Moritt Hock & Hamroff LLP
ATTORNEYS AT LAW
STRENGTH IN PARTNERSHIP®

ALERT

April 2020

New York SHIELD Act Now In Effect: Has Your Company Adequately Protected Private Information?

By: Terese L. Arenth & Stephen Breidenbach

If your business collects private information from a New York State resident, be aware of a recently effective New York law that requires companies to strengthen their data security programs and significantly expands a company's potential liability. When cybersecurity risks are at an all-time high as hackers seize on the COVID-19 pandemic to launch more attacks, it is advisable to take a closer look at how your business is protecting personal data.

As of March 21, 2020, the New York "Stop Hacks and Improve Electronic Data Security Act" ("SHIELD Act") specifically requires any person or business collecting private information of a New York resident to develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of that private information, including but not limited to, disposal of the data.

Private Information was amended to now include: (1) social security numbers; (2) driver's license numbers or non-driver identification card numbers; (3) account numbers, credit or debit card numbers, if those numbers would permit access to an individual's financial account; (4) biometric information; or (5) a user name or e-mail address in combination with information that would permit access to an online account.

The SHIELD Act enumerates several administrative, technical and physical safeguards that larger businesses must develop, implement and maintain. These safeguards include, but are not limited to, the following:

Reasonable Administrative Safeguards: (1) identifying reasonably foreseeable internal and external risks; (2) designating one or more employees to coordinate the security program; (3) assessing the sufficiency of safeguards in place to control identified risks; (4) training and managing employees in the security program's practices and procedures; (5) selecting service providers capable of maintaining the appropriate safeguards and requiring those safeguards by contract; and (6) adjusting the security program in light of business changes or new circumstances.

Moritt Hock & Hamroff LLP
ATTORNEYS AT LAW
STRENGTH IN PARTNERSHIP®

ALERT

Reasonable Technical Safeguards: (1) assessing risks in network and software design; (2) assessing risks in information processing, transmission, storage and disposal; (3) detecting, preventing and responding to attacks, system failures and intrusions; and (4) regularly testing and monitoring the effectiveness of key controls, systems and procedures.

Reasonable Physical Safeguards: (1) assessing the risks of information storage and disposal; (2) detecting, preventing and responding to intrusions; (3) protecting against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and (4) disposing 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.

For small businesses, the Act simply provides that "the small business's security program [should contain] reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers." *N.Y. Gen. Bus. Law §899-bb(2)(c)*. A small business is any person or business with fewer than 50 employees, less than three million dollars in gross annual revenue in each of the last three fiscal years, or less than five million dollars in year-end total assets.

While the SHIELD Act does not provide for a private right of action, it does impose civil penalties of not more than $5,000 for failing to implement reasonable security and, under New York's Breach Notification law, potential penalties are the greater of $5,000 or up to $20 per instance for failing to notify affected consumers of a data breach, not to exceed $250,000. *N.Y. Gen. Bus. Law §899-aa(6)(a) and §350-d*.

The potential quagmire with the SHIELD Act and similar laws in effect, however, is that despite all of these legal requirements and safeguards, what constitutes "reasonable security" remains ambiguous. While most laws currently provide that the safeguards implemented by a business should be reasonable and appropriate given the size of the business and the information they collect, agencies such as the Federal Trade Commission have recognized that there is no such thing as perfect security, and that security is a continuing process that requires the business to detect risks and adjust their safeguards accordingly. *See* NIST Cybersecurity Framework & the FTC.

Consequently, as best practices, businesses seeking to come into compliance are well-advised to review sources such as the FTC's published guidance on requirements for their business type. Many of the FTC guidelines detail the types of safeguards businesses should implement, including the FTC's guidelines for small businesses and the FTC's explanatory material on the Cybersecurity Framework published by the National Institute of Standards and Technology ("NIST") (a voluntary framework that includes standards,

Moritt Hock & Hamroff LLP
ATTORNEYS AT LAW
STRENGTH IN PARTNERSHIP®

ALERT

guidelines and best practices to manage cybersecurity risk). *See* FTC Tips Cybersecurity For Small Business; NIST Cybersecurity Framework & the FTC. *See also* Financial Institutions & Customer Information: Complying With The Safeguard Rule; FTC-Start With Security: A Guide For Business.

Most businesses collect and maintain sensitive personal information about their customers. The key takeaway is to first assess the type of business that you operate and the types of personal information that you collect. From that starting point, develop, implement and maintain a sound security plan to collect only the information that you need, to keep that information safe, and to dispose of it securely. This will provide the necessary foundation to help your business meet its legal obligations and protect that sensitive data.

If you have any questions regarding how to navigate the SHIELD Act requirements, please feel free to contact Terese Arenth (tarenth@moritthock.com or (516) 880-7235) or Stephen Breidenbach (sbreidenbach@moritthock.com or (516) 880-7285). We are here to assist you.

◆ ◆ ◆ ◆ ◆

This Alert is published solely for the interests of friends and clients of Moritt Hock & Hamroff LLP for informational purposes only and should in no way be relied upon or construed as legal advice.

Terese Arenth is a Partner with the firm and serves as Chair of its Promotional Marketing and Advertising Practice Group, as well as Co-Chair of its Cybersecurity, Privacy and Technology Practice Group, both of which are within the firm's Intellectual Property Department. Ms. Arenth concentrates her practice in promotional marketing, advertising and Internet/new media, as well as privacy and technology related matters. She also has significant involvement in the firm's intellectual property practice area and vast experience in commercial and corporate litigation.

Stephen Breidenbach is an associate with the firm and serves as Co-Chair of its Cybersecurity, Privacy &Technology Practice Group within the firm's Intellectual Property Department. Mr. Breidenbach concentrates his practice in technology related legal matters, including cybersecurity and privacy compliance

400 Garden City Plaza, Garden City, NY 11530 | Tel (516) 873-2000 | Fax (516) 873-2010
1407 Broadway, 39th Floor, New York, NY 10018 | Tel (212) 239-2000 | Fax (212) 239-7277
www.moritthock.com