COVINGTON

New York SHIELD Act Data Security Requirements Become Effective

March 22, 2020

Data Privacy and Cybersecurity

On March 21, 2020, the data security requirements of the New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act (the "Act") became effective. These provisions require businesses that own or license computerized data that includes the "private information" of New York residents to maintain "reasonable" security measures. Generally speaking, the Act's provisions expand both the kinds of businesses and the types of information that are subject to the data security requirements. The Act also provides more detail about what New York's data security requirements are and how to comply with them. Businesses that own or license information of New York residents should evaluate the extent to which these requirements might apply to them and, if so, whether their current data security practices comply with the Act's newly-effective requirements.

We discuss the Act and its implications more broadly in further detail below.

Overview

The Act represents an expansion of New York's existing cybersecurity and data breach notification laws. The Act has two main impacts on businesses:

1. it expands data breach notification requirements under New York law; and
2. it requires businesses to maintain "reasonable safeguards" to protect the "private information" of New York residents.

The Act was signed into law on July 25, 2019, but has phased effective dates for different sections of the law, as set forth below.

Data Breach Notification: The Act's data breach notification requirements amend New York's data breach notification law (§899-aa of Article 39-F of New York's General Business Law) to expand data breach notification requirements relating to the "private information" of New York residents. Those provisions took effect on October 23, 2019.

"Reasonable Safeguards" Requirements: The Act's "reasonable safeguards" provisions add §899-bb to New York's General Business Law, which requires any person or business that owns or licenses the "private information" of New York residents to develop, implement, and maintain "reasonable safeguards" to protect such information. These reasonable safeguards requirements, also discussed below, came into effect on March 21, 2020.

What Entities are Covered?

The Act's data security requirements apply to any person or business that owns or licenses computerized data that includes a New York resident's "private information." This change, discussed further below, is an expansion from New York's prior law, which applied to businesses that owned or licensed New York residents' private information **and** conducted business in New York. In other words, the new law drops the requirement that a covered entity must conduct business in New York—owning or licensing a New York resident's private information is now enough to be covered by the Act's data security requirements.

What Types of Information are Covered?

The Act applies to New York residents' "private information." Private information is defined as either:

(i) "personal information" (which means "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person") *in combination with* one or more specifically enumerated data elements (set forth below), when such information was not encrypted or was encrypted with an encryption key but accessed or acquired; or

(ii) a user name or e-mail address *in combination with* a password or other security question and response that would permit access to a user's online account.

With respect to the enumerated "data elements" referenced in item (i), the Act amended the prior list of data elements to add:

(i) account, credit, or debit card numbers where such number could be used *without* other identifying information, security code, access code, or password to access an individual's financial account, and

(ii) biometric information, such as fingerprints, voice prints, and retina or iris images, that are used to authenticate or ascertain an individual's identity.

These two additions join the pre-existing list of data elements:

(iii) Social Security number;

(iv) driver's license number or non-driver identification card number; and

(v) account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account.

What Are Reasonable Safeguards?

If an entity owns or licenses computerized data that includes the private information of New York residents, the Act's data security provisions require the entity to "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."

The Act provides two primary means by which covered entities may achieve compliance. A covered entity will be "deemed in compliance" if it either:

(i) complies with one of a list of regulatory frameworks, or

(ii) implements a data security program that includes specific elements.

Each of these compliance paths is explained in further detail below. (Note also that the Act appears to leave open the possibility that a covered entity may comply with the Act's data security requirements through means other than these two paths by showing that it has "reasonable safeguards" in place, but the specific methods and requirements of any such alternative compliance paths are not entirely clear.)

The Act also includes specific provisions applicable to small businesses, which are more fully described below.

(i) Compliance with Established Regulatory Frameworks

Covered entities can be deemed in compliance based on their status as regulated entities that are subject to and compliant with the following regulations:

- the Health Insurance Portability and Accountability Act ("HIPAA");
- the Gramm-Leach-Bliley Act. ("GLBA");
- the New York Department of Financial Services Cybersecurity Regulations (23 NYCRR 500); or
- any other data security rules and regulations administered by a federal or New York state government department, division, commission, or agency.

