Lipsitz Green Scime Cambria LLP
ATTORNEYS AT LAW

SPECIAL ALERT ON DEVELOPMENTS IN

Cybersecurity Law

Preparing Your Business to Comply With New York State's SHIELD Act

As we begin a new year, organizations should continue to be prepared to address challenges arising from the ongoing proliferation of cybersecurity threats that wreak havoc on businesses and customers. In response to an increase in cybersecurity incidents, a number of state and federal laws have been passed, including New York State's recently enacted "The Stop Hacks and Improve Electronic Data Security Act," commonly referred to as the "SHIELD Act".

The SHIELD Act's provisions are not effective until March 21st of this year. This means, organizations still have time to review their existing practices and cybersecurity policies to minimize exposure to data breaches and to ensure compliance with applicable laws, including the SHIELD Act.

This communication is intended to summarize the material provisions of the SHIELD Act (and other relevant cybersecurity laws that may impact you) and to assist you in determining whether you need to comply with the new law. We have also proposed certain best practices that can be implemented to minimize the likelihood of a cybersecurity incident and to ensure compliance with relevant cybersecurity laws.

What is the SHIELD Act?

The SHIELD Act imposes requirements that are aimed to reduce the likelihood of data breaches by requiring certain individuals, businesses and organizations to adopt preventative cybersecurity programs.

Any individual, business or organization (including non-profit organizations) that owns or licenses computerized data which receive, collect, or maintain "private information" of New York residents must comply with the law. In practice, this means every employer in New York must comply with the SHIELD Act, as in all likelihood the employer will possess, at a minimum, "private information" relating to its employees.

Effective **March 21, 2020**, all individuals, businesses and organizations must implement and maintain reasonable safeguards to protect the security of New York residents' "private information."[1] Compliance is achieved by adopting a data security program that

[1] See N.Y. Gen. Bus. Law § 899-bb (McKinney's 2019)

For more information, contact one of the following attorneys at Lipsitz Green Scime Cambria.

Michael Schiavone

Michael Schiavone has provided legal guidance to businesses for over 30 years. He concentrates his practice in the areas of business law, tax planning, commercial real estate, sports law, and estate planning. Mr. Schiavone can be reached at:
Phone: 716 844 3500
E-mail: mschiavone@lglaw.com

Mark L. Stulmaker

Mark L. Stulmaker practices in the areas of employee benefits and taxation, serving as counsel to trustees of public and private pension and health and welfare benefit plans as well as to closely held businesses.
Phone: 716 849 1333, ext. 358
E-mail: mstulmaker@lglaw.com

Matthew B. Morey

Matthew B. Morey counsels clients through significant events in the life of their businesses including contractual matters, corporate and partnership tax matters, compliance matters, cost-effective solutions when conflicts arise, and strategies to assist in the growth of their businesses. Mr. Morey can be reached at:
Phone: 716 849 1333, ext. 509
E-mail: mmorey@lglaw.com

incorporates reasonable administrative, technical, and physical safeguards. *Id.*

What is "Private Information"?

"Private information" is personally identifying information of a natural person, such as:

- a social security number;
- a driver's license number or non-driver identification number;
- an email address (with accompanying password and security question information); and
- bio-metric data and health information.[2]

There are limited exceptions to the extent the data is encrypted. *Id.*

What is a Compliant Data Security Program?

In developing and implementing a compliant data security program under the SHIELD Act, the program must incorporate "reasonable safeguards" in three separate ways:

1. administratively;
2. technically; and
3. physically.

The SHIELD Act does not specifically state what constitutes "reasonable safeguards" for purposes of a compliant plan. Instead, the Shield Act provides that an organization will be considered as being in compliance if the implemented data security program includes certain minimum criteria enumerated in the statute itself, including:

- One or more employees should be designated to coordinate the data security program;

- The program should reasonably foresee internal and external cybersecurity risks and take appropriate remedial measures;

The program should require the training and management of employees in the security program practices and procedures;

- The program should assess the risks in the network and software design;

- The program should assess the risks in information processing, transmission and storage;

- The program should address the protection of unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and

- The program should dispose of private information within a reasonable amount of time after it is no longer needed for business purposes.

The "Small Business" Exception

If you are a "small business," then you only need to adopt and maintain a "reasonable" data security program given the size and complexity of the business, the scope of the business' activities, and sensitivity of personal information collected or maintained by the business.[3] Accordingly, the criteria enumerated above may or may not need to be adopted in the data security program of the "small business," depending on the size and complexity of the business itself.

