A Timely Analysis of Legal Developments

ASAP®

August 6, 2012

Fourth Circuit Joins Courts Limiting Employers' Use of the Computer Fraud and Abuse Act to Prosecute Disloyal Employees

By Matthew Hank and Nina Markey

The federal Computer Fraud and Abuse Act (CFAA) allows an employer to bring a civil action against an employee who accesses the employer's computers "without authorization" or in a manner that "exceeds authorized access." Although the CFAA is primarily a criminal statute designed to combat hacking, employers often bring claims under the CFAA when a "disloyal employee" (typically, an employee who has accepted employment with a competitor) downloads or emails confidential information for the benefit of the employer's competitor.

In *WEC Carolina Energy Solutions LLC v. Miller*, the U.S. Court of Appeals for the Fourth Circuit confronted such a situation. According to the complaint, shortly before the employee resigned from his position as project director for WEC, he downloaded to his personal computer and emailed to himself or his assistant a substantial number of WEC's confidential documents. Shortly thereafter, the employee resigned and used WEC's information to make a presentation to a potential WEC customer on behalf of WEC's competitor. Although WEC had authorized the employee's access to the company's intranet and computer servers, WEC's policies prohibited using that information without authorization or downloading it to a personal computer. After the customer awarded two projects to the competitor (allegedly as a result of the employee's actions), WEC sued its former employee under the CFAA, claiming that he violated the CFAA because, under WEC's policies, he was not permitted to download WEC's proprietary information to a personal computer. By doing so, WEC argued, the employee either: (1) lost all authorization to access the confidential information; or (2) exceeded his authorization.

The district court dismissed WEC's CFAA claim, reasoning that WEC's policies regulated *use* of information, not *access* to that information. While the employee's purpose in accessing the information was contrary to WEC's policies regulating *use*, this was not a violation of a policy relevant to *access.* Consequently, the district court found that there was no liability under the CFAA.

The Fourth Circuit affirmed the district court's holding. The court noted that there are two schools of thought as to whether the CFAA's operative terms "without authorization" and "exceeds authorized access" extend to situations where a "disloyal employee" uses a computer he otherwise has access to through his employer to perform disloyal acts such as downloading or emailing confidential or proprietary information.

The first school of thought is the cessation-of-agency theory. Under this theory, promulgated in a line of cases following *International Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), an employee is deemed to act "without authorization" or in a manner that "exceeds authorized access" whenever he uses the employer's computer to misappropriate the employer's confidential information or facilitate a breach of the duty of loyalty. Breach of the duty of loyalty, under this analysis, immediately terminates the agency relationship and with it any authority to access the employer's computers.

The Fourth Circuit rejected the cessation-of-agency theory. Instead, it adopted the reasoning of the Ninth Circuit and the district court, holding that the plain meaning of the terms "without authorization" or "exceeds authorized access" does not encompass a scenario where the employer allows the employee access to data and the employee then uses that information improperly. The Fourth Circuit took a more literal and narrow interpretation of "without authorization" and "exceeds authorized access," holding that these terms apply "only when an individual accesses a computer without permission or obtains or alters information on a computer beyond that which he is authorized to access."

Unlike some other opinions that have also interpreted the CFAA narrowly, *WEC Carolina Energy Solutions* makes clear that a disloyal employee's violation of a computer use policy, no matter how outrageous, will not support a CFAA claim if the employee was authorized to access the data at the time that he downloaded or retrieved the information. In so holding, the court noted that the CFAA is primarily a criminal statute and that courts must construe criminal statutes strictly. The court further opined that Congress did not intend to subject employees who violate their employers' computer use policies to criminal penalties.

The lesson for employers is twofold. *First*, an employer who wishes to retain the ability to bring a CFAA claim in the disloyal employee context must deny access to its trade secrets in the first place, or withdraw that authorization *before* the employee accesses the data. Even under the restrictive analysis of *WEC Carolina Energy Solutions*, an employee who uses a computer to steal the employer's off-limits data may still be prosecuted under the CFAA. *Second*, in the more typical disloyal employee situation, where the employee downloads information to which he was permitted access and then misuses that data to benefit a competitor, the employer will not have recourse to a CFAA claim and should focus on state law claims. The latter lesson applies, for now, only in the Fourth and Ninth Circuits, but *WEC Carolina Energy Solutions* is likely part of a trend that other courts will follow.

Matthew Hank is a Shareholder, and Nina Markey is an Associate, in Littler Mendelson's Philadelphia office. If you would like further information, please contact your Littler attorney at 1.888.Littler or info@littler.com, Mr. Hank at mhank@littler.com, or Ms. Markey at nmarkey@littler.com.