BRACEWELL

INSIGHTS

New York's Deadline to Comply With New Data Privacy Law Fast Approaching

March 5, 2020

By: ***David A. Shargel***

The Stop Hacks and Improve Electronic Data Security Act (known as the SHIELD Act), signed into law by Governor Cuomo last year, comes into full effect on March 21, 2020. The Act's expansive reach requires businesses in New York, as well as those outside the state that maintain New York residents' private information, to take concrete steps intended to prevent data breaches. A failure to comply with the new data security requirements raises the specter of enforcement actions by the New York State Attorney General, whose powers are significantly expanded under the SHIELD Act. The SHIELD Act brings New York State into the fold with a growing number of states that have recently enacted legislation or strengthened existing laws aimed at protecting consumer data security and privacy, making it imperative for companies to review, assess, and enhance their compliance capabilities.

Signed by Governor Cuomo on July 25, 2019, the SHIELD Act was designed to become effective in two phases. First, effective October 23, 2019, the Act significantly revised § 899-aa of the General Business Law (GBL), including by expanding the definition of "private information" to include account numbers, biometric information, and email addresses (when combined with a password or security question and answer).

Second, the SHIELD Act added a new § 899-bb to the GBL, which sets forth formal data security requirements tailored by business size, as well as an enforcement provision for non-compliance. Due to the nature of the affirmative requirements set forth in new § 899-bb, businesses were given until March 21, 2020 to achieve compliance. By that time, new GBL § 899-bb(2)(a) requires that "[a]ny person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data."

The steps necessary to comply with this mandate depend on business size and type. Any business other than a "small business," as defined in GBL § 899-bb(1) and discussed below, will be deemed "in compliance" if it either (i) is a "compliant regulated entity," as defined in GBL § 899-bb(1), such as businesses regulated by the federal Gramm-Leach-Bliley Act, certain financial services companies, and entities subject to HIPAA; or (ii) implements a data security program that includes certain "reasonable" administrative, technical, and physical safeguards, as follows:

- **Administrative Safeguards** – these include designating one or more employees to coordinate the security program; identifying reasonably foreseeable internal or external risks; assessing the sufficiency of safeguards in place to control identified risks; training and managing employees in security program practices and procedures; selecting service providers capable of maintaining appropriate safeguards (and requiring those safeguards by contract); and adjusting the security program in light of business or new circumstances. GBL § 899-bb(2)(b)(ii)(A).

- **Technical Safeguards** – these include assessing risks in network and software design; assessing risks in information processing, transmission, and storage; detecting, preventing, and responding to attacks or system failures; and regularly testing and monitoring the effectiveness of key controls, systems and procedures. GBL § 899-bb(2)(b)(ii)(B).

- **Physical Safeguards** – these include assessing risks of information storage and disposal; detecting, preventing, and responding to intrusions; protecting against unauthorized access to or use of private information during or after the collection, transportation, and destruction or disposal of the information; and disposing of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed. GBL § 899-bb(2)(b)(ii)(C).

Under GBL § 899-bb(2)(c), a "small business"—defined by the Act as a company with less than 50 employees, less than $3 million in gross annual revenue or less than $5 million in year-end total assets— will be deemed in compliance if its security program contains reasonable administrative, technical, and physical safeguards that are "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."

Significantly, GBL § 899-bb not only creates affirmative data security requirements, but provides a powerful enforcement mechanism for noncompliance. Under GBL § 899-bb(2)(d), any person or business that fails to comply with the requirements of GBL § 899-bb(2) shall be deemed to have violated GBL § 349, which makes deceptive acts or practices unlawful. This provision authorizes the Attorney General to bring an action to enjoin violations, and to obtain civil penalties of $5,000 per violation, as set forth in GBL § 350-d (civil penalties). Section 899-bb(2)(e) explicitly states that a breach of the data security requirements does not create any private right of action.

As mentioned above, GBL § 899-bb brings the SHIELD Act into full effectiveness. While the new data security requirements are a key piece of the legislation, the Act's revisions to GBL § 899-aa have already taken effect. These revisions include an expanded definition of "private information," an expanded definition of data "breach," updates to the notification system for discovered breaches, broadened territorial application to any person or business which owns or licenses computerized data that includes private information of a resident of New York (previously, it required such person or business conduct business in New York), and the application of many of these new definitions to state government agencies and entities.

The SHIELD Act brings New York State into the fold along with states such as California, Nevada, Maine, Massachusetts, New Jersey, Maryland, Oregon, Texas, and Washington that have recently enacted legislation aimed at protecting consumer data security and privacy.

With March 21 quickly approaching, companies both in New York and those maintaining New Yorkers' "private information" should review, assess, and enhance their compliance with the SHIELD Act, as noncompliance may prove costly.