Crowell

CLIENT ALERT

Another University Data Breach Adds to Growing Trend

February 20, 2014

The University of Maryland announced yesterday that it is the most recent university to fall victim to a data breach. According to the University's President, UM was the target of a "sophisticated" computer attack that exposed the personally identifiable information (PII) of over 300,000 individuals. Specifically, the hack targeted records that relate to the University's student identification (ID) system and thus compromised the PII of various students and staff who had been issued a University ID since 1998. The compromised PII includes names, Social Security numbers, dates of birth, and University ID numbers.

The compromised records were maintained by the school's IT Department and protected by "sophisticated, multi-layered security defenses" that the hackers were nonetheless able to bypass. This reflects the painful reality that data breaches are often a matter of *when*, not *if*, especially for universities.

Educational institutions are particularly attractive targets for both cyber criminals and state-sponsored groups. As repositories of extensive personal, financial, and health information, they offer a wealth of opportunity for identity thieves. The intellectual property that many research institutions generate is similarly appealing to state-sponsored actors looking to capitalize on U.S. economic investments. As the *New York Times* has reported, at least one university has faced up to 100,000 daily penetration attempts from China alone. It thus comes as no surprise that dozens of educational institutions – many with highly sophisticated defense systems in place – have reported data breaches in recent years.

Not only are the risks to educational institutions substantial, but the consequences are also daunting. Educational institutions are subject to numerous federal laws governing data protection, including FERPA, the Gramm-Leach-Bliley Act, and the Federal Trade Commission Act, as well as a number of state laws. The collection and analysis of health data that many universities undertake may also trigger a range of obligations under HIPAA and the HITECH Act. Finally, those receiving government funding must ensure compliance with other unique requirements, such as those arising under their government contracts.

Cyber events need not be devastating. Educational institutions can and should take a variety of proactive steps to ensure that they are adequately protected against cyber attacks, yet prepared for data breaches. Risk assessments, such as that outlined in the recently released Cybersecurity Framework, and detailed incident response plans are essential. In the event that a breach does occur, universities should immediately hire experienced counsel to manage the inevitable notification requirements and reinstitution of privacy safeguards. Just as importantly, responsible counsel can assess and minimize litigation exposure, particularly that posed by class actions. These and other measures – both preventative and responsive – can mean the difference between catastrophe and calm.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1.202.624.2775

Email: jposton@crowell.com

Laurel Pyke Malson
Partner – Washington, D.C.
Phone: +1.202.624.2576
Email: lmalson@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1.202.624.2615
Email: ewolff@crowell.com