Published on *The National Law Review* https://natlawreview.com

# Looming Data Security Requirements Under the New York SHIELD Act: What Businesses Need to Know

Article By:

Patrick M. Collins

Jamie Haar

By March 21, 2020, nearly every business—not only those that conduct business in New York State—that owns or licenses computerized data that includes the private information of any New York State resident, will be required to implement certain safeguards to protect the security of such information.

As we reported in September 2019, the New York State Legislature passed and Governor Andrew Cuomo signed two bills last year that aim to improve protections for the handling of computerized private information of New York residents. The Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) amended New York law by requiring businesses to implement safeguards for handling the private information of New York residents and broadened security breach notification requirements. While the SHIELD Act's breach notification requirements are already in effect, the "reasonable safeguards" requirements are not effective until March 21, 2020.

As expanded by the SHIELD Act, "private information" of a New York resident is now defined as:

1. a username or email address in combination with a password or security question and answer that would permit access to an online account; or

2. personal information (name, number, personal mark, or other identifier that can be used to identify a natural person) in combination with any one or more of the following data elements, when either the data element alone or the data element in combination with the personal information is not encrypted or is encrypted with an encryption key that has been accessed or acquired:

    - Social Security number;

    - driver's license number or non-driver ID card number;

    - account number, credit or debit card number (a) in combination with any required security code, access code, password, or other information that would permit access

to an individual's financial account, or (b) if circumstances exist wherein such number can be used to access an individual's account *without* additional identifying information, security or access code, or password; or

- biometric information (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 or digital representation of biometric data that is used to authenticate or ascertain an individual's identity.

Pursuant to the SHIELD Act, any business that owns or licenses computerized data that includes private information of any New York resident is required to develop and implement a data security program that contains reasonable safeguards to protect the security, confidentiality, and integrity of such information and its disposal. A compliant data security program includes:

1. **Reasonable administrative safeguards**, such as the following, in which a business:
    - designates one or more employees to coordinate the security program;
    - identifies reasonably foreseeable internal and external risks;
    - assesses the sufficiency of safeguards in place to control the identified risks;
    - trains and manages employees in the security program practices and procedures;
    - selects service providers capable of maintaining appropriate safeguards and requires those safeguards by contract; and
    - adjusts the security program in light of business changes or new circumstances.

2. **Reasonable technical safeguards**, such as the following, in which a business:
    - assesses risks in network and software design;
    - assesses risks in information processing, transmission, and storage;
    - detects, prevents, and responds to attacks or system failures; and
    - regularly tests and monitors the effectiveness of key controls, systems, and procedures.

3. **Reasonable physical safeguards**, such as the following, in which a business:
    - assesses risks of information storage and disposal;
    - detects, prevents, and responds to intrusions; and
    - protects against unauthorized access to or use of private information during or after

the collection, transportation, and destruction or disposal of 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 SHIELD Act does not create a private right of action, but the New York attorney general may sue to enjoin violations of the act and seek civil penalties.

Excluded from the safeguards' requirements are "small businesses," which are defined as those with fewer than 50 employees, less than $3 million in gross annual revenue in each of the last 3 fiscal years, or less than $5 million in year-end total assets. A small business need only ensure that its data security safeguards are appropriate for its size and complexity, the nature and scope of its activities, and the sensitivity of the personal information it handles. Also excluded from these requirements are businesses subject to other federal or New York State regulatory schemes governing data security, such as the regulations under the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA), or the cybersecurity regulations of the New York State Department of Financial Services.

With the effective date of the SHIELD Act's "reasonable safeguards" requirements approaching, any business that does not fall within one of the act's exceptions and that owns or licenses computerized data that includes private information about any New York resident may want to review its data security program closely with its legal, HR, and information technology professionals.



National Law Review, Volume X, Number 71