New York Expands The Data Breach Umbrella: More Cybersecurity Incidents Will Require Breach Compliance From Businesses Who Possess Private Information For New York Residents

Insights
8.21.19

On July 25, 2019, New York Governor Anthony Cuomo signed the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) into law. The Act creates additional protections for the residents of New York and their private information. It also endeavors to improve cybersecurity measures for those who possess private information about New York residents.

Importantly, the SHIELD Act (1) amends General Business Law Section 899-aa, New York's data breach notification statute, to provide updated definitions and additional coverage, and (2) creates the new General Business Law Section 899-bb, which imposes data security requirements on any person or business that owns or licenses computerized data that includes private information for a New York resident.

Modifications to the data breach notification law (Section 899-aa) will become effective on October 23, 2019, while the new data security protections (Section 899-bb) will become effective on March 21, 2020.

Data Breach Notification Law
The New Definition of "Private Information"

New York's original data breach notification law included definitions for both "personal information" and "private information." The current definition of "personal data" remains unchanged, and will continue to be "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person."

However, the SHIELD Act amends the definition of "private information" to include three new types of personal information that are covered by the law: (1) an account number, credit or debit card number, even without additional identifying information or a password; (2) biometric information, such as an individual's fingerprint, voice print, or retina image; and (3) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

Expanding the Definition of a "Breach"

Expanding the Definition of a "Breach"

Not only has New York included more categories of information that could trigger a breach, but it has also broadened the activity that constitutes a breach. Previously, a breach was the unauthorized acquisition of "personal" information. The new law deems a breach to have occurred if there was the acquisition of, or access to, "private" information.

When evaluating whether access occurred, the Act provides that a business may consider "indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person."

The SHIELD Act's Global Reach

The old New York data breach law applied to any "person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information…" The Act has removed the "conducts business in New York state" requirement. Now, regardless of whether the person or business is conducting business in New York, the SHIELD Act applies to those who possess private information for a New York resident.

Changes to Data Breach Notification Requirements

The Act now provides that notice to affected persons is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the person or business reasonably determines that such exposure will not likely result in misuse of such information or cause financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials. If this exception applies, the person or business must document the determination and maintain the documentation for at least five years. If the incident affects more than five hundred New York residents, the written determination must be provided to the New York Attorney General within ten days after the determination.

For those business who are required to comply with data breach requirements under laws such as Health Insurance Portability and Accountability Act of 1996 ("HIPAA") or the Gramm-Leach-Bliley Act, additional notifications are not required to be issued to impacted New York residents. However, these businesses are required to notify the New York Attorney General, the New York Department of State, and the New York Division of State Police.

The SHIELD Act also requires that breach notifications include the telephone numbers and websites of the relevant New York State and federal agencies that provide information regarding security breach response and identity theft prevention and protection information.

Data Security Protections

In an effort to reduce the likelihood of data breaches, the SHIELD Act creates new "Data Breach Security Protections." All persons or business that own or license computerized data that includes private information for a New York resident will now be required to comply with a "reasonable security requirement," meaning that they will need 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 reasonable safeguards require any applicable person or business (i) to be in compliance with laws such as HIPAA or the Gramm-Leach-Bliley Act or (ii) to implement a data security program that includes the following:

(A) reasonable administrative safeguards such as the following, in which the person or business:

(1) designates one or more employees to coordinate the security program;

(2) identifies reasonably foreseeable internal and external risks;

(3) assesses the sufficiency of safeguards in place to control the identified risks;

(4) trains and manages employees in the security program practices and procedures;

(5) selects service providers capable of maintaining appropriate safe-guards, and requires those safeguards by contract; and

(6) adjusts the security program in light of business changes or new circumstances; and

(B) reasonable technical safeguards such as the following, in which the person or business:

(1) assesses risks in network and software design;

(2) assesses risks in information processing, transmission and storage;

(3) detects, prevents and responds to attacks or system failures; and

(4) regularly tests and monitors the effectiveness of key controls, systems and procedures; and

(C) reasonable physical safeguards such as the following, in which the person or business:

(1) assesses risks of information storage and disposal;

(2) detects, prevents and responds to intrusions;

(3) protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and

(4) disposes 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.

While small businesses are subject to the reasonable security requirement, the SHIELD Act provides that these safeguards may be "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." The Act considers a small business to be one that has less than fifty 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.

What Steps Should You Consider?
In light of the SHIELD Act, companies may consider the following:

- Determine if you are in possession of private information for New York residents, even if you are not conducting business in New York. This may be the opportunity to assess whether you need to retain this information for ongoing business purposes.
- Ensure that you have administrative, technical, and physical safeguards in place that comply with the requirements of the SHIELD Act.
- Develop, or revisit, internal policies for how the company will identify and respond to a data breach. Ensure that your employees understand the policies and that they are properly implemented.

We will continue to monitor developments and provide updates as they are available. If you have any questions regarding how the SHIELD Act could impact your business, please consult your Fisher Phillips attorney.

Related People

Jeffrey M. Csercsevits
Partner
610.230.2159
Email