In yet another example of its focus on imposing greater data security accountability, the New York Attorney General (“NYAG”) recently announced a significant settlement with Marymount Manhattan College (“the College”). The settlement stems from a data breach to which the College was subject in 2021. Following an investigation, which, according to the NYAG, revealed inadequacies in the College’s data security program, the NYAG secured a commitment from the College to invest $3.5 million over the next six years to bolster that program. Specifically, the College committed to:

- maintaining a comprehensive information security program that includes regular updates to keep pace with changes in technology and security threats;
- encrypting all personal information, whether stored or transmitted, between documents, databases, or elsewhere;
- maintaining reasonable policies to perform security updates and patch management;
- enabling multifactor authentication for users logging into the College’s networks;
- scanning for vulnerabilities and potential weaknesses; and
publicly sharing the College’s plans for collecting, retaining, and deleting personal information.

In its press release announcing the settlement, the NYAG made a point of highlighting some of its other recent six- and seven-figure settlements with organizations that have experienced data breaches, including organizations in the sportswear, healthcare, clothing, supermarket, and e-commerce spaces. The NYAG also referenced the data security guidance it issued in April 2023, which we discussed here, outlining safeguards the NYAG views as high-priority, including access controls, encryption of sensitive information, service provider vetting and contracting, data mapping, and incident response planning.

Given the NYAG’s heightened enforcement posture over the past couple of years, as well as the recent bolstering of the New York Department of Financial Service’s cybersecurity regulations, which we discussed here, organizations that process personal information relating to New York residents face increased pressure to continuously assess the adequacy of their data security programs and to make timely upgrades.

Jackson Lewis P.C. © 2023

National Law Review, Volumes XIII, Number 308