LEGALcurrents®

July 30, 2019

Harter Secrest & Emery LLP

ATTORNEYS AND COUNSELORS

PRIVACY AND DATA SECURITY

GOVERNOR CUOMO SIGNS NEW YORK SHIELD ACT INTO LAW: A HOST OF BREACH NOTIFICATION AND DATA SECURITY CHANGES ARE COMING

Authors: F. Paul Greene and Daniel J. Altieri

On July 25, 2019, Governor Cuomo, as expected, signed into law the "Stop Hacks and Improve Electronic Data Security Act" (the "SHIELD Act" or "Act"), which significantly amends New York's existing data breach notification statute, General Business Law § 899-aa. Also, in keeping up with revisions to various sister states' statutes, the SHIELD Act also creates a new § 899-bb, effective 240 days from the date of the Governor's signature, which requires comprehensive implementation of substantive data security controls for businesses and other organizations worldwide that process the "private information" of even one New York resident. The Act's most noteworthy elements are summarized briefly below.

Broader reach. More persons and entities are covered under the new law. Previously, New York's data breach notification statute limited its application to "any person or business which conducts business in New York." Under the SHIELD Act, any person or business, anywhere in the world, that owns or licenses "private information" concerning a resident of New York is now in scope under the law. In other words, as the Act is written, a business' substantive contacts to New York, such as location or state of incorporation, are irrelevant. If the business processes a New York resident's private information, it is on the hook for compliance. The Act also lowers the threshold for breach reporting, which was previously limited to circumstances showing unauthorized "acquisition" of a New Yorker's private information. Under the SHIELD Act, mere "access" to such information is enough to create a reporting duty.

Broader definition of "private information." More information is protected under the new law. The SHIELD Act expands the existing definition of protected "private information," adding an individual's username and password for an online account, as well as various types of biometric information, including fingerprints and voiceprints. The Act also clarifies that a compromise of an account number, or credit or debit card number, *even without a compromise of an associated access code or password*, is reportable, "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."

Notification exception. The SHIELD Act creates a notification exception for situations involving "inadvertent disclosure by persons authorized to access private information" if "such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials." A person or business taking advantage of this caveat must document its determination and maintain it for at least five years. If more than five hundred New York residents are affected, the person or business must provide that written determination to the New York Attorney General within ten days of making it.

Substantive security requirements. In what will likely—and rightfully—garner the most attention, by way of new § 899-bb, the SHIELD Act creates, for the first time, substantive security requirements for persons or businesses that own or license the private information of a New York resident, with very limited exceptions. Specifically, § 899-bb requires "reasonable safeguards to protect the security, confidentiality and integrity of

private information" and provides criteria by which a person or business will be "deemed to be in compliance" with this otherwise generic requirement.

A person or business covered under § 899-bb can either show that it is a "compliant regulated entity," as defined in the statute, or it can implement a data security program including certain administrative, technical, and physical safeguards identified in the statute. These include, under administrative safeguards, designating one or more employees to coordinate the program, identifying reasonably foreseeable internal and external risks to the organization, and adjusting the security program in light of business changes or new circumstances. In relation to technical and physical safeguards, § 899-bb requires assessing risks in network and software design, testing and monitoring key controls, assessing risks of information storage and disposal, and disposing of private information within a reasonable amount of time after it is no longer needed.

Section 899-bb expressly excludes any private right of action for any violation of the statute. Lest anyone think the new provisions are all bark but no bite, however, the Act provides that violations shall be deemed unfair or deceptive practices, which themselves are actionable under New York's "little FTC Act," N.Y. Gen. Bus. Law § 349.

The Take-Away

Today, where a business' very existence, let alone its ability to successfully compete in the marketplace, depends upon its efficient use, processing, and storage of personal information, the SHIELD Act brings with it a wide range of new legal and practical considerations.

Although it remains to be seen how aggressive the State will be in ensuring statutory compliance, when signing the Act into law, Governor Cuomo foreshadowed what is to come: "The stark reality is security breaches are becoming more frequent and with this legislation New York is taking steps to increase protections for consumers and holding these companies accountable when they mishandle sensitive data."

Any business, anywhere in the world, with contact with New Yorkers is subject to the SHIELD Act, and should plan accordingly, including by evaluating existing information security programs, incident response plans, and recent risk assessments, if any, for SHIELD Act compliance.

If you would like more information regarding the SHIELD Act, please contact a member of Harter Secrest & Emery LLP's Privacy and Data Security practice group or visit www.hselaw.com.

F. Paul Greene, 585.231.1435, fgreene@hselaw.com

Daniel J. Altieri, 716.844.3741, daltieri@hselaw.com