Proskauer

A Primer on the SHIELD Act: New York's Move to Adopt More Stringent Data Security Requirements, Part II

Minding Your Business Blog on **March 12, 2018**

What would companies need to do to comply with the law?

The Stop Hacks and Improve Electronic Data Security (SHIELD) Act imposes requirements in two areas: cybersecurity and data breach notification. The cybersecurity provisions of the proposed SHIELD Act would require companies to adopt "reasonable safe-guards to protect the security, confidentiality and integrity" of private information. The Act provides examples of appropriate administrative, technical, and physical safeguards, such as designating an employee to oversee the company's data security program; identifying "reasonably foreseeable" risks to data security; selecting vendors that can maintain appropriate safeguards; detecting, preventing and responding to attacks and system failures; and preventing unauthorized access to private information.

The Act also attempts to set out a number of alternative ways a company can ensure it is considered compliant with the cybersecurity provisions. For example, it states that a company may be considered compliant with the Act if it is covered by and compliant with certain other federal or New York state data security regulations or statutes. However, this provision has the potential to moot the safeguard provisions in the SHIELD Act, because businesses not subject to the jurisdiction of the specified banking or health regulators generally are considered subject to the jurisdiction of Federal Trade Commission (FTC), and Section 5 of the FTC Act has been interpreted by the FTC to require businesses to take reasonable and necessary information security measures to protect sensitive personally identifiable information. Therefore, in attempting to provide an exception that is beneficial for businesses, this provision of the Act actually introduces more confusion, because it is unclear whether companies should tailor their compliance efforts to the SHIELD Act's requirements or the FTC Act's standards (to the extent the two conflict).

The Act also deems companies that have been annually certified by an authorized third party assessor as compliant with any of several specified cybersecurity standards to be complaint with the cybersecurity provisions of the Act, as long as there is no evidence of willful misconduct, bad faith, or gross negligence.

The data breach provisions of the Act revise New York's current data breach notification law, codified as New York General Business Law § 899-AA. In addition to broadening the Act's key definitions as discussed above, the Act provides for an alternative means for notifying people whose email account credentials have been compromised by the data breach. The Act also requires specific information to be included in breach notifications to consumers, and provides an additional notification obligation for payment card issuers when they replace a payment card due to a data breach. However, the Act refrains from making a number of changes to New York's current breach notification law that would bring the law in line with its counterparts in many other states. For example, the Act does not include a "risk of harm" threshold, which would require companies to notify individuals of a data breach only if the potential harm to individuals reached a particular level. Additionally, the Act does not set a threshold number of individuals who must be affected by a breach in order to trigger a company's duty to notify state agencies.

Would the SHIELD Act include any exceptions for small businesses?

Yes. Small businesses would be considered compliant with the cybersecurity requirements of the Act "if they implement and maintain reasonable safeguards [for private information] that are appropriate to the size and complexity of the small business." The Act defines a "small business" as one consisting of fewer than 50 employees, having a gross revenue of under $3 million for last three fiscal years, or having under $5 million in assets.

What are the proposed penalties for noncompliance?

Any company that fails to comply with the cybersecurity requirements of the Act is considered to have violated New York's law prohibiting deceptive acts and practices. While the Act does not provide a private right of action to consumers, the Act authorizes the attorney general to bring an action for damages of not more than $5000 per violation, pursuant to New York General Business Law 350-d. However, what constitutes a "violation" remains unclear; example, it could be measured in terms of individuals affected, or in terms of number of records of personal information maintained, or in terms of the number of ways the business failed to meet the Act's substantive cybersecurity requirements. The Act leaves this issue unresolved.

The Act also would increase the penalties for a company's failure to provide proper notice of a data breach to affected data subjects. Actual damages are available for failure to notify where notification was required, as is the case in the existing New York law. Companies that knowingly or recklessly fail to issue proper notice may be subject to a civil penalty of the greater of $5000, or $20 per failed notification (up from $10 per failed notification), the latter of which is capped at $250,000 (up from $150,000 under New York's current breach notification law).

When does the law go into effect?

It is important to note that the SHIELD Act is a bill currently before the New York Legislature, so it has not become law yet and remains subject to amendment. The Act states that its effective date will be January 1, 2018, but as of the date this blog post went live, the bill remained before the New York State Senate's Finance Committee. Companies that believe they would be subject to its jurisdiction should continue to track its progress.

Please stay tuned to this blog and Proskauer's Privacy Law Blog for further updates.

View Original