BLANKROME

Cybersecurity & Data Privacy

OCTOBER 2019 • NO.4

New York SHIELD Act Will Impose Noteworthy New Data Security & Breach Notification Requirements on Companies That Handle Data of New York Residents

As the risk of data breach events—both from malicious outsiders and negligent insiders—continues to rise with no end in sight, New York recently enacted the Stop Hacks and Improve Electronic Data Security Handling ("SHIELD") Act, which provides key changes to the state's data security and data breach notification laws. Significantly, the law applies to any business that collects or utilizes the data of New York residents, even if that business does not conduct any operations within the state. Covered businesses will need to take immediate action to get in compliance with New York's SHIELD Act by the law's March 21, 2020 effective date.

"REASONABLE" DATA SECURITY REQUIREMENT

By far, the aspect of the SHIELD Act that has received the greatest attention—and for good reason—pertains to the new data security requirements that have been imposed under the law. Under the SHIELD Act, any individual or entity that processes the personal data of New York residents must "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." Importantly, the law provides that a business will be deemed in compliance with the requirement to implement reasonable data security measures if it maintains a data security program that incorporates a detailed series of administrative, technical, and physical controls that are set forth in the law. In addition, businesses that are in compliance with the data security mandates of laws such as the GLBA, HIPAA, and HITECH are also deemed to be in compliance with the SHIELD Act's reasonable security requirement.

The SHIELD Act relaxes the standard for satisfying the reasonable security requirement for small businesses—those with fewer than 50 employees, less than three million dollars in gross annual revenue, or less than five million dollars in year-end total assets—by providing that those businesses are in compliance with the reasonable security aspect of the law if their security programs contain

safeguards that are appropriate for the size and complexity of the business, the nature and scope of the business's activities, and the sensitivity of the data the business collects on consumers.

Businesses that are found to have violated the law's "reasonable" security requirement can be held liable for civil penalties of up to $5,000 per violation.

EXPANDED DEFINITION OF PROTECTED "PRIVATE INFORMATION"

In addition, the SHIELD Act also expands the scope of the state's prior breach notification law in several different respects. First, the law broadens the types of personal data that trigger data breach notification obligations. New York's original breach notification law defined "private information"—information that is sufficient to trigger breach notice obligations—to include Social Security numbers; driver's license or non-driver ID card numbers; and account, credit card, or debit card numbers *in combination with* any required security code, access code, or password that could be used to access an individual's financial account. Under the SHIELD Act, "private information" now also includes account, credit card, or debit card numbers *alone, and without any additional identifying information,* if the information could be used to access an individual's financial account; biometric data; and online account login credentials.

BROADENED APPLICABILITY OF BREACH NOTIFICATION OBLIGATIONS

The SHIELD Act also expands the scope of the covered entities' breach notification obligations by extending those obligations to cover all entities that process the private information of New York residents, regardless of whether those entities do business in the state. As such, a physical presence or conducting business in the state is *not* a prerequisite to falling under the scope of the SHIELD Act's breach notice mandates.

Moreover, the SHIELD Act also broadens the circumstances that are sufficient to trigger notice to impacted individuals by providing that notice is required not only when data has been improperly *acquired,* but also that which has been improperly *accessed* as well—a very low threshold that encompasses actions such as viewing, using, or altering private information without valid authorization. As such, moving forward a much wider range of data breach incidents will trigger notice obligations on the part of the breached entity.

BREACH NOTIFICATION REQUIREMENTS

Under the SHIELD Act, any person or business must disclose any breach of the security system to any resident of New York whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. In addition, in the event that a breach triggers notification obligations to New York residents, the breach victim must also notify the New York Attorney General, Department of State, and State Police regarding the number of impacted individuals and the timing, content, and distribution of the entity's breach notices. In addition, the breach victim must also provide a template of the notice that was sent to impacted individuals as well. Where a breach impacts more than 5,000 New York residents, the breach victim must also provide notice to consumer reporting agencies.

