THE
NATIONAL LAW REVIEW

New York Enacts the SHIELD Act

jackson lewis.

Article By
Joseph J. Lazzarotti
Damon W. Silver
Mary T. Costigan
Maya Atrakchi
Jackson Lewis P.C.
Workplace Privacy Blog

- Communications, Media & Internet
- Election Law / Legislative News

- New York

Friday, July 26, 2019

On Thursday, New York Governor Andrew Cuomo signed into law the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), sponsored by Senator Kevin Thomas and Assemblymember Michael DenDekker. The SHIELD Act, which amends the State's current data breach notification law, imposing more expansive heightens data security and data breach notification requirements on companies, in the hope of to ensuring better protection for New York residents from data breaches of their private information. The SHIELD Act takes effect on March 21, 2020. Governor Cuomo also signed into law the Identity Theft Prevention and Mitigating Services Act that requires credit reporting agencies that face a breach including Social Security numbers to provide five years of identity theft prevention and mitigation services to affected consumers, and allows for consumers, at no cost, the right to freeze their credit. This law becomes effective in 60 days.

Below are several FAQs highlighting key features of the SHIELD Act:

What is Private Information under the SHIELD Act?

Unlike other state data breach notification laws, New York's original data breach notification law included definitions for "personal information" and "private information." The current definition of "personal information" remains: "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person." However, the SHIELD Act expands the definition of "private information" which sets forth the data

elements that, if breached, could trigger a notification requirement. Under the amended law, "private information" means either:

- *personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired:*
  - *social security number;*
  - *driver's license number or non-driver identification card number;*
  - *account number, credit or debit card number, in combination with any required security code, access code, password or other 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 identifying information, security code, access code, or password; or*
  - *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*
- *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.*

It is worth mentioning that the SHIELD Act's expansive definition of "private information" is still not as broad as the definition of the analogous term under the laws of other states. For example, Illinois, Oregon, and Rhode Island have expanded their definitions to include not only medical information, but also certain health insurance identifiers.

How has the term "breach of security of the system" changed?

The SHIELD Act alters the definition of "breach of the security of the system" in two significant ways. First, as discussed above, it expands the categories of information that could result in a breach of the security of the systems. And second, it broadens the circumstances that qualify as a "breach" by including within the definition of that term incidents that involve "access" to private information, regardless of whether they resulted in "acquisition" of that information. Under the old law, access absent acquisition did not qualify as a breach. Notably, the SHIELD Act retains the "good faith employee" exception to the definition of "breach," and also provides several factors for determining whether there has been unauthorized access to private information, including *"indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person."*

Are there any substantial changes to data breach notification requirements? And who must comply?

Any person or business that owns or licenses computerized data which includes private information of New York residents must comply with breach notification requirements, regardless of whether the person or business conducts business in

New York. That said, there are several circumstances which would exempt a business from the breach notification requirements. For example, notice is not required if "exposure of private information" was an "inadvertent disclosure and the individual or business reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials". Further, businesses that are already regulated by and comply with data breach notice requirements under certain applicable state or federal cybersecurity laws (*e.g.,* HIPAA, NY DFS Reg 500, Gramm-Leach-Bliley Act) are not required to further notify affected New York residents, however, they are still required to notify the New York attorney general, the New York State Department of State Division of Consumer Protection, and the New York State Division of the State Police.

What are the "reasonable" data security requirements? And who must comply with them?

As with the notification requirements, the SHIELD Act requires that any person or business that owns or licenses computerized data which includes private information of a resident of New York must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information. Again, businesses in compliance with laws like HIPAA and the GLBA are considered in compliance with this section of the law. Small businesses are subject to the reasonable safeguards requirement, however safeguards may be *"appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers."* A small business is considered any business with fewer than fifty employees, less than $3 million in gross annual revenue in each of the last 3 years, or less than $5 million in year-end total assets.

The law provides examples of practices that are considered reasonable administrative, technical and physical safeguards. For example, risk assessments, employee training, selecting vendors capable of maintaining appropriate safeguards and implementing contractual obligations for those vendors, and disposal of private information within a reasonable time period, are all practices that qualify as reasonable safeguards under the law.

Are there penalties for failing to comply with the SHIELD Act?

The SHIELD Act does not authorize a private right of action, and in turn class action litigation is not available. Instead, the attorney general may bring an action to enjoin violations of the law and obtain civil penalties. For data breach notification violations that are *not* reckless or knowing, the court may award damages for actual costs or losses incurred by a person entitled to notice, including consequential financial losses. For knowing and reckless violations, the court may impose penalties of the greater of $5000 dollars or up to $20 per instance with a cap of $250,000. For reasonable safeguard requirement violations, the court may impose penalties of not more than $5,000 per violation.

Conclusion

The SHIELD Act has far reaching effects, as any business that holds private information of a New York resident – regardless of whether that organization does business in New York – is required to comply. “The SHIELD Act will put strong safeguards in place to curb data breaches and identity theft,” said Justin Brookman, Director of Privacy and Technology Policy for Consumer Reports. The SHIELD Act signifies how seriously New York, like other states across the nation, is taking privacy and data security matters. Organizations, regardless of their location, should be assessing and reviewing their data breach prevention and response activities, building robust data protection programs, and investing in written information security programs (WISPs).