CLIENT ALERT

New York Enacts the SHIELD Act

Aug.20.2019

Late last month, New York enacted the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act). In doing so, it has become the latest state to impose additional data security and breach notification obligations on businesses handling private data. The breach notification amendments take effect on October 23, 2019, while the data security requirements take effect on March 21, 2020.

Expanded Breach Notification Requirements

The SHIELD Act revises various definitions and increases the scope of the state's breach notification statute. The law expands the definition of "private information" to include:

- Financial account information that can be used to access an individual's financial account without a security code, access code, or password.
- Biometric information used to authenticate or ascertain an individual's identity.
- 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 SHIELD Act also expands the definition of "breach of the security of the system" to include any unauthorized "access" to computerized data that compromises the security, confidentiality, or integrity of private information. Unauthorized "acquisition" of such data is no longer the sole trigger for breach notification obligations – a distinction that only a handful but growing number of states make.

In addition, the SHIELD Act expands the jurisdiction of the breach notification statute, making it applicable to any person or business that maintains private information of New York residents, regardless of whether that person or business conducts business in New York. There are, however, several exceptions to this jurisdictional reach. For example, the law adopts a risk-of-harm inquiry, where a business need not provide notification if "the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the person or business reasonably determines 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." Moreover, businesses subject to certain breach notification requirements, such as the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the New York Division of Financial Services Cybersecurity Regulation (NYDFS Cybersecurity Regulation), do not need to make additional notifications to affected New York residents, though such businesses still need to notify the New York attorney general and state regulators in accordance with the statute.

Data Security Requirements

In addition to expanding the state's breach notification requirements, the SHIELD Act imposes additional data security obligations on businesses that own or license private information of New York residents. Such businesses are required to implement various administrative, technical, and physical safeguards designed to protect the security, confidentiality, and integrity of private information. The SHIELD Act lists various examples of such safeguards, including designating one or more employees to coordinate the security program, conducting risk assessments, training and managing employees, selecting vendors capable of maintaining appropriate safeguards and requiring such safeguards contractually, adjusting the security program based on business changes or new circumstances, and disposing private information within a reasonable amount of time after it is no longer needed for business purposes.

"Small businesses" are permitted to tailor their security programs based on their size, the nature of their activities, and the sensitivity of the personal information. The SHIELD Act defines a small business as any person or business with (a) fewer than 50 employees, (b) less than $3 million in gross annual revenue in each of the last three fiscal years, or (c) less than $5 million in year-end total assets. Here too, the SHIELD Act allows businesses to leverage their other regulatory obligations: Companies subject to, and in compliance with, other legal and regulatory regimes such as GLBA, HIPAA, and the NYDFS Cybersecurity Regulation are considered in compliance with this part of the SHIELD Act.

Penalties

There is no private right of action under the SHIELD Act. Nonetheless, covered businesses are subject to attorney general enforcement with civil penalties for knowing and reckless violations of the breach notification obligations of up to $20 per instance with a cap of $250,000. Violations of the reasonable safeguard requirements may carry penalties of up to $5,000 per violation. The SHIELD Act also lengthens the statute of limitations from two years to three years.

Conclusion and Takeaways

The SHIELD Act greatly increases the jurisdictional reach of New York's breach notification statute, which now applies to entities that do not do business in the state, as long as they maintain private information of New York residents. It also expands various key definitions. Businesses across the country that maintain private information on New York residents will want to consider reviewing their security programs and incident response plans to determine if any changes are needed to comply with the SHIELD Act.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Kate M. Growley, CIPP/G, CIPP/US
Partner – Washington, D.C.

Phone: +1 202.624.2698
Email: kgrowley@crowell.com

Jarno Vanto, CIPP/E, CIPP/US
Partner – New York
Phone: +1 212.803.4025
Email: jvanto@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com

Brandon C. Ge
Counsel – Washington, D.C.
Phone: +1 202.624.2531
Email: bge@crowell.com