RubinFortunato

CLIENT ALERT

October 2017

NO HARM, NO FOUL:
An Employer's Data Breach Does Not Necessarily Provide Employees with Standing to Sue

Gregory T. Laudadio

Last month, the United States District Court for the District of Columbia held that, without a showing of concrete financial harm, employees have no standing to sue their employers for loss of personal information in a cyberattack.[1]

Recent data security breaches involving companies like Wells Fargo and Equifax[2] have heightened the national awareness of, and concern over, the vulnerability of consumer information. Courts have been willing to make assumptions about injuries when a data breach stems from retail establishments or financial entities because, in those cases, sensitive financial information usually has been compromised, and fraud is therefore seen as inevitable. However, here, the District Court was faced with addressing the standards applicable to non-financial data theft resulting from a "cyberattack," and within the context of an employer-employee relationship.[3]

In June 2015, the United States Office of Personnel Management[4] ("OPM") revealed that it had suffered a massive cyberattack affecting more than 21 million former, current, or prospective employees. The lost information included sensitive data, such as names, birthdates, current and former addresses, fingerprints, medical histories, psychiatric profiles, and even Social Security numbers.

As a result, both OPM and its outside contractor responsible for employee background checks, KeyPoint Government Solutions ("KeyPoint"), were the subject of multiple suits across the United States.

The suits were consolidated into two complaints filed with the District Court in the District of Columbia. The complaints alleged that OPM and KeyPoint were grossly negligent in protecting the data, which was required for mandatory background checks of prospective

[1] In Re: U.S. Office of Personnel Management Data Security Breach Litigation, Misc. Action No. 15-1394 (ABJ), 9/19/17.

[2] The Wells Fargo incident was a data breach, while the Equifax incident was a cyberattack. A "data breach" is any unauthorized release of information, whereas a "cyberattack" is a malicious act of hacking.

[3] The court engaged in some particularized analysis because the cyberattack targeted a United States government database, but the legal principles espoused in the opinion are nonetheless applicable to private sector employers, depending on the type of information stolen.

[4] OPM is a government agency responsible for overseeing and executing the employment policies of the federal government.

employees. More specifically, the plaintiffs alleged that OPM and KeyPoint were aware that the sensitive information was being regularly targeted, yet failed to implement appropriate security measures.

The plaintiffs alleged three types of injuries and the court's primary focus was whether the alleged injuries created standing to sue.

First, the plaintiffs alleged injury solely because of the theft of their private information. This alleged injury was clearly insufficient in the eyes of the court, which pointed to a complete lack of precedent on such a claim in case law from both the United States Court of Appeals for the D.C. Circuit and the United States Supreme Court. It stated that a cyberattack resulting only in the theft of personal data, but not specific financial data (*i.e.*, credit card numbers), is not enough to constitute standing. Actual financial harm or a material threat of future financial harm is required.

Second, the plaintiffs alleged injury because of identity theft or fraudulent credit card activity. Even these allegations were deficient for the court, which required a showing of actual monetary damage. Instead, out of the 20 plaintiffs alleging this particular injury, all but two failed to show any out of pocket expenses that were not properly reimbursed by credit card companies or other commercial entities.

Third, the plaintiffs alleged injury because of the threat of future identity theft and other future harms, including claims for money spent on credit protection, lost opportunity costs for time spent on credit monitoring, and the stress and fear of future identity theft. Again, the court was unpersuaded. It required evidence of monetary damages *expressly* connected to the breach, and none of the plaintiffs argued that anything other than personal information had been stolen.

As a result, the court dismissed the lawsuit in its entirety, but created a clear path for employees to sue their employers in the event of not only a data breach, but also a cyberattack. Now, more than ever, employers must ensure the protection of private information.

Gregory T. Laudadio's Pennsylvania Bar Admission is expected in December 2017. He may be reached at 610-408-2052 or at glaudadio@rubinfortunato.com.