ALERT MEMORANDUM

New York Passes Expansive New Cybersecurity Law

July 29, 2019

On July 25, 2019, New York Governor Andrew Cuomo signed into law the Stop Hacks and Improve Electronic Data Security Act (the "SHIELD Act" or the "Act"), which expands data breach notification obligations under New York law and for the first time imposes affirmative cybersecurity obligations on covered entities.

The Act makes five principal changes to existing New York law:

— (1) Expanding the law's jurisdiction to entities that maintain private information of New York residents, regardless of whether or not such entities actually conduct business within the State;

— (2) Broadening the scope of "private information" triggering notification obligations in the event of a breach, including to biometric data;

— (3) Expanding the definition of a "breach" to include unauthorized "access" to private information, in addition to unauthorized "acquisition" of such information;

— (4) Increasing civil penalties for violations of notification obligations; and

— (5) For the first time, affirmatively requiring covered businesses to develop, implement, and maintain "reasonable" data security safeguards, which include, among other things, conducting risk assessments and addressing identified risks.

The first four provisions go into effect on October 23, 2019, while the fifth provision requiring companies to adopt and maintain a cybersecurity compliance program becomes effective on March 21, 2020.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

NEW YORK

Jonathan S. Kolodner
+1 212 225 2690
jkolodner@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

Russell A. Mawn, Jr.
+1 212 225 2467
rmawn@cgsh.com

© Cleary Gottlieb Steen & Hamilton LLP, 2019. All rights reserved.
This memorandum was prepared as a service to clients and other friends of Cleary Gottlieb to report on recent developments that may be of interest to them. The information in it is therefore general, and should not be considered or relied on as legal advice. Throughout this memorandum, "Cleary Gottlieb" and the "firm" refer to Cleary Gottlieb Steen & Hamilton LLP and its affiliated entities in certain jurisdictions, and the term "offices" includes offices of those affiliated entities.

Expanded Definition of Covered Entities

The SHIELD Act[1] removes the requirement that in order to be covered by the law a person or business must do business in New York. The law currently in effect applies to a person or business "which [1] conducts business in New York state, *and* [2] which owns or licenses computerized data which includes private information." By eliminating the first requirement, the law will now apply to all persons or companies that "own or license" the private information of New York residents, regardless of the location of the company's business activities. Consistent with the exterritorial trend in data security and privacy laws exemplified by the European Union's General Data Protection Regulation ("GDPR") and California's Consumer Privacy Act ("CCPA"), the Act will cover businesses that operate outside of New York (or even outside of the United States), if such entities maintain private information of New York consumers, employees, or other residents.

Expanded Definition of "Private Information"

Since 2005, New York has required entities that suffer a breach of "private information" of New York residents to notify affected individuals, New York authorities, and, where the breach affects more than 5,000 people, consumer reporting agencies. Prior to the passage of the Act, "private information" has been defined as "personal information"—"any information concerning a natural person which, because of name, number, and personal mark, or other identifier, can be used to identify such natural person"—*in combination with* one of the following: (1) social security number; (2) driver's license number or non-driver identification number; or (3) account number or credit or debit card number, with a password or code that would allow access to a financial account.

The SHIELD Act adds fourth and fifth data elements that trigger notification obligations in combination with "personal information": (4) an account number or credit or debit card number if it provides access to a financial account without a password or access code and (5) biometric information.[2] In addition, the Act adds notification obligations upon a breach where the information obtained includes "a username or e-mail address in combination with a password or security question and answer that would permit access to an online account." Notification of a breach of this type involving email/username information is triggered *whether or not in combination with "personal information."*

In expanding the categories of information triggering data breach notification obligations to include email/username information alone, New York is now in line with certain other states that have included the same protections in their own breach notification laws such as California, Florida, and Illinois, among others.

Expanded Definition of a Breach

In further broadening the scope of the law, the Act amends the definition of a "breach of the security of the system," from "unauthorized acquisition" to "*unauthorized access to* or acquisition of" private information. Cybersecurity incidents can often involve unauthorized actors only gaining access to systems and private information, without actually acquiring such information, either because a company's defenses prevent such acquisition or the hacker does not seek to acquire the information at that time. Under the Act's new definition of breach, evidence of exfiltration is no longer needed to trigger notification obligations. The Act elaborates that, in "determining whether information has been accessed," a company may consider "indications that the information was viewed, communicated with, used, or altered."[3]

[1] The new law is available here: https://legislation.nysenate.gov/pdf/bills/2019/S5575B.

[2] Biometric information is defined as "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."

