New York SHIELD Act Expands Breach Notice Requirements Starting in October

As we recently reported, New York’s new SHIELD Act contains data security provisions. It also contains a number of key changes to New York’s existing breach notification obligations. These changes will become effective October 23, 2019.

As amended, the scope of private information which, if breached, may trigger notification obligations to individuals will be broadened. Added to the existing definition of private information will be biometric information, username in combination with a password or security question and answer that permits access to an online account, and an account number or credit or debit card numbers without additional identifying information if the number can be used to access an individual’s financial account. The amendment similarly broadens the definition of a breach, which will now include “access” alone to triggering information (as opposed to the prior definition which limited a breach to “acquisition of” triggering information). In determining whether unauthorized access has occurred, the SHIELD Act now explains that businesses may consider “indications that the information was viewed, communicated with, used or altered.”

Companies who determine that misuse or financial harm is unlikely do not need to notify, but must document that determination and maintain it for at least 5 years.
However, if the incident involves over 500 New York residents, the company will have to submit that determination in writing to the attorney general within ten days after making such a determination. The law also contains some minor additional modifications, like including in any consumer notice the phone number and website of the relevant state and federal agencies that provide information on security breach response and identity theft prevention and protection information.

**Putting it Into Practice:** Companies that maintain a nationwide breach notice plan will want to take into account these updates to the NY notice requirements, including the expanded scope of triggering information and the definition of a “breach.”

Copyright © 2020, Sheppard Mullin Richter & Hampton LLP.