Proskauer

The New SHIELD Act Changes Breach Notification Rules and Data Security Standards for New Yorkers' Personal Information

August 21, 2019

Reflecting the movement to toughen data security laws on a state-by-state basis, on July 25, 2019, Governor Cuomo signed into law the Stop Hacks and Improve Electronic Data Security Act (the "**SHIELD Act**" or the "**Act**"). The Act amends New York State's current data breach notification law, which covers breaches of certain personally-identifiable computerized data (referred to in the New York breach law as "**Private Information**"). The Act also breaks new ground by imposing substantive data security requirements on businesses that own or lease the Private Information of New York residents, regardless of whether the businesses otherwise conduct business in New York State. Both portions of the Act are backed by potential civil penalties for noncompliance.

In addition, in an unusual move, the SHIELD Act imposes new data breach reporting requirements on entities that are "covered entities" under the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"). The Act requires HIPAA covered entities to report to the New York State Attorney General in the event data breach reporting to the Secretary of Health and Human Services is "required" under HIPAA, even if the data at issue does not count as Private Information under New York's breach notification law, and apparently even if the information subject to HIPAA breach reporting was not in electronic form. N.Y. Gen. Bus. Law § 899-aa(9). The broad language of this new provision suggests that a failure to report a breach "required" under HIPAA, leading to a decision to fail to report the breach to the New York Attorney General, could result in a violation of both HIPAA *and* New York's SHIELD Act, potentially triggering civil penalty provisions under both measures.

The SHIELD Act's breach notification provisions will take effect on October 23, 2019, while the Act's new data security requirements will take effect on March 21, 2020.

Below is a brief summary of the significant provisions of the SHIELD Act. We urge that businesses that maintain or otherwise process New York residents' personally-identifying information, including, without limitation, health care providers and health plans that are HIPAA covered entities, assess any new obligations that they may have under the SHIELD Act, and begin to address compliance efforts.

"Private Information" Subject to the SHIELD Act

Generally, the SHIELD Act expands the definition of Private Information that, if breached, could trigger a notification requirement. In particular, under the Act, identifiers now also include biometric information (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), and 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. N.Y. Gen. Bus. Law § 899-aa(1)(b).

Access to Data Counts as a Breach

The SHIELD Act expands the definition of "breach of the security system" to include any unauthorized access to Private Information, such as viewing, but not obtaining copies of, the Private Information. *Id.* § 899-aa(1)(c). Previously, the State's data security law only considered the unauthorized acquisition of personal information to be a breach.

Expanded Jurisdiction

Prior to the enactment of the SHIELD Act, any person or business that conducted business in the State had to comply with the law's breach notification requirements. Now, jurisdiction has expanded, and any person or business that owns or licenses computerized data which includes Private Information, regardless of whether the person or business otherwise conducts business in New York, must comply if the affected individual is a resident of New York. *Id.* § 899-aa(2).

However, the SHIELD Act also adds an important new exception to breach notification, which is based on a "harm to the individual" standard. Under the new rule, a business may be exempt from the breach notification requirements if "exposure of Private Information was an inadvertent disclosure and the individual or business reasonably determines 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." *Id*. § 899-aa(2)(a). Certain documentation requirements apply.

Regarding HIPAA, and breaches of Private Information that also count as reportable HIPAA breaches, the new law clarifies that HIPAA covered entities need not further notify affected New York residents regarding such breaches under New York's breach notification law; however, notification must be provided to the State Attorney General, Department of State Division of Consumer Protection, and Division of the State Police regarding the breach. *Id*. § 899-aa(2)(b).

New Data Security Standards for Businesses with Private Information

In a substantial expansion of current law, the SHIELD Act requires any person or business that is not subject to (and, notably, in compliance with) certain other data security laws (e.g., HIPAA), and which owns or licenses computerized Private Information of a resident of New York, "to develop, implement and maintain reasonable safeguards to protect the security of, confidentiality and integrity of the Private Information including, but not limited to, disposal of data. N.Y. Gen. Bus. Law § 899-bb(2). The new law provides, among other things, that a person or business shall be deemed to meet this standard if it implements a data security program that includes:

- Reasonable administrative safeguards, such as the following: (a) the designation of one or more employees to coordinate the security program; (b) identification of reasonably foreseeable internal and external risks; (c) assessment of the sufficiency of safeguards in place to control the identified risks; (d) training and managing employees in the security program practices and procedures; (e) the selection of service providers capable of maintaining appropriate safeguards, and requiring those safeguards by contract; and (f) adjusting the security program in light of business changes or new circumstances. *Id*. § 899-bb(2)(b)(ii)(A).
- Reasonable technical safeguards, such as where the business: (a) assesses risks in network and software design; (b) assesses risks in information processing, transmission and storage; (c) detects, prevents and responds to attacks or system

failures; and (d) regularly tests and monitors the effectiveness of key controls, systems and procedures. *Id*. § 899-bb(2)(b)(ii)(B).

- Reasonable physical safeguards, such as where the business: (a) assesses risks of information storage and disposal; (b) detects, prevents and responds to intrusions; (c) protects against unauthorized access to or use of Private Information during or after the collection, transportation and destruction or disposal of the information; and (d) disposes 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. *Id*. § 899-bb(2)(b)(ii)(C).

Penalties

The SHIELD Act toughens the potential civil penalties for breach notification law violations, increasing them to up to twenty dollars per instance of failed notification (capped at $250,000), and imposes new civil penalties (up to $5,000 per violation, with no cap) for certain failures to comply with the new data security standards.

More specifically, the SHIELD Act does not authorize a private right of action, but does authorize the Attorney General to bring an action and obtain civil penalties. N.Y. Gen. Bus. Law § 899-aa(6)(a); N.Y. Gen. Bus. Law § 899-bb(2)(d)-(e). For knowing and reckless violations of the data breach notification requirements, a court may impose penalties of the greater of $5,000 or up to $20 per instance of failed notification, with a cap of $250,000. N.Y. Gen. Bus. Law § 899-aa(6)(a). For violations of the new data security standards, a court, looking to New York's consumer fraud statute, may impose penalties of up to $5,000 "per violation." This penalty provision does not include an upper limit, and it is also unclear what would count as a single "violation" under the law. N.Y. Gen. Bus. Law §§ 899-bb(2)(d) and 350-d.

Implications of the SHIELD Act

The passage of the SHIELD Act continues the trend, in New York and other states, to enact state-level data privacy and security laws. The SHIELD Act will inevitably have a significant impact on businesses that hold Private Information of New York residents, regardless of whether such entities otherwise conduct business in New York. As part of compliance efforts, companies should address the identification of the information subject to the SHIELD Act, and update written data security and breach notification policies and related practices, to incorporate new requirements.

Related Professionals

- **Ellen H. Moskowitz**

  Senior Counsel