JENNER&BLOCK

## Data Privacy and Cybersecurity

# New York SHIELD Act Goes Into Effect

By: David P. Saunders and Allison N. Douglis

On March 21, 2020, the cybersecurity provisions of the New York "Stop Hacks and Improve Data Security" (SHIELD) Act go into effect. The SHIELD Act puts New York into the small but growing list of states requiring that companies that control resident data take specific actions to protect that data. While much ink has been spilt on the move by New York to join this minority, the requirements of the SHIELD Act are likely familiar to businesses that have been taking steps to protect consumer data. Thus, although the SHIELD Act represents a new potential avenue for regulatory liability to businesses, it is likely that businesses will not have to take many—if any—additional internal steps to come into compliance with the cybersecurity provisions of the SHIELD Act. Below we detail the Act's cybersecurity elements.

- **New data security protections.** The SHIELD Act requires that any "person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information." This is the cornerstone of the SHIELD Act's cybersecurity provisions and should be familiar to most data privacy practitioners. The concept of adopting "reasonable safeguards" is part of the National Institute of Standards and Technology (NIST)'s cybersecurity framework as well as most developed cybersecurity programs. The SHIELD Act, however, goes a step farther by outlining three ways that a business can satisfy its cybersecurity requirements:

    - **Comply with federal or New York State regulations.** The SHIELD Act provides that any "compliant regulated entity" is deemed in compliance with the SHIELD Act's cybersecurity provisions. As a result, entities regulated under HIPAA, GLBA, or additional federal or New York data security laws, rules, or regulations will be deemed to be in compliance with the SHIELD Act.

    - **Implement a data security program with administrative, technical, and physical safeguards.** If not qualified as a "compliant regulated entity" or a "small business", a person or business can comply with the new cybersecurity provisions of the SHIELD Act by implementing a data security program that includes certain administrative, technical, and physical safeguards, many of which ought to be familiar. Under the SHIELD Act, data security programs must include: (i) identifying one or more employees to coordinate the program; (ii) ongoing risk assessments and security adjustments ; (iii) a training program for employees; (iv) a service provider diligence program to ensure integrity and protection of data; (v) methods for detection, prevention and remediation of attacks or security weaknesses; (vi) regular technical control tests and monitoring; and (vii) procedures for the secure disposal of data.

    - **For small businesses, institute proportionally adequate protections.** Recognizing that the investment a Fortune 100 company can make in cybersecurity is different than that which a small business can afford, the SHIELD Act provides that a "small business"—fewer than 50 employees, making less than $3 million in annual gross revenue in the last three fiscal years, or having less than $5 million in total year-end assets—need only implement reasonable safeguards that are appropriate for "the size and complexity of the small business, the nature and scope of [its] activities, and the sensitivity of the personal information [it] collects from or about consumers." This safe harbor language provides important flexibility to small businesses as they grow.

- **Attorney general enforcement.** The SHIELD Act expressly provides that "[n]othing in this section shall create a private right of action." As a result, enforcement is left to the New York attorney general. The New York attorney general can bring enforcement actions to enjoin violations and

obtain civil penalties. Civil penalties under the SHIELD Act can be as high as $5,000 for each violation without any aggregate liability cap.

## Contact Us


**David P. Saunders**

dsaunders@jenner.com | Download V-Card

**Allison N. Douglis**

adouglis@jenner.com | Download V-Card


**Meet Our Team**