New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 262—NO. 20
MONDAY, JULY 29, 2019

Outside Counsel

Expert Analysis

NY SHIELD Act Promises More Data Breach Enforcement, and International Reach

By **Paul Greene**

On July 25, the Governor signed into law Senate Bill 5575, the "Stop Hacks and Improve Electronic Data Security Act" (the SHIELD Act), which had passed the Legislature on June 17, 2019. The SHIELD Act was originally proposed in the 2017-2018 session, but died in committee. It returned with gusto in 2019: proposed in the Legislature in February and passing both houses in a little more than four months.

The SHIELD Act does two things, primarily: It amends New York's data breach notification statute, General Business Law §899-aa to update its definitions, and also creates a new §899-bb requiring substantive data security controls of any person or business that owns or licenses computerized data including the defined "private information" of a New York resident. In doing this, New York has brought itself into line with a number of states concerning how they define a data breach, and, where applicable, what substantive security controls they require. The SHIELD Act also adopts the approach of several states, including Massachusetts, Florida, and Nevada, which purport to extend their jurisdictional reach to any person or business, anywhere in the world, that owns or licenses data concerning a resident of that state. In this regard, New York has converted §899-aa into, and created a new §899-bb that functions as, a possession statute: If you process computerized private information concerning a New Yorker, you now fall under the statute's requirements.

This change in territorial scope, of course, vastly increases the pool of persons and entities that are subject to possible enforcement under §899-aa, and creates an entirely new ground for enforcement against this increased pool under §899-bb. The statute's expanded definition of "private information" also increases the likelihood of enforcement. Before the SHIELD Act, many security incidents involving New Yorkers would be reportable under other regulatory frameworks—for instance under another state's laws or the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended—but would not be reportable under §899-aa. This is because, under §899-aa, the definition of "private information" that could give rise to a breach was limited

New York has brought itself into line with a number of states concerning how they define a data breach, and, where applicable, what substantive security controls they require.

F. PAUL GREENE *is a partner and chair of the privacy and data security practice group at Harter Secrest & Emery, a full-service business law firm with offices throughout New York. He can be reached at fgreene@hselaw.com.*

to an identifier, such as name, number, or personal mark, plus Social Security number, driver's license number or non-driver identification card number, or account number, credit or debit card number, in combination with a code or password that would permit access to an individual's financial account.

The SHIELD Act expands this definition, adding username and password for an online account as well as biometric information. The SHIELD Act also makes clear that compromise of an account number, or credit or debit card number, even without compromise of an 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."

Missing from the definition of "private information," but present in other states' data breach notification laws, are elements such as digital signature (North Carolina), passport number (Alabama), medical information (California), DNA profile (Delaware), and mother's maiden name (North Dakota). In addition, §899-aa remains focused on "computerized data," with a paper breach remaining outside of its scope. The data breach notification requirements in Massachusetts, by contrast, have long treated paper and electronic breaches in the same fashion. See Mass. Gen. Laws ch. 93H §1(a) (including paper records within the scope of the Massachusetts data breach notification statute).

Section 899-aa also changes breach notification duties, including the notification trigger. Pre-amendment, §899-aa required notification to affected individuals "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 reasonable integrity of the system." The SHIELD Act removes the "reasonable" qualifier from this definition, leaving the rest intact. It also creates a reporting 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 500 New York residents are affected, the person or business must provide that written determination to the New York Attorney General within 10 days of making it.

> As for enforcement, §899-bb expressly states that it does not create a private right of action, but enterprising litigants are certain to refer to its substantive security requirements as a new floor in New York, at least when alleging negligence in relation to a data breach.

In the new §899-bb, the SHIELD Act creates, for the first time, substantive security requirements for all persons or businesses that own or license the private information of a New York resident. In doing so, §899-bb threads the regulatory needle between states that simply require "reasonable" information security efforts, such as Delaware, without detailing specific safeguards that must be implemented, and those that prescribe more substantive policies and controls, such as Massachusetts. Section 899-bb does this by requiring "reasonable safeguards to protect the security, confidentiality and integrity of private information, but also providing criteria by which a person or business would be "deemed to be in compliance" with this generic requirement.

Specifically, a person or business covered under §899-bb can either show that it is a defined "compliant regulated entity," 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 reason-

ably foreseeable internal and external risks to the organization, and adjusting the security program in light of business changes or new circumstances. In this regard, §899-aa is similar to both 201 C.M.R. 17.03 in Massachusetts and the Gramm-Leach-Bliley Act (GLBA) Safeguards rule, 16 C.F.R. §§314.3 and 313.4, which include nearly identical requirements.

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. These too are familiar controls, borrowed generally from the New York Department of Financial Services cybersecurity regulations (23 N.Y.C.R.R. Part 500), the GLBA Safeguards Rule, or HIPAA.

As for a "compliant regulated entity," §899-bb defines that term as any person or business subject to and compliant with the security requirements of GLBA, HIPAA, Part 500, or "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 … ." Importantly, §899-bb does not include entities regulated under other state or international law as "compliant regulated entities." Section §899-bb is also silent as to how an entity can prove that it is compliant with any of these regulatory schemes. Accordingly, because compliance is measured at a point in time, it is possible under §899-bb for a bank subject to GLBA or a hospital subject to HIPAA to fall out of compliance with their primary regulator, and therefore become ineligible for the "compliant regulated entity" caveat built into §899-bb.

As for enforcement, §899-bb expressly states that it does not create a private right of action, but enterprising litigants are certain to refer to its substantive security requirements as a new floor in New York, at least when alleging negligence in relation to a data breach. Further, §899-bb makes violations of its provisions a violation of the state's "little FTC Act," N.Y. Gen. Bus. Law §349. In many states, including in New York, this has been common practice, using unfair and deceptive acts and practices laws to enforce or investigate in relation to a data breach. If there was any question as to this practice in New York, §899-bb now codifies it.

Given this added support to enforcement efforts, the vastly expanded reach to §899-aa, and the new provisions of §899-bb—which potentially cover entities regulated under other security frameworks such as GLBA and HIPAA, inasmuch as they are out of compliance with those frameworks—the SHIELD Act will certainly bring more enforcement, as well as an increase in breach reporting in New York. Many would welcome this development, as reporting obligations in New York have lagged behind other states. Others will feel the pinch of the new requirements, especially concerning reasonable data security safeguards, as they may not have not been required by law to engage in such practices before. Whatever the reception, enforcement will show just what the state expects under these requirements, which will remain fluid until defined in more detail in practice, either via enforcement efforts and consent decrees, or in the courts.