NELSON MULLINS

Privacy & Data Security Alert

July 2, 2019

New York Data Privacy and Security Update

By Colton Driver, Roy Wyman

The trend of state-level legislation to increase security protections and breach notification requirements for consumer data is one step closer to adding another state law to its ranks, after New York legislators advanced a new bill to Governor Cuomo's desk last week. Senate Bill 5575, also known as the *Stop Hacks and Improve Electronic Data Security Act* ("SHIELD Act"), expands on New York's current data breach notification laws by broadening current definitions within the Act and requiring new steps to be taken to protect data. Most notably, the SHIELD Act would broaden the definitions of "private information" and "breach." *Private information* is defined within the Act as including credit card information, biometric information, and email or username when combined with information that would permit access to an online account, such as a password or security question and answer. S. 5575, 2019 Leg., Reg. Session (NY 2019) § (1)(b)(4)-(5). Previously, the definition was limited to social security numbers, driver's license numbers, or account numbers (in more limited circumstances). *Breach* has been amended within the Act to include access to information, rather than requiring actual acquisition. Id at (1)(c).

The Act will affect "any person or business that owns or licenses computer data which includes private information of a resident of New York." S. 5575, 2019 Leg., Reg. Session (NY 2019) § 2. Any entity that is already a "compliant regulated entity," such as those already subject to legal obligations under HIPAA or GLBA, would be provided a safe-harbor, but others would be required to "develop, implement and maintain reasonable safeguards" in order to protect private information. S. 5575 at § 4 (2)(b)(i); S. 5575 § 4 (2)(a). To be compliant with the SHIELD Act, those businesses not falling within the safe-harbor exemption would need to devise programs that contain reasonable administrative, technical, and physical safeguards, which would include training employees, assessing risk, and protecting information, among other things. S. 5575 § 4 (2)(b)(ii). The current deadline to notify those affected by a breach would not be shortened, but the Act does include additional requirements before determining breach notification is not necessary. Id at § 3 (2)(a)-(b). These additional requirements include ensuring the exposure was inadvertent and to authorized persons and a reasonable finding that disclosed information will not be misused or cause financial or emotional harm. Id. Additionally, businesses would need to document and retain for five years any determination that information would not be used malevolently and would be required to notify the Attorney General if more than 500 New York residents' information is exposed. Id. No private right of action will be created by the SHIELD Act, but the Attorney General will be able to impose civil penalties. S. 5575 at § 4 (d)-(e).

Meanwhile, the New York Privacy Act ("NYPA") remained pending in the NY Senate Consumer Protection Committee at the conclusion of the 2019 New York Legislative session. While it does not appear that it will be enacted at this time, NYPA would likely be the most stringent data protection law ever enacted in the United States. For that reason, NYPA and any similar legislation have our full attention, and we will be sure to keep a vigilant eye on these laws for our clients.

View on Website

GET IN TOUCH

Roy Wyman
Partner
T 615.664.5362
roy.wyman@nelsonmullins.com

Colton Driver
Associate
T 803.255.9558
colton.driver@nelsonmullins.com