

This post provides an overview of the cybersecurity requirements of the SHIELD Act in light of its looming compliance deadline, excluding modifications to the New York breach statute that have already taken effect. It also discusses the NY Department of Financial Services Cybersecurity Regulation to the extent it relates to the SHIELD Act.

As the privacy landscape gets more complex with upcoming deadlines under the SHIELD Act, organizations covered should ensure their current practices comply with what is required and represent industry best practices. Our team is prepared to assist every step of the way.

What is the SHIELD Act?

The SHIELD Act expanded the scope of data breach notifications under New York law, for example, by covering biometric data. Those provisions have been in force since fall 2019. The SHIELD Act also mandates cybersecurity protections for Private Information. Those new cybersecurity requirements take effect in March.

Subject to certain exceptions, the cybersecurity provisions of the SHIELD Act mandates that any person or business that owns or licenses the computerized Private Information of any New York resident, which is broadly defined to encompass a range of information that could be used to identify a person when combined with other statutorily specified data elements, to maintain "reasonable safeguards" to protect this information.

The SHIELD Act applies to all organizations that process the Private Information of New York residents, regardless of whether the organizations are domiciled in New York State. Notably, there is no minimum threshold for the statute to apply – meaning that the Private Information of even a single New York resident triggers the SHIELD Act's provisions.

What information is covered under the SHIELD Act's data security requirements?

The SHIELD Act applies to Private Information, defined to mean either:

(i) Any **unencrypted (or encrypted with a key that has been accessed)** information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person (**"personal information") in combination with any one or more of the following data elements**:

- Social security number;
- Driver's license number or non-driver identification card number;
- Account number, credit or debit card number (in combination with information that would permit access to an individual's financial account);
- Account number, credit or debit card number (if circumstances exist wherein such number could be used to access an individual's financial account without additional information);
- Biometric information (meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity),

or

(ii) A user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

Private Information excludes publicly available information that is lawfully made available to the general public from federal, state, or local government records.

What are the SHIELD Act's cybersecurity requirements?

The SHIELD Act does not provide a comprehensive outline of what is required to provide "reasonable" security. But the law does specify a range of measures, encompassing administrative, technical, and physical safeguards that are sufficient. This includes:

- **Implement reasonable administrative safeguards**: This encompasses measures such as conducting a cybersecurity risk assessment, designating an employee responsible for cybersecurity, continuously updating risk assessment and necessary security measures, selecting service providers capable of providing appropriate safeguards and training and

managing all employees on the security program.

- **Implement reasonable technical safeguards**: This encompasses measures sufficient to identify and assess risks in network and software design and information processing, transmission and storage. It also includes detecting and responding to attacks or system failures and regularly testing and refining the technical security of the system.

- **Implement reasonable physical safeguards**: This encompasses measures concerning information storage and disposal, detecting and responding to intrusions, protecting against unauthorized access to or use of Private Information and ensuring the timely and secure disposal of data that is no longer needed for business purposes.

These standards are similar to existing regulations in specific areas like finance (under the FTC's Safeguards Rule). One way to think about the SHIELD Act is that it takes sector-specific cybersecurity requirements and applies them broadly to all businesses (to the extent they have Private Information as defined in the statute).

Are there exemptions to the SHIELD Act's cybersecurity requirements?

Entities required to comply and in full compliance with the following cybersecurity regimes are automatically "deemed to be in compliance" with the SHIELD Act's "reasonableness" standard:

- The federal Gramm-Leach-Bliley Act ("GLBA");

- The federal healthcare standards ("HIPAA/HITECH");

- The NYDFS Cybersecurity Regulation; or

- "[A]ny other data security rules and regulations" promulgated by the federal or New York State government.

Special rules apply to "small business" with fewer than 50 employees, less than $3 million in annual revenue for the preceding three years, or less than $5 million in assets. Their security programs are deemed compliant if they are appropriate for the size and complexity of the business, but is still subject to the reasonable security requirement. What is reasonable under the circumstances is informed in part by the sensitivity of the Private Information the small business collects from or about consumers.

How will the SHIELD Act be enforced?

The SHIELD Act provides the New York Attorney General enforcement authority pursuant to Section 349 of the General Business Law for any covered person or entity found to have failed to implement reasonable cybersecurity – even in the absence of a data breach. The state attorney general may seek injunctive relief and civil penalties (including up to $5,000 per violation) under Section 350-d for violation of the data security standards.

Failure to maintain adequate cybersecurity under the SHIELD Act may also give rise to litigation, including potential class actions. The SHIELD Act expressly does not create a private right of action,

but it says that any violation of the statute “shall be deemed to have violated” Section 349. Under Section 349 (which is New York’s general consumer deceptive practices law), a person injured by a violation can sue for an injunction or for actual damages. We expect to see litigation about whether the SHIELD Act’s reference to Section 349 also encompasses the Section 349 private cause of action. In addition, private plaintiffs may also try to work SHIELD Act arguments into unfair or deceptive practices claims under other state laws, by contending that cybersecurity that does not meet the SHIELD Act standard constitutes a violation of law that is obviously unfair (and could be deceptive if a company has made representations about its privacy practices).

National Law Review, Volumess X, Number 36