September 26, 2019

The New York Shield Act:
Businesses Face New Data Security Compliance Deadlines

Large, high profile data breaches involving consumer information have been part of the news cycle for a decade and more. Everything from the world's largest companies to government agencies and local businesses have been victims of hacks, employee misconduct, and accidental disclosures. Legislatures are responding. The SHIELD Act is New York's latest response.

In 2005, New York passed the Information Security Breach and Notification Act. The SHIELD Act amends the 2005 law, modernizing and expanding upon it. The SHIELD Act takes effect in two parts. The first part, concerning data breach notification, takes effect October 23, 2019, and the second part, concerning data security, takes effect March 21, 2020. The prior 2005 law, which also required breach notification, remains in effect until October 23, 2019.

Breach Notification

The SHIELD Act requires that New York residents be notified of any unauthorized access to or acquisition of computerized data that compromises the security, confidentiality, or integrity of their private information maintained by any person or business subject to the Act (hereinafter a "breach"). The New York Attorney General, New York Department of State, and the state police must also be notified. Consumer reporting agencies must also be notified in the case of large breaches.

The SHIELD Act applies to any person or business that owns or licenses computerized data containing private information. Persons and businesses that maintain but do not own such private information must notify the owner or licensee of such computerized data so that appropriate notifications can be made. Several features of the SHIELD Act are worth noting.

Private Information – Private information is specifically defined by the Act and must either (1) include both an identifier and an additional data element (such as a social security number, account access information, driver's license number, or biometric information) or (2) be a user name and password (or security question information) for an online account. Generally, encrypted information that has not been compromised is exempt.

Extraterritorial Effect – More than one observer has noted that the law obligates any person or business anywhere in the world if they own, license, or maintain the private information of New York residents. The law purports to apply to any person or business so long as they own or license computerized data containing the private information of New York residents. Undoubtedly, constitutional jurisdictional limitations will blunt the extraterritorial effect to some degree.

Enforcement – The Act permits the attorney general to bring an action against any person or business that violates the Act and to recover damages on behalf of the affected New York residents as well as, in cases of reckless or knowing violation, civil penalties up to $250,000. The statute of limitations is lengthy—up to six years from the date the breach was discovered by the responsible person or business. The Act tolls the statute indefinitely if there are efforts to hide the breach.

Lawsuits - Courts generally have refused to infer any private right for consumers to sue for a failure to adhere to the 2005 law. There is no indication from the language of the SHIELD Act that the legislature intended to change that interpretation with respect to the breach notification part of the Act. The right to enforce the Act should lie exclusively with the attorney general. At least one court, however, permitted a lawsuit premised on the 2005 law to proceed under the guise of a deceptive business practices lawsuit under New York General Business Law ("GBL") § 349. If your business provides consumers with a privacy policy or statement of any kind, it should be drafted carefully to avoid lawsuits from consumers.

Coordination with Law Enforcement – The Act requires that notification to New York residents occur only after law enforcement has determined that notification will not compromise any criminal investigations.

Exceptions – The Act does not require duplicate notice to the affected persons where the person or business makes notice pursuant to an enumerated list of other laws and regulations. The Act also does not require notice to the affected persons where the person or business documents a determination that the breach was inadvertent, made by a person authorized to access private information, and otherwise low risk (as defined by the Act). Businesses should be cautious, however, as the above exceptions do not entirely excuse the obligation to report to certain

agencies. Another exception applies to good faith access to or acquisition of private information by an employee or agent of the business (so long as it does not involve an unauthorized disclosure).

Health Care Entities – The Act requires that any breach that is reportable to the U.S. Department of Health and Human Services as a HIPAA breach also be reported to the attorney general.

Security

The Act adds a new security requirement that was not part of the 2005 law. Under the security requirement, businesses that are subject to the Act must implement a security program. The Act defines the minimum requirements of a compliant security program and takes a cue from HIPAA, breaking the minimum security requirements into administrative, technical, and physical safeguards. Violations are once again enforced by the attorney general and include the possibility of civil penalties.

Lawsuits – The security part of the Act specifically states that it does not afford a private cause of action. Creative plaintiffs, therefore, should have a more difficult time using the security requirement as a basis for private lawsuits; however, the Act also specifically provides that a violation of the security requirement is an automatic violation of GBL § 349 (deceptive business practices).

Flexibility – The security requirement was drafted to permit a fair amount of flexibility depending on the particularities of the business involved, including the size of the business and the type of private information maintained. Smart business managers will be careful not to mistake flexibility for permission to be lax.

Compliant Regulated Entity Exception – The Act, in a small demonstration of business mindedness, deems persons and businesses that are already compliant with any of a list of enumerated privacy laws and regulations (including HIPAA and Gramm-Leach-Bliley) as having met the security program requirement.

In Summary

As with any law, there are nuances and additional requirements in the statute that could not be practically summarized here, and the application of these laws to your situation or business requires careful analysis. While entities that are already experienced with privacy law compliance, such as those in the health care or financial sector, will have a leg up when it comes to compliance with the security requirement, even those entities should evaluate whether they are compliant with the breach notification provisions of the Act and whether they will fall within the compliance regulated entity exception to the

security requirement of the Act. All businesses should also review their privacy and security policies and practices and vendor agreements, including HIPAA business associate agreements, to ensure they take account for obligations created by the SHIELD Act.

If you have any questions about this Legal Briefing, please contact any attorney of our Firm at 585-730-4773.