Cybersecurity & Data Privacy and Consumer Financial Services Update

New York's new "Shield Act" applies to those using "private information" of a NY resident

November 1, 2019

Intro

New York has enacted legislation to expand its cybersecurity and data breach law with the **Stop Hacks and Improve Electronic Data Security Act** (the "Shield Act"). The Shield Act, which becomes effective on March 21, 2020, amends, and more importantly broadens, the scope of the general business and state technology laws in New York. The expansion of New York's governing cybersecurity and data breach laws arrives on the heels of the Equifax data breach settlement, in which Equifax reached a global settlement with the Federal Trade Commission, the largest in history, after a data breach exposed the personal information of 147 million people across the 50 U.S. states and territories. With these supplements to the existing laws, New York residents will have increased cybersecurity and data protections. Correspondingly, this law will increase the burdens and obligations for individuals and businesses, regardless of whether they conduct business in New York State, to carefully navigate these changes to ensure compliance.

Scope

Among the most important changes, the Shield Act expands New York's data protection and breach notification laws so that they are no longer limited to persons or entities that conduct business in New York State. The requirements are now **applicable to any person or entity which owns or licenses computerized data that includes "private information" of a New York resident**. The Shield Act also expands the definition of "private information" to mean either:

(i) **personal information** consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired:

(1) social security number;

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

(3) 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;

(4) account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or

(5) 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 is used to authenticate or ascertain the individual's identity; or

(ii) 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.

Requirements

Under the Shield Act any person or business that owns or licenses computerized data which includes private information of a resident of New York is now required 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. A person or business shall be deemed compliant if it either: (i) is a compliant regulated entity[1], or (ii) implements 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 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;

1 "Compliant regulated entity" means any person or business that is subject to, and in compliance with, any of the following data security requirements: (i) regulations promulgated pursuant to Title V of the federal Gramm- 44 Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time; (ii) regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended from time to time, and the Health Information Technology for Economic and Clinical Health Act, as amended from time to time; (iii) part five hundred of title twenty-three of the official compilation of codes, rules and regulations of the state of New York, as amended from time to time (i.e., the Department of Financial Services Cybersecurity Regulations); or (iv) any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such rules, regulations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts.

(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.

Compliance through meeting the definition of a "compliant regulated entity" means that financial institutions, entities holding licenses or authorizations from the Department of Financial Services, and other regulated industries are deemed compliant by meeting data security requirements imposed on them by other statutes/regulations.

Notice Provision Expanded

In the event of a breach or exposure, the Shield Act contains various documentation and notification provisions that specify how notice must be communicated to the affected individual and/or New York State, depending on the depth and scope of a breach or exposure. Any person or business that owns or licenses computerized data which includes private information of a New York resident shall **disclose any breach** of the security of the system following discovery or notification of the breach in the security of the system **to the resident** of New York whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. **The Shield Act enlarged the notice requirement provision to include private information that was, or is reasonably believed to have been accessed**, not just acquired. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the integrity of the system.[2]

Enforcement

The Shield Act specifies that the amendments do not create a private right of action, meaning New York residents do not personally have an actionable claim under the Shield Act. Consequently, the policing power of the Shield Act remains exclusively in the confines of the State of New York, and more specifically the state's Attorney General.

Increased Penalties

The penalties for a violation of the Shield Act range from an injunction to enjoin and restrain the continuation of the violation, to a possible award for cost or losses incurred by the person entitled to receive notice. In the latter case, if notice was required but not provided, damages may also include consequential financial losses. However, if a court finds that a person or a business violated the Shield Act, knowingly or recklessly, the court may impose a civil penalty of the greater of $5,000 or up to $20 per instance of failed notification, increased from $10 per instance, provided that the latter amount shall not exceed $250,000, increased from $150,000.

2 However, "personal information" excludes information that is "publicly available," which generally means information that is lawfully made available from federal, state, or local government records.

Key Take-Aways

Individuals and business subject to Shield Act should review the security systems and protocols they have in place to protect private information to ensure that they are adequate and complaint with the requirements listed above. Due to the nuances and complexities of New York's cybersecurity and data breach laws, businesses and individuals subject to the Shield Act would be prudent to seek counsel, to navigate this ever-developing landscape.

Summary

The Shield Act greatly expands existing New York's cybersecurity and data breach laws and extends its reach to include businesses across the country. As such, it places more responsibility and onus on those that maintain private information of New York residents, but the Shield Act does offer specific guidelines and terms for compliance. Even though the amendments do not offer a private right of action, the Shield Act **increases the potential for civil liability** that can cost as much as $250,000 upon the determination of a knowing or reckless violation.

.....

If you have questions about this alert, please contact the author or any member of the firm's Cybersecurity and Data Privacy Team or Consumer Financial Services Compliance and Litigation Teams.

Odera Chuke
Associate, New York City
(646) 362-4048
ochuke@mcglinchey.com