CARTER/LEDYARD

our resources

NY's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) Takes Effect

November 06, 2019

New York's "Stop Hacks and Improve Electronic Data Security Act (SHIELD Act)" (the "Act") officially took effect on October 23, 2019. In pertinent part, the Act amends New York General Business Law ("GBS") § 899 to expand the scope of "private information" covered under existing data breach notification provisions, to more broadly define what constitutes a "breach" of data security, and to add new data security requirements. The Act applies to all businesses that collect private information of New York residents, including nonprofits.

Breach Notification. Under the previous law, "private information" was defined as information that could be used to identify a person ("personal information") in combination with a social security number; a driver's license or non-driver's identification card number; or a financial account or credit card number with an access code or password that would permit access to an individual's account. The Act broadens the definition of "private information" significantly to include personal information in combination with (a) credit card and financial account numbers that can be used alone to access an individual's account; (c) biometric information (e.g., fingerprints, voice prints, etc. used to authenticate an individual's identity); and (c) a user name or email address in combination with a password or security question that would permit access to an individual's online account.

Importantly, whereas the previous law defined a breach of system security as "unauthorized acquisition" of certain data, the Act expands that definition to include "unauthorized access" to such data. Businesses must disclose a security breach to any resident of New York state whose private information is believed to have been wrongfully accessed or acquired. Notably, the Act provides that notice is not required if exposure of private information occurs as the result of an inadvertent disclosure by a person authorized to access the information, and the business determines that exposure will not result in misuse of the information, or in financial (or emotional) harm to the affected person.

In addition to the previous notice specifications, notice must now include the telephone numbers and websites of the state and federal agencies that provide information regarding data breach response and identity theft protection. The Act also (a) increases the penalty from $10 to $20 for each instance of failed notification, with a maximum penalty of $250,000 (up from $150,000 previously), and (b) lengthens the time period during which the Attorney General may bring an action for violation of the notice provisions—up to six years from the date of the business' discovery of the data breach, and longer if the business made efforts to hide the breach.

Data Security. The Act adds a new GBS § 889-bb, which requires businesses that own or license data that includes private information of New York residents to "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of . . . private information." A business will be deemed compliant with the Act if it implements a data security policy that requires:

- Reasonable administrative safeguards (e.g., a designated employee to coordinate a security program; identification of internal/external risks; assessment of current safeguards; employee training in security practice and procedures; engagement of qualified service providers to implement safeguards)

- Reasonable technical safeguards (e.g., assessment of risks in network and software; assessment of risks in information handling; system failure prevention, detection, and response; testing and monitoring of key controls and procedures)

- Reasonable physical safeguards (e.g., assessment of risks of information storage and disposal; system intrusion prevention, detection, and response; protection against unauthorized use or access to data; disposal of private information after use)

Note that a "small business" (defined as one with less than 50 employees, less than $3 million in revenue during the previous 3 years, or less than $5 million in year-end assets) shall be deemed compliant with the Act's data security requirements if the business has a security program with safeguards appropriate for its size and complexity, the nature and scope of its activities, and the sensitivity of the personal information it collects.

Businesses that already meet existing data breach notification or data security requirements mandated by other state or federal law may automatically be deemed compliant with the Act. Note also that the Act expressly does not create a private right of action; only the Attorney General is empowered to bring action for violations of its provisions.

The data breach notification provisions of the Act are effective as of October 23, 2019, and the data security provisions take effect March 21, 2020. All nonprofit organizations that collect private information of New York residents should consult legal counsel and review their existing policies and protocols to ensure compliance with the new requirements.

– Ahsaki Benion

related professionals

Pamela A. Mann / Partner
D 212-238-8758
mann@clm.com

Jeremy S. Steckel / Partner
D 212-238-8786
steckel@clm.com