Businesses Everywhere Who Collect Private Information on New York Residents Must Soon Plan to Comply with New York's New Cybersecurity Statute (SHIELD ACT)

Client Advisories

10.02.2019

Businesses that collect the private information of New York residents must comply with new and more stringent cybersecurity requirements under that state's newly enacted "Stop Hacks and Improve Electronic Data Security Act" (the "SHIELD ACT"), which applies to businesses located both inside and outside NY.

Although the new law goes into effect on March 21, 2020, some changes it requires will take many businesses time to adopt. Therefore, those businesses that collect private information of NY residents should act now and evaluate their cybersecurity practices, not only to ensure that they will be in compliance with the law when the time comes, but also to make certain that they are in a strong position to protect against a cyber breach and its legal and financial consequences, and to detect and respond to a breach when and if it occurs.

The SHIELD ACT requires businesses covered by the law to implement "reasonable" administrative, technical and physical "safeguards" to protect against the unauthorized access to NY residents' "private information." The Act provides examples of such safeguards, including that businesses:

- designate a coordinator for the security program,
- identify internal and external risks,
- design and implement technical and physical safeguards to control the risks,
- assess and test the sufficiency of those safeguards on an ongoing basis,
- train and manage employees in the security program's practices and procedures, and

- require their "service providers" to maintain appropriate safeguards.

A business may comply with these requirements if it is governed by and complies with other laws and regulations which are listed in the SHIELD ACT, including regulations promulgated under the Gramm-Leach-Bliley Act, the NY State Department of Financial Services Regulations, and HIPAA.

"Small businesses" (those with (i) fewer than fifty employees; (ii) less than $3,000,000 in gross annual revenue in each of the last three fiscal years; or (iii) less than $3,000,000 in year-end total assets) get a bit of a break--they can comply with these requirements by adopting reasonable safeguards that are appropriate for the size and complexity of their business, the nature and scope of their activities, and the sensitivity of the personal information they collect.

The Act expands the scope of NY's law to require certain actions under many circumstances--including notice to data subjects--if there is "unauthorized access" to private information. It had previously required those actions only if private information had been "acquired" as opposed to merely "accessed." The statute also modifies certain data breach notification requirements.

Furthermore, the "private information" that is covered by the law will now include items like:

- an account, debit card or credit card number under circumstances in which it alone could be used to access the account,
- biometric information, 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.

Those businesses that do not comply with the NY's data privacy and cybersecurity laws now face increased civil penalties of up to $250,000 that may be imposed by courts in enforcement actions brought by the NY Attorney General.

If you have a question about how this new law affects your business, or would like to discuss ways to protect your business in light of this and other cybersecurity laws and bills, contact Robert T. Egan at 856-354-3079, or regan@archerlaw.com, or any other member of Archer's Data Privacy and Cybersecurity Group in Haddonfield, N.J., at (856) 795-2121, in Princeton, N.J., at (609) 580-3700, in Hackensack, N.J., at (201) 342-6000, in Philadelphia, Pa., at (215) 963-3300, in Harrisburg, Pa. at (717) 686-4109 or in Wilmington, Del., at (302) 777-4350.

DISCLAIMER: This client advisory is for general information purposes only. It does not constitute legal or tax advice, and may not be used and relied upon as a substitute for legal or tax advice regarding a specific issue or problem. Advice should be obtained from a qualified attorney or tax practitioner licensed to practice in the jurisdiction where that advice is sought.