Importantly, the SHIELD Act provides an exemption from the law's notice requirements for breaches that arise out of an inadvertent disclosure of private information, if the breach victim reasonably determines that the risk of misuse of the information, or harm to the impacted individuals, is not likely.

Businesses that are found to have violated the SHIELD Act's breach notice provisions can be held liable for actual damages incurred by individuals entitled to receive notice if notification is not provided in accordance with the law. In addition, those businesses found to have committed knowing or reckless violations may be assessed penalties the greater of $5,000 or up to $20 per instance of failed notification, provided the latter does not exceed $250,000.

COMPLIANCE STEPS

Critically, the SHIELD Act now expressly requires that covered entities "develop, implement, and maintain reasonable safeguards" to protect personal data from falling into the wrong hands. This particular facet of the SHIELD Act represents a growing trend among state-level legislators in enacting legislation geared toward requiring companies that handle sensitive personal data to tighten up and strengthen their data privacy and data security practices. In addition, the SHIELD Act greatly expands the scope of potential data breach events that are now sufficient to trigger breach notification requirements under New York law, which, in turn, greatly expands the potential that businesses will find themselves subject to the onerous data breach notification obligations of the SHIELD Act in the event the organization suffers a data compromise event—making it even more essential that businesses implement

strong defensive data security strategies to curb the risk of data compromise events.

In terms of actionable compliance steps, businesses that handle the data of New York residents—even if they do not conduct any business in the state—should take immediate action to update their data security programs to incorporate the administrative, technical, and physical safeguards set forth in the SHIELD Act that will allow them to be "deemed" in compliance with the law's reasonable security requirement. In doing so, businesses should also consider incorporating several other specific, essential data security controls that will significantly aid in combating the risk of data compromise events:

- Perform periodic risk assessments to identify the primary risks to the personal information that is possessed by the entity, and implement any necessary modifications to the organization's information security program so as to minimize the risk of these vulnerabilities being exploited by a data breach.
- Maintain stringent password protection policies, which should encompass elements such as password expiration, complexity, and length. In addition, companies should also consider requiring multi-factor password authentication for all accounts.
- Ensure that all company data is encrypted, both while at rest and in transit.
- Utilize the principle of least privilege and grant employees only the minimal level of access or privilege that is necessary for the individual to carry out his or her job duties and responsibilities. Strategically tailoring access is an effective way to ensure the security of organizational data.
- Utilize a strong firewall to protect the company's systems by controlling the Internet traffic that flows in and out of its networks, as well as antivirus protection, which can serve as the last line of defense should a malicious attack make its way inside the perimeter of an organization's network.
- Monitor the use and transmission of electronic data by employees, with an eye toward unusual activity—especially if data is being pulled off the entity's network—which can not only detect data leaks when they happen, but can discourage employees from taking unnecessary risks in connection with organizational data.

THE FINAL WORD

The ultimate impact of the SHIELD Act is significant and far-reaching, as all businesses that handle the private information of New York residents—regardless of whether the entity conducts business in the state—must comply with the new law. In particular, the SHIELD Act's reasonable security and breach notification requirements substantially expand the potential scope of liability exposure faced by covered entities stemming from data breach incidents. Beyond that, the potential exists that the New York Attorney General may pursue civil penalties against companies that fail to implement reasonable data security safeguards, even in the absence of a data breach. Taken together, the SHIELD Act necessitates the implementation effective defensive data security controls to protect networks, systems, devices, and data from cyber attacks and other data compromise events. Importantly, because the process of building an effective information security program that comports with the SHIELD Act's reasonable security requirements will be time-consuming and complex, businesses should take immediate action to update and enhance their data security and breach notification policies, practices, and protocols in order to ensure compliance by the law's March 21, 2020 effective date.

For additional information, please contact:

Jennifer J. Daniels
412.932.2754 | daniels@blankrome.com

David J. Oberly
513.362.8711 | doberly@blankrome.com