Legislative Changes to New York's Data Breach Notification Laws

August 22, 2019 | **CLIENT ALERTS**

On July 25, 2019, Governor Andrew Cuomo signed legislation, The Stop Hacks and Improve Electronic Data Security Act (the "SHIELD" Act), that amends Section 899-aa of the New York General Business Law and adds a new section, Section 899-bb. This new law will take effect on March 21, 2020.

To view the amended Section 899-aa and the new Section 899-bb, click here .

Section 899-aa of the New York General Business Law controls the disclosures of any breach of data to New York residents.

To keep up with fast paced technological advancements, the SHIELD Act will impose stricter obligations on those who own or license computerized private data. Specifically, it requires a more stringent protocol when an individual's private information was, or is reasonably believed to have been, accessed without authorization.

The SHIELD Act redefines "Private Information" under Section 399-aa as "either: (i) 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: (1) social security number; (2) driver's license number or non-driver identification card number; (3) 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; (4) 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 (5) 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."

This change broadens the types of data that, if breached, triggers a notification requirement. Under the old definition, Private Information was considered only the first three of five data elements. The new definition of Private Information also triggers a breach so long as the information was accessed, regardless of any actual acquisition of private information. Under the old law, acquisition of information was required to constitute a breach. Additionally, Section 899-aa also enhances the disclosure requirements and procedures that must be followed when a breach has occurred.

Moreover, Section 899-aa now reaches beyond just those who conduct business in New York State. Any company

that holds Private Information of a New York resident is subject to the notification requirements set forth in Section 899-aa.

The new Section 899-bb of the SHIELD Act creates considerable security requirements for those who hold private information of a New York resident.

To comply with Section 899-bb, those holding private information of a New York resident can either show that they are a "compliant regulated entity" or they can implement a data security program which implements strict safeguards identified in the statute. Section 899-bb defines what is it to be a "compliant regulated entity" which now extends the SHIELD Act to those in compliance with data security requirements of the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the New York Department of Financial Services (DFS).

Furthermore, Section 899-bb tailors security requirements to the size and complexity of the company holding a customer's private information. Failure to comply with the requirements of Section 899-bb is a violation of New York's General Business Law Section 349, Deceptive Acts and Practices Unlawful.

To comply with the SHIELD Act, companies in possession of customers' private data will be required to update their safeguards against data breaches.

If you have any questions regarding this client alert, please contact Dennis C. Vacco, Team Leader of the Lippes Mathias Wexler Friedman LLP Government Investigations and Enforcement Actions Team dvacco@lippes.com or 716.853.5100 Ext.1255.

Related Team

Dennis C. Vacco
Partner | Executive
Committee | Team
Co-Leader -
Government &
Corporate
Investigations