White and Williams LLP

Taking a Look at the New York SHIELD Act

Cyber Law and Data Protection Alert **| August 16, 2019**

By: Sedgwick M. Jeanite

On July 25, 2019, the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) was signed into law. The SHIELD Act amends New York notification requirements for unauthorized access to private information, including biometric data, and adds new requirements for businesses and persons that own or license private information of a New York resident to comply with reasonable data security protections.

The SHIELD Act broadens the definition of "breach of the security of the system" to include incidents involving "access to" private information, regardless of whether the incident resulted in the acquisition of that information. The SHIELD Act also expands the definition of "private information" to include (i) account numbers, credit or debit card numbers (if circumstances exist that could allow such number to be used to access an individual's financial account without additional identifying information), security codes, access codes or passwords, and (ii) biometric information. The SHIELD Act defines biometric information as 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 or digital representation of biometric data which are used to authenticate or ascertain the individual's identity. With the enactment of the SHIELD Act, New York becomes the latest state in the United States to regulate the collection of biometric information.

The SHIELD Act amends the General Business Law by enacting a "reasonable security requirement." This requirement obligates businesses that own or license computerized data that includes the "private information" of New York residents 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. The new data security requirements cast a wide net and will apply to companies whether or not they operate in New York. This is noteworthy because the SHIELD Act arguably applies to any company that collects computerized data of New York residents and places a significant burden on those companies to develop, implement and maintain reasonable safeguards to protect private information.

The "reasonable safeguards" include administrative, technical, and physical safeguards identified in the SHIELD Act. Small businesses (less than 50 employees, less than $3 million in gross annual revenues and less than $5 million in year-end total assets) are able to comply with the requirement if they have a data security program that contains reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the activities of the small business and the sensitivity of the personal information the small business collects from or about consumers.

Additional changes brought about by the SHIELD Act including the following:

- Broadens the jurisdictional reach of current New York law to cover any person or business that owns or licenses computerized data that includes the private information of a New York resident. The statute essentially requires compliance with the breach notification requirements by any person or business to which the law applies, regardless of whether the person or business conducts business in New York.
- Enhances penalties for knowing and reckless violations and permits a court to impose a civil penalty of the greater of $5,000 or up to $20 per instance of failed notification, provided that the latter will not exceed $250,000.
- Extends the statute of limitations from two years to three years after either the date on which the state attorney general becomes aware of the violation, or the date of notice to the state attorney general, whichever is earlier. An action must be brought within six years after the discovery of the breach unless the person or business took steps to hide it.

The SHIELD Act does not create a private right of action and permits enforcement only by the Attorney General. The amendments to the New York breach notification law required by the SHIELD Act will take effect on October 23, 2019. The new data security requirements become effective on March 21, 2020.

If you have questions or would like additional information, please contact Sedgwick Jeanite (jeanites@whiteandwilliams.com; 212.631.4413) or another member of the Cyber Law and Data Protection Group.

This correspondence should not be construed as legal advice or legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only, and you are urged to consult a lawyer concerning your own situation and legal questions.