What Your Company Needs to Know About the March 2020 Amendment to the New York SHIELD Act

Articles, Privacy, Technology and Data Security March 10, 2020

New York residents will soon benefit from greater protections following a data breach when an amendment of New York's data breach notification law—the Stop Hacks and Improve Electronic Data Security Act, or SHIELD Act—goes into effect on March 21, 2020. Under this amendment, companies need to employ stricter data security measures over an individual's confidential personal information. This accompanies the Act's breach notification requirements that are already in place.

Significantly, the amendment to the SHIELD Act will impact not only businesses and employers that do business in New York, but also a company and/or employer in *any* jurisdiction that is in possession of a New York resident's personal information, which includes: social security numbers, drivers' license numbers, credit/debit card numbers, financial account numbers (including security codes), biometric information, email addresses and passwords, and email security questions and answers. The SHIELD Act requires these companies to "develop, implement, and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information."

The SHIELD Act does not identify the precise safeguards that a company must employ. However, it does outline specific elements of a "data security program" that, if implemented, would put an employer in compliance with the SHIELD Act's mandates. Those elements fall into three general categories:

- Administrative safeguards (*e.g.*, the designation of an employee or multiple employees to coordinate the data security program; the identification of reasonably foreseeable internal and external risks; the implementation of controls to mitigate those risks; the training of employees regarding proper security program practices and procedures)
- Technical safeguards (*e.g.*, the assessment of network, software design, and information processing, transmission, and storage risks; the implementation of measures to protect against system failures; the regular testing of the effectiveness of key controls)
- Physical safeguards (*e.g.*, the detection, prevention, and response to intrusions; the protection against the unauthorized access to or use of personal information; a means of securely destroying and disposing of personal information within a reasonable time after is no longer needed)

The New York State Attorney General will be responsible for enforcing the SHIELD Act and ensuring that employers are compliant with its mandates. To make sure that your company is fully able to comply with the SHIELD Act, it is critical that your managers work in conjunction with the IT team, the HR team, and legal counsel to (1) familiarize themselves with the purpose and requirements of the SHIELD Act; (2) create and implement a clear and thorough data security program; and (3) train your employees on the importance of information security.

For additional information contact Maribeth Thomas or any of the attorneys in the Privacy, Data Security & Technology Group.