KNOW GREATER VALUE™

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

NY SHIELD Act: Increased Cyber Protections

By Thomas J. DeMayo, Principal, Cyber Risk Management

As the cybersecurity threat continues to escalate, New York has joined the expanding list of states and countries to impose obligations on businesses to protect private information. On July 26, 2019, Gov. Andrew Cuomo signed into law the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act).

The SHIELD Act, which amends the current NYS Information Security Breach and Notification Act, has the following key changes:

- The definition of "private information" has been expanded.
- Businesses will be required to implement specific safeguards to protect the private information of New York residents.
- The definition of what constitutes a breach of private information has been broadened.
- The Act removes the requirement that the person or business must operate in New York.

When Does It Go into Effect?

The SHIELD Act goes into effect March 21, 2020.

Who Does It Apply to?

The SHIELD Act will apply to any person or business that owns or licenses personal private data in electronic form, regardless if the person or business operates in New York. For example, a person or business may have physical operations in New Jersey, but if that office has employees and customers that reside in New York, they will be subject to the Act and its requirements. Like many recent privacy laws, such as the California Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR), it is becoming clear that physical boundaries will not restrict the reach of these laws and any future laws to be adopted by other states and countries.

What Is Private Information?

New York defines "Private Information" as "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 simple terms: private information is information that is about a person, but not in and of itself, considered sensitive. "Private Information," which businesses will have a duty to protect and an obligation to report if breached, is defined as the following:

- Any "Private Information" in combination with one, or more of the following data sets:

    - Social Security number;
    - driver's license number or non-driver identification card number;
    - account number, credit or debit card number, in combination with a security code or without, if the numbers can be used alone to access the financial account of the individual.

- biometric information, meaning 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 representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity; OR
- 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.

What Data Security Protections Are Required?

The SHIELD Act requires the implementation of "reasonable" administrative, technical, and physical security safeguards. What will be the most impactful is that the Act defines what will be considered "reasonable" as 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 safeguards, 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.

What Is Considered a Breach and Who to Notify?

The SHIELD Act substantially changes the definition of a breach. Prior to the SHIELD Act, the definition of a breach was restricted to the unauthorized acquisition of private information. The SHIELD Act expands the definition to also include the unauthorized access to private information. The inclusion of unauthorized access to private information will result in a substantial increase in the number of businesses that will be required to report a breach.

Should a breach occur, you will need to notify the impacted individuals as well as: the New York State Attorney General, the Department of State, and the Division of State Police. If the breach impacts more than 5,000 New York residents, consumer reporting agencies must also be notified. If you are already subject to HIPAA, GLBA, or the NY DFS 500 Cyber Regulation, duplicate notifications to the individual is not required.

What Are the Penalties?

The good news is that the penalties have a tiered structure. Should you blatantly ignore the requirements of the regulation and not implement reasonable safeguards as defined, fines could be up to $250,000.

Should violations occur and you have implemented reasonable safeguards, penalties will be limited to $5,000. The SHIELD Act does not permit a private right of action.

How Can We Help?

PKF O'Connor Davies has a team of professionals dedicated to cybersecurity, information security, and data privacy who can assist your business in further understanding the requirements and help you develop a practical strategy in developing a cybersecurity program designed to not only satisfy the requirements of the SHIELD Act, but more importantly, protect your business, your customers, your employees and your hard earned reputation.

Contact Us

We welcome your comments, insights and questions. Please contact our Cyber Risk Management Principal directly to explore how we may help you safeguard the security of your organization, business, clients and constituency.

Thomas J. DeMayo, Principal, Cyber Risk Management
CISSP, CISA, CIPP/US CPT CEH CHFI MCSE

PKF O'Connor Davies, LLP
665 Fifth Avenue, New York, NY, 10022
212.867.8000 or 646.449.6353 (direct)
tdemayo@pkfod.com

About PKF O'Connor Davies

PKF O'Connor Davies, LLP is a full-service certified public accounting and advisory firm with a long history of serving clients both domestically and internationally. With roots tracing to 1891, nine offices in New York, New Jersey, Connecticut and Maryland, and more than 700 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is ranked 28th on *Accounting Today's* 2017 "Top 100 Firms" list and is recognized as one of the "Top 10 Fastest-Growing Firms." PKF O'Connor Davies is also recognized as a "Leader in Audit and Accounting" and is ranked among the "Top Firms in the Mid-Atlantic," by *Accounting Today.* In 2017, PKF O'Connor Davies was named one of the 50 best accounting employers to work for in North America, by *Vault*.

PKF O'Connor Davies is the lead North American representative in PKF International, a global network of legally independent accounting and advisory firms located in 440 locations, in 150 countries around the world.