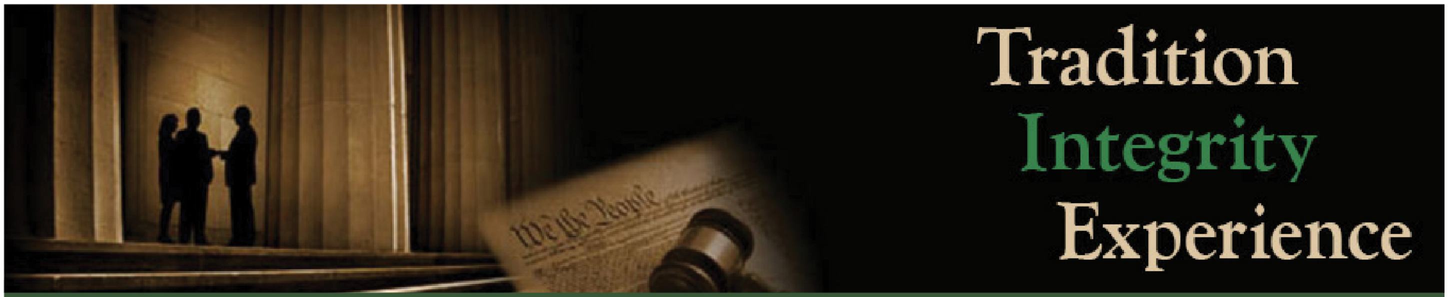
Putney

Putney, Twombly, Hall & Hirson LLP | *Counselors at Law*
521 Fifth Avenue | New York, NY 10175 | (212) 682-0020 | putneylaw.com



CLIENT UPDATE

AUGUST 15, 2019

New York State Enacts S.H.I.E.L.D. Act Imposing Heightened Data Security and Breach Notification Requirements on Employers

On July 25, 2019, New York Governor Andrew Cuomo Governor signed legislation to protect New Yorkers against security breaches. The Stop Hacks and Improve Electronic Data Security, or S.H.I.E.L.D. Act (the "Act"), imposes tougher obligations on businesses handling private data to provide proper notification to affected consumers in the event of a security breach. The Act takes effect on March 21, 2020.

The Act requires the implementation of a data security program, including risk assessment measures, workforce training, incident response planning and testing, and secure data destruction protocols. The Act covers all businesses and individuals -- regardless of size or location -- who collect private information on New York State residents.

What "Private Information" Does the Act Protect?

Under the Act, "private information" means:

> Any individually identifiable information, such as a name, number, or other identifier that can be used to identify a natural person, in combination with any one or more of the following data elements:
>
> - social security number;
> - driver's license number or non-driver identification card number;

- 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; 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
- 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 Measures Must Employers Take to Protect "Private Information"?

The Act requires that "any person or business" that owns or licenses computerized data that includes private information of a New York State resident "shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information." To comply with the Act, businesses must implement a data security program to protect private information that includes:

A. Reasonable Administrative Safeguards, including designation of one or more employees to coordinate the security program, identification of reasonably foreseeable external and insider risks, assessment of existing safeguards, workforce cybersecurity training, and retaining a service provider(s) contractor capable of maintaining safeguards and requiring those safeguards;

B. Reasonable Technical Safeguards, including network risk assessments, software design, and information processing, transmission, and storage, implementation of measures to detect, prevent, and respond to system failures, and regular testing and monitoring of key controls; and

C. Reasonable Physical Safeguards, that may include detection, prevention and response to intrusions, and protections against unauthorized access to or use of private information during or after collection, transportation, and destruction or disposal of the information.

It should be noted that businesses that are covered by, and in compliance with, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act ("HIPAA"), and/or the New York State Department of Financial Services ("NYSDFS") cybersecurity regulations (23 NYCRR 500) are deemed to be in compliance with the Act.

Penalties for Noncompliance with the Act

The Act does not authorize a private right of action. Therefore, class action litigation is not available. However, the attorney general may bring an action to enjoin violations of the Act and obtain civil penalties. For data breach notification violations that are not reckless or knowing, the court may award damages for actual costs or losses incurred by a person entitled to notice, including consequential financial losses. For knowing and reckless violations, the court may impose penalties of the greater of $5,000 dollars or up to $20 per instance up to $250,000. For reasonable safeguard requirement violations, the court may impose penalties of not more than $5,000 per violation.

Takeaway for Employers

Employers businesses handling private data should use this time to make sure their data protection practices and safeguards comply with the Act. As the Act affects New York employer, regardless of size and location, we encourage you to contact us for assistance in complying therewith.

* * *

If you have any questions regarding this alert, or any other issue, please do not hesitate to contact us.

PUTNEY, TWOMBLY, HALL & HIRSON LLP