Cullen | Dykman

Students Sue University of Central Florida for Data Breach

February 15, 2016

Recently, students and employees of the University of Central Florida (the “University”) filed a proposed class-action lawsuit in Florida federal court against the University alleging that the University failed to adequately safeguard their personal data from a recent data breach that exposed the personal information of nearly 63,000 current and former students and employees.

The University was subject to a data breach in January 2016 whereby hackers were able to access students’ and employees’ Social Security numbers, employee and student identification numbers and their names. According to the University’s official announcement on February 4, 2016, no credit card numbers, financial records, medical records, or grades were accessed by the hackers. The first group affected by the breach consisted of current student-athletes, former students who played in the 2014-15 season, and athletic department staff. The second group affected by the breach consisted of current and former employees, including students who worked at the University as graduate assistants, resident assistants, student government leaders, and students who participated in work-study programs.

Soon after the data breach was announced by the University, two former student body presidents filed a proposed class-action lawsuit against the University claiming the University "breached its duty" on several issues, including failing to "timely notify Plaintiffs and the Class about the breach" and failing to "safeguard and protect" personal information of the alleged victims. The complaint also alleges that the University violated the Family Educational Rights and Privacy Act (“FERPA”), a federal law that requires schools to protect the privacy of student education records. Further, the plaintiffs also allege that the University violated Florida’s Deceptive and Unfair Trade Practices Act, arguing that the victims were “consumers” of the University. The lawsuit also requests, among other things, an order mandating the University "to adequately safeguard" the victims’ personal information, enjoining the University "from engaging in similar unfair, unlawful and deceptive misconduct in the future," and for "damages to be determined at trial."

In response to the breach, the University’s president, John C. Hitt, said, “Safeguarding your personal information is of the utmost importance at UCF. To ensure our vigilance, I have called for a thorough review of our online systems, policies, and training to determine what improvements we can make in light of this recent incident. Every day, people and groups attempt to illegally access secure data from institutions around the world. Higher education institutions are popular targets.” Hitt also stated that the University launched an investigation immediately following the breach, and the University reported the incident to law enforcement. The University is

offering one year of free credit monitoring and identity protection services to the affected individuals.

The degree, nature, and timing of cyber-attacks are difficult to predict. Institutions should review their Internet security policies and hone in on the risk factors that make them vulnerable to hackers. Additional steps must be taken to protect university databases in order to prevent a massive amount of information from being leaked to the general public. Additionally, institutions should review their insurance policies and consider other ways to mitigate data-breach risks.

If your institution has questions or concerns regarding employment or education-related issues, please contact James G. Ryan at jryan@cullenanddykman.com or at 516-357-3750.

Thank you to Garam Choe, a law clerk at Cullen and Dykman, for his help with this post.