Cullen | Dykman

New York State Expands Scope of Data Breach Notification Law

September 16, 2019

New York State has made significant amendments to the existing state law that requires notices to consumers and governmental authorities for certain data security breaches. The amendments expand the scope of information covered by the law and require the implementation of a data security program for certain persons and businesses.

The amendments are set forth in the Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act" or the "Act"), which was signed into law by Governor Cuomo in July. The Act amends New York General Business Law Section 899-aa to broaden the scope of information covered by that section and adds a new Section 899-bb which requires the implementation of a data security program for certain persons or businesses holding private information of a New York State resident. Most provisions of the Act take effect on October 23, 2019, except for new Section 899-bb which is effective on March 21, 2020.

New York General Business Law Section 899-aa, enacted in 2005, requires notices to New York State residents and governmental agencies for certain data security breaches. Effective October 23, 2019, Section 899-aa has been amended as follows:

- The definition of "private information" has been expanded to include "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."
- The list of data elements that are included in the definition of "private information" has also been expanded to include (i) biometric information and (ii) 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.
- The scope of the law has been broadened so that the notice requirement applies to any person or entity with private information of a New York resident, not just to those that "conduct business" in New York State.
- The definition of a "breach of the security of the system" has been broadened to include unauthorized access to private information.
- The Act clarifies that notice to affected persons is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the business reasonably determines that 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. This determination must be documented in writing and maintained for at least five years. If the incident affects over 500 residents of New York State, this written determination must be provided to the state attorney general within 10 days after the determination.

New Section 899-bb, effective March 21, 2020, requires any person or business that owns or licenses computerized data which includes private information of a resident of New York State to 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. These safeguards include:

- reasonable administrative safeguards,such as, designation of one or more employees to coordinate the security program, identification of reasonably foreseeable internal and external risks, assessment of sufficiency of existing safeguards, workforce cybersecurity training, and selection of service providers capable of maintaining appropriate safeguards and requiring those safeguards by contract;
- reasonable technical safeguards,such as, risk assessments of network, software design, information processing, transmission and storage, and implementation of measures to detect, prevent and respond to system failures, and regular testing and monitoring of the effectiveness of key controls, systems and procedures; and
- reasonable physical safeguards,such as, risk assessments of information storage and disposal, detection, prevention and response to intrusions, protections against unauthorized access to or use of private information during or after collection, transportation and destruction or disposal of the information, and disposal 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.

Businesses that are covered by and in compliance with the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and/or the New York State Department of Financial Services cybersecurity regulations (Part 500) shall be deemed in compliance with the requirement to implement this data security program. This will cover most financial institutions and health care companies.

Failure to comply with new Section 899-bb will subject businesses to a possible action by the New York Attorney General, as well as civil penalties. The Act specifies that there is no private right of action with respect to this law, meaning that a resident of New York State cannot recover damages from a third party under Section 899-bb.

If you have any questions regarding the SHIELD Act or data breach security requirements in general, please feel free to contact Elizabeth A. Murphy at (516) 296-9154 or via email at emurphy@cullenanddykman.com, Joseph D. Simon at (516) 357-3710 or via email at jsimon@cullenanddykman.com, Kevin Patterson at (516) 296-9196 or via email at kpatterson@cullenanddykman.com, or Mandy Xu at (516) 357-3850 or via email at mxu@cullenanddykman.com.

Practices

- Banking and Financial Services

Industries

- Business Reorganization and Financial Restructuring

Attorneys

- Elizabeth A. Murphy

- Joseph D. Simon
- Kevin Patterson