Legal Update Article

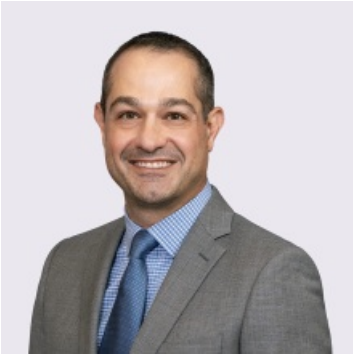
New York Enacts SHIELD Act, Adding Data Security Requirements and Strengthening Data Breach Requirements

By Joseph J. Lazzarotti, Jason C. Gavejian, Mary T. Costigan & Damon W. Silver

July 26, 2019

Meet the Authors

Joseph J. Lazzarotti
Principal
908-795-5205
Joseph.Lazzarotti@jacksonlewis.com



Jason C. Gavejian
Office Managing Principal
908-795-5139
Jason.Gavejian@jacksonlewis.com

New York has enacted the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) to amend the state's data breach notification law to impose more expansive data security and data breach notification requirements on companies. The move aims to ensure New York residents are better protected against data breaches of their private information.

Governor Andrew Cuomo signed the SHIELD Act, which was sponsored by Senator Kevin Thomas and Assemblymember Michael DenDekker, on July 25, 2019. The SHIELD Act takes effect on March 21, 2020.

Governor Cuomo also signed the Identity Theft Prevention and Mitigation Services Act on July 25, 2019. This new law requires credit reporting agencies that have experienced a breach involving Social Security numbers to provide five years of identity theft prevention and mitigation services to affected consumers. It also gives consumers the right to freeze their credit at no cost. This law becomes effective on September 23, 2019, 60 days after enactment.

Private Information under 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." "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 explains the data elements that, if breached, could trigger a notification requirement.

Under the amended law, "private information" means:

• 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

Mary T. Costigan
Principal
908-795-5135
Mary.Costigan@jacksonlewis.com

Damon W. Silver
Principal
(212) 545-4063
Damon.Silver@jacksonlewis.com

Related Services

Privacy, Data and Cybersecurity
Technology

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 email address in combination with a password or security question and answer that would permit access to an online account.

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

"Breach of Security of the System"

The SHIELD Act revises the definition of "breach of the security of the system" in two significant ways. First, it broadens the circumstances that qualify as a "breach" by including incidents that involve "access" to private information, regardless of whether they resulted in "acquisition" of that information. Currently, mere access, without acquisition, did not qualify as a breach. The SHIELD Act also adds 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."

Second, the SHIELD Act's expansion of the definition of private information effectively expands the types of situations covered that could result in a breach of system security. The SHIELD Act retains the "good faith employee" exception to the definition of "breach." That exception provides that an employee's good faith access to or acquisition of private information for purposes of the business does not constitute a breach if the private information is not used or subject to unauthorized disclosure.

Changes to Data Breach Notification Requirements

The SHIELD Act provides that any person or business that owns or licenses computerized data that includes New York residents' private information must comply with the breach notification requirements, *regardless of whether the person or business conducts business in New York.*

A business may be exempt from the breach notification requirements under certain circumstances. 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 already are regulated by and comply with data breach notice requirements under certain applicable state or federal cybersecurity laws *(e.g.,* HIPAA, NY DFS Reg. 500, and Gramm-Leach-Bliley Act [GLBA]) need not further notify affected New York residents; however, these businesses are still required to notify the state Attorney General, Department of State Division of Consumer

Protection, and Division of the State Police.

"Reasonable" Data Security Requirements

As with the notification requirements, the SHIELD Act provides that any person or business that owns or licenses computerized data that includes a New York resident's private information must develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information. Businesses in compliance with such laws as HIPAA and the GLBA are considered in compliance with this requirement.

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 any business with fewer than 50 employees, less than $3 million in gross annual revenue in each of the last three years, or less than $5 million in year-end total assets.

The law provides examples of practices 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 are all practices that qualify as reasonable safeguards.

Penalties

The SHIELD Act does not authorize a private right of action and 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, a 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, a court may impose penalties of the greater of $5,000 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.

Implications

The SHIELD Act has far-reaching effects. Any business that holds a New York resident's private information — 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, state Director of Privacy and Technology Policy for Consumer Reports.

The SHIELD Act signifies how seriously New York, likeother 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), among other things.

Jackson Lewis attorneys are available to answer inquiries on the SHIELD Act and other laws and assist businesses in their compliance efforts.

Focused on employment and labor law since 1958, Jackson Lewis P.C.'s 1,000+ attorneys located in major cities nationwide consistently identify and respond to new ways workplace law intersects business. We help employers develop proactive strategies, strong policies and business-oriented solutions to cultivate high-functioning workforces that are engaged and stable, and share our clients' goals to emphasize belonging and respect for the contributions of every employee. For more information, visit https://www.jacksonlewis.com.