(ii) Implementing Specific Data Security Program Elements

Entities that do not comply with one of the specifically enumerated regulatory frameworks listed in the Act can also be "deemed in compliance" if they implement a data security program that includes the below elements:

- *reasonable administrative safeguards*, such as:
  - designating one or more employees to coordinate the security program;
  - identifying reasonably foreseeable internal and external risks;
  - assessing the sufficiency of safeguards in place to control identified risks;
  - training and managing employees in the practices and procedures of the security program;
  - selecting service providers capable of maintaining appropriate safeguards and requiring those safeguards by contract; and
  - adjusting the security program in light of business changes or new circumstances; and
- *reasonable technical safeguards*, such as:
  - assessing risks in network and software design;
  - assessing risks in information processing, transmission, and storage;

- detecting, preventing, and responding to attacks or system failures; and
- regularly testing and monitoring the effectiveness of key controls, systems, and procedures; and

- *reasonable physical safeguards*, such as:
  - assessing risks of information storage and disposal;
  - detecting, preventing, and responding to intrusions;
  - protecting against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and
  - disposing of private 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.

Small Businesses: The Act does include an alternative compliance option for "small businesses," which are defined to include businesses with fewer than 50 employees, less than $3 million in gross annual revenue in each of the last three fiscal years, or less than $5 million in year-end total assets. If a business meets one of these requirements, it can satisfy the Act's reasonable safeguards requirements if it implements a security program that contains "reasonable administrative, technical, and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers."

What About the Data Breach Notification Requirements That Were Already in Effect?

Since October 2019, covered entities have also been subject to additional data breach notification requirements implemented through the Act's amendments to existing New York breach notification law. Most notably,

(i) the definition of "private information" that might trigger a reportable breach was expanded by the Act to include additional categories of covered information (as explained above), and

(ii) the definition of "breach," which triggers notification requirements under New York notification law, was expanded by the Act to include both unauthorized "acquisition" of, and unauthorized "access" to, private information.

In determining whether an unauthorized person accessed, or can be reasonably believed to have accessed, private information, the Act states that businesses should consider "indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person."

Notably, the Act also added a new exception to the state's notification requirement. Specifically, the Act states that even if private information was exposed, notice is ***not*** required if the exposure "was an inadvertent disclosure by persons authorized to access the private information" and the business "reasonably determines [that] 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." An entity that relies on this exception must provide

notice of its determination to the New York Attorney General within ten days of the determination.

Finally, the Act also added certain exceptions to the statutory notice requirement, but an entity relying on those exceptions must still follow the law's requirements for notification to New York state regulators, including the New York Attorney General.

What Should Companies Expect in Enforcement?

The New York Attorney General is authorized to bring actions for violations of the Act's data security requirements. A failure to comply with the Act's requirement for the implementation of reasonable safeguards will be subject to civil penalties of up to $5,000 per violation under N.Y. Gen. Bus. Law Section 350-d. The Act specifically states that it should not be read to provide a private right of action. Although the Attorney General has not yet provided detailed guidance on how the Act's data security requirements will be enforced, entities subject to these provisions may want to monitor enforcement actions and trends in the coming months.

The Act also increases the civil penalties for violations of New York's breach notification requirements, as well as the time for the Attorney General to bring an action for such violations. Specifically, violations of the notification requirements are subject to a civil penalty of the greater of $5,000 or up to $20 per instance of failed notification (increased from a previous limit of $10 per instance). The total per-instance civil penalty shall not exceed $250,000, up from a previous limit of $150,000. In addition, the Act amends the time limitations for bringing an action, permitting the Attorney General to bring an action within three years from when the Attorney General becomes aware of a breach. This is an extension of the prior two-year time period to commence an action. The Act also establishes a maximum time range beyond which the Attorney General may not commence an action, which should provide companies with additional clarity on potential enforcement risks following a data breach. Specifically, the Attorney General may not bring an action for violation of the statute's breach notification provisions after six years from the date of the discovery of a breach, unless the company took steps to hide the breach.

***

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Data Privacy and Cybersecurity practice:

Micaela McMurrough	+1 212 841 1242	mmcmurrough@cov.com
Micha Nandaraj Gallo	+1 212 841 1216	mnandarajgallo@cov.com
Caleb Skeath	+1 202 662 5119	cskeath@cov.com