BOUSQUET HOLSTEIN PLLC Alert

New NYS Data Security Regulations That May Impact Your Operations - SHIELD Act

Syracuse ♦ Ithaca ♦ New York City May 2020

Across the country, businesses are reopening and adapting to the COVID-19 pandemic. In doing so, however, businesses must keep in mind new data security regulations from New York that could impact their operations. As of March 21, 2020, New York may penalize qualifying businesses that fail to implement "reasonable safeguards" over collected data or fail to follow strict protocols under its Stop Hacks and Improve Electronic Data Security Act (SHIELD Act).

What Businesses Qualify Under SHIELD Act regulations?

The SHIELD Act regulations apply to any persons or businesses **in and out of New York** that collect or retain "private information" about New York residents. "Private information" is defined two ways: first, as online account access information (i.e. login name with password or associated security questions). Second, as unencrypted personal information (like a name) stored with the following data:

- social security number or driver's license number;
- biometric data used to validate a person's identity; or
- financial information that would enable outside parties to access NY residents' accounts, like credit card numbers with its associated security code.

What Do SHIELD Act Regulations Require?

Data Security Requirements

Qualified businesses must implement "reasonable safeguards" for NY residents' data. To meet this threshold of reasonableness, businesses must implement several protocols, which include:

- appointing a security program coordinator; and
- creating a data protection program with reasonable physical, technical, and administrative safeguards. Examples of reasonable safeguards include regular risk assessments; mitigation against unauthorized access; on-going tests of network, software, and physical vulnerabilities; protocols for intrusion responses; requiring all employees to undergo routine security training; and working only with IT service providers that can and will abide by required data safeguards.

The SHIELD Act exempts some businesses from the new data security requirements. Small businesses, as defined in the SHIELD Act[1], are only required to have security requirements that are reasonable to the "nature and scope" of the business's work, the "size and complexity" of the business, and the "sensitivity" of the data it collects. Additionally, businesses that already comply with HIPPA, HITECH, or the Gramm-Leach Bliley Act comply under the SHIELD Act security requirements as well.

New Security Breach Notification Protocols.

Under the SHIELD Act, businesses must follow new protocols when a data security breach occurs or when a business "reasonably believes" an unauthorized party accessed its stored private information.

[1] The SHIELD Act defines small businesses fewer as having "(i) fewer than fifty employees; (ii) less than three million dollars in gross annual revenue in each of the last three fiscal years; or (iii) less than five million dollars in year-end total assets, calculated in accordance with generally accepted accounting principles."

Continued on next page

New NYS Data Security Regulations That May Impact Your Operations - SHIELD Act

Depending on the circumstances of the breach, certain parties must be notified. Businesses must disclose the breach to affected NY residents within a reasonable time. Before notice is sent to NY residents, however, businesses must inform the NY Department of State, the NY State Police, and the NY State Attorney General about the number of residents involved, the notice's content, its delivery method, and when it will be sent. Additionally, if over 5,000 NY residents must be notified, businesses must also notify consumer credit agencies as well.

The SHIELD Act specifies the acceptable methods of notice to NY residents. Businesses can send written notice without limitation. Telephonic or electronic notice are sufficient so long as the NY resident "expressly consented" to electronic notice, and businesses keep a log of all parties given telephonic or electronic notice. Substituted notice may be made if certain circumstances are met, such as when the breach affects over 500,000 NY residents, or the business lacks necessary information to contact affected residents.

The SHIELD Act also prescribes the format of the notice as well. The notice must include a description of the data compromised along with contact information for the affected business, and for relevant government agencies.

There are exceptions to the new breach notification protocols. If a business must already comply with federal or state breach notification laws, including HIPPA, HITECH, and Gramm-Leach Bliley Act, the business is only required to provide additional notice to NY State Police, the NY State Attorney General, the NY Department of State, and potentially credit reporting agencies as well. Additionally, if there is an inadvertent disclosure of private information affecting five hundred or less NY residents, and a business "reasonably determines" it will not lead to misuse or harm (financially or emotionally), the business only needs to create a written report of the incident and retain it for five years. If the inadvertent disclosure impacts more than five hundred NY residents, however, the business must also send its report to the NY State Attorney General within ten days of making its determination.

What if a Business Fails to Follow SHIELD Act Requirements?

The SHIELD Act authorizes the NY State Attorney General to seek injunctions and civil penalties up to $250,000 for failures to notify affected parties. Additionally, the NY State Attorney General may seek injunctions and fines up to $5,000 per violation when businesses fail to implement reasonable safeguards for private information.

Conclusion

The SHIELD Act imposes a bevy of new obligations on businesses that collect data on New York residents, whether the business is physically present in New York or not. If you are concerned about whether your business qualifies under the SHIELD Act or wish to speak to someone about how to improve your compliance with the SHIELD Act regulations, feel free to contact our firm for more information.

For more information or to discuss how changes to State and Federal laws and regulations will impact you or your business, please call or email:

Nathan M. Jerauld Ph: 315.701.6387 jerauld@bhlawpllc.com

Joseph J. Porcello Ph: 315.701.6440 jporcello@bhlawpllc.com