A "small business" is any person or business:

i. with fewer than fifty (50) employees; or
ii. that has less than Three Million Dollars in gross annual revenue in each of the last three (3) fiscal years; or
iii. that has less than Five Million Dollars in year-end total assets, calculated in accordance with generally accepted accounting principles.[4]

[2] See N.Y. Gen Bus. Law. § 899-aa(b) (McKinney's 2019)
[3] See N.Y. Gen. Bus. Law § 899-bb(1)(c), 899-bb(2)(c) (McKinney's 2019)
[4] See N.Y. Gen. Bus. Law § 899-bb(1)(c) (McKinney's 2019)

Moreover, in the event an organization has a data security program that already complies with the requirements of certain other federal and state laws, such as the regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPPA) or the New York Department of Financial Security Regulations, such data security programs will be deemed in compliance for purposes of the requirements of the SHEILD Act.

Notice Requirements

Covered individuals and businesses are also obligated to disclose any breach of the security of their data systems to New York residents whose "private information" was, or is reasonably likely to have been, accessed or acquired without authorization by a third party.[5]

The disclosure must be made without unreasonable delay, and, in certain instances, disclosure may also need to be made to law enforcement and the New York Attorney General. *Id.* Further, notice must be made in the specific manner directed by statute. *Id.*

What if you don't comply with the SHIELD Act?

In the event of a failure to comply, the New York Attorney General is authorized to enforce the law and impose fines. Further, although the statute specifically provides that it does not confer a private right of action for residents in the event of noncompliance (the right to maintain a class action lawsuit), failure to comply may be cited as an example of a company's malfeasance in maintaining appropriate safeguards of New York residents' personal information.

Are there other laws with which I need to be concerned?

There are many laws in other jurisdictions that may apply to businesses and employers based in New York. Unfortunately, such an analysis is beyond the scope of this communication. However, depending on the scope of your business and where you do business (particularly if the scope of your business is on a national or international scale), it is likely that your organization will be impacted by other jurisdictions' specific cybersecurity and privacy laws. Two such laws include the General Data Protection Rule (GDPR) in Europe and the recently enacted California Consumer Privacy Act.

Should I obtain Cybersecurity Insurance?

In light of the increased number of cybersecurity incidents and data breaches, it's natural that some organizations will inquire whether they should obtain cyber insurance policies to insure against losses arising from such incidents.

Generally, most businesses maintain commercial general liability (CGL) insurance policies. However, those policies typically do not insure for losses arising from cyber-attacks or other data breaches. Accordingly, you may want to obtain cyber insurance coverage (in addition to blanket commercial general liability (CGL) insurance) to mitigate against the impact of losses arising from data breaches and failures to comply with specific jurisdictions' cybersecurity and privacy laws. This requires an analysis of:

1. the scope of the business and risk associated with cybersecurity threats and data breaches;
2. the cost and availability of the insurance; and
3. exclusions from coverage.

Each policy is different, thus requiring an analysis on a policy by policy basis.

In addition, owners should consider the type of coverage that is provided. For example, first-party coverage would insure a business for actual damage incurred to

[5] See N.Y. Gen. Bus. Law § 899-aa (McKinney's 2019)

the business' own property in the event of a cyber event, while third-party coverage would insure the business from claims made by third parties (such as a claim by a customer that its personal information was hacked). In certain situations, insurance may be able to insure against fines imposed as a result of a business' failure to comply with specific cybersecurity laws (such as the SHIELD Act), although those policies are likely to be expensive and have numerous exclusions to coverage.

In sum, cyber insurance may help mitigate certain losses incurred as a result of a data breach or other cybersecurity event. However, a detailed analysis of the scope of the business, specific coverage provided by a policy, and the cost of the policy would need to be undertaken.

Conclusion

As we start a new year, organizations will continue to struggle with how to mitigate against losses arising from cybersecurity and data breaches, let alone complying with the number of new laws passed to address these concerns. Accordingly, in light of the impending March 21st deadline to comply with the SHIELD Act, we encourage you to take time now to:

- Review your existing record retention and cybersecurity plans to determine whether they comply with the requirements of the SHIELD Act. If you don't have an existing data security program, businesses should take immediate steps to consult with their legal counsel and other advisors to develop, implement and maintain a compliant program by the March 21st deadline.
- Review the scope of your business and determine whether other jurisdictions' specific privacy and data security laws apply to where you do business and who you do business with. In many cases, compliance with state or foreign laws can be triggered even with minimal contact to that jurisdiction. Accordingly, an in-depth review with your legal counsel may be necessary, resulting in modifications to your record retention, privacy and cybersecurity policies.
- Review with your legal counsel and insurance advisor your existing insurance policies and determine whether it is economically prudent to obtain a cyber insurance policy to mitigate against losses arising from data breaches or fines associated with noncompliance of specific cybersecurity laws, such as the SHIELD Act.
- Regularly communicate with employees on the importance of being aware of the increased occurrence of cybersecurity threats, including providing on-going technical training as needed and alerts on potential cybersecurity threats.
- Designate a specific employee at your company (if not your IT department) to be responsible for maintenance of your company's record retention and cybersecurity plans, as well as monitoring federal and state cybersecurity and data privacy laws.