[3] In another new provision, the Act provides that individuals do not have to be notified if their data was exposed unintentionally to someone authorized to access their private information, as long as the information is not expected to be misused by that person or cause financial or emotional harm to the individual. Companies will still have to document such an event and keep records of it for five years. If such an incident involves the information of more than 500 residents in New York, the person or company will be

Increased Civil Monetary Penalties for Violation of Notification Obligations

Previously, New York law provided for civil penalties of the greater of $5,000 for a violation of the notification obligations, or $10 per instance of failed notification, with the latter amount being capped at $150,000. The Act retains the $5,000 minimum penalty, but doubles the penalty per failed notification to $20, with a correspondingly greater cap of $250,000.

As before, these penalties apply to a person or business that violates the law "knowingly or recklessly." Additionally, the Act increases the statute of limitations for violations, giving the Attorney General three years, rather than two, to bring an enforcement action against the company, measured from the date of discovery by the Attorney General or notification by the company, whichever is earlier. The Act includes a statute of repose prohibiting any action six years "from the date of discovery of the breach by the company unless the company took steps to hide the breach."

Affirmative Data Security Requirements

Perhaps most notably, the SHIELD Act for the first time imposes an affirmative duty on companies to develop, implement, and maintain "reasonable safeguards" for computerized data which includes private information of New York residents.

The Act elaborates the data security measures that "shall" deem a company in compliance with the "reasonable safeguards" requirement, which include "administrative safeguards," "technical safeguards," and "physical safeguards." The Act identifies risk assessments, training, and selecting appropriate service providers as among the reasonable safeguards to ensure compliance with the Act:

Administrative Safeguards	(1) designates one or more employees to coordinate the security program; (2) identifies reasonably foreseeable internal and external risks; (3) assesses the sufficiency of safeguards in place to control the identified risks; (4) trains and manages employees in the security program practices and procedures; (5) selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and (6) adjusts the security program in light of business changes or new circumstances.
Technical Safeguards	(1) assesses risks in network and software design; (2) assesses risks in information processing, transmission and storage; (3) detects, prevents and responds to attacks or system failures; and (4) regularly tests and monitors the effectiveness of key controls, systems and procedures.
Physical Safeguards	(1) assesses risks of information storage and disposal; (2) detects, prevents and responds to intrusions; (3) protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and (4) disposes 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.

The Act's apparent intention is to provide the above-listed measures as examples of the respective safeguards to ensure compliance with the Act, but there is potential uncertainty over the amount of flexibility that New York regulators will provide to

required to provide a written determination to the state Attorney General's Office within 10 days of determining whether notification is necessary or not.

companies in deviating from the specific compliance provisions set forth in the statute.

For violations, the New York Attorney General is empowered to enforce the Act's reasonable safeguards provisions with penalties not to exceed $5,000 "for each violation," although the law does not clarify what constitutes a "violation" for purposes of imposition of a fine. The law is explicit in stating that "[n]othing in this section shall create a private right of action."

The "reasonable safeguards" requirements exempts certain businesses from compliance: (i) "small businesses," defined as those with fewer than 50 employees, less than $3 million in gross annual revenue for three fiscal years, or less than $5 million in year-end assets;[4] and (ii) businesses in the financial and healthcare industries that are regulated by and compliant with the Gramm-Leach-Bliley Act, New York DFS's cybersecurity regulations (23 NYCRR 500), the HIPAA Act, or the HITECH Act. The Act also includes a catchall exemption for companies regulated by and compliant with "any other data security rules and regulations" at the federal or New York state level. All other companies that own or license private information of New York residents will need to be compliant with the law by March 21, 2020.

Conclusion

Taken as a whole, the SHIELD Act represents a major step in expanding New York data breach obligations and security requirements for companies that obtain or license the data of New York residents. Most importantly, companies that collect private information of New York consumers, employees, or other residents must now develop, implement, and maintain reasonable safeguards to protect such information. The law is specific in identifying certain measures to ensure compliance, many of which are in line with current best practices for mitigating cybersecurity risk, including, among others:

- designating responsible personnel;
- conducting risk assessments;
- training employees;
- conducting due diligence and imposing contractual safeguards requirements on vendors;
- deleting data no longer needed for business purposes, and
- regularly testing key processes and controls.

Time will tell how aggressive New York authorities will be in enforcing these obligations in the absence of a breach. However, given that for almost every company it is only a matter of time before the next breach occurs, businesses should expect that there will be ample opportunity for vigorous enforcement and plan accordingly.

…

CLEARY GOTTLIEB

[4] Small businesses are required to implement "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."