SANDS ANDERSON

North Carolina Law Life

You Cannot Use the CFAA to Rein in Rogue Employees

By: Donna Ray Berkelhammer. *Tuesday, September 4th, 2012*

Employers in North Carolina, Virginia, Maryland, West Virginia and South Carolina have lost a potentially powerful method of protecting their electronic secrets from disgruntled employees who download sensitive material and take it with them to a competitor.

online fraud (Photo credit: ivers)

Some companies in this situation have sued the ex-employee under the federal **Computer Fraud and Abuse Act** ("CFAA"). The CFAA is a criminal statute intended to combat computer hacking, but it allows a civil lawsuit against a person who obtains information from another's computer "without authorization." The **Fourth Circuit** Court of Appeals recently held in **WEC Carolina Energy Solutions, LLC v. Miller** that the CFAA cannot be used where an employee gains access to information appropriately (ie, without hacking) and then ***misuses this information*** against company policy.

In April 2010, Mike Miller resigned from his position as Project Director for WEC Carolina Energy Solutions, Inc.(WEC). Twenty days later, he made a presentation to a potential WEC customer on behalf of WEC's competitor, Arc Energy Services, Inc. (Arc). The customer ultimately chose to do business with Arc. WEC contends that before resigning,Miller, acting at Arc's direction, downloaded WEC's proprietary information and used it in making the presentation. Thus, it sued Miller, his assistant, and Arc for, among other things, violating the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030.

WEC had typical employment policies that restricted employees from misusing confidential information and trade secrets, including prohibitions against employees using WEC information without authorization and downloading the information to their personal computers.

Civil liability under the CFAA occurs where:

1. The defendant intentionally accessed a computer without authorization or by exceeding authorized access;
2. The defendant thereby obtained information from a protected computer;
3. The conduct involved an interstate or foreign communication; and
4. Loss to one or more persons occurred during any 1-year period aggregating to at least$5,000 in value.

The Fourth Circuit held the CFAA did not apply to Miller's actions because WEC had given him authorization to access the information he took – the fact that he misused that information in violation of WEC's policies did not violate the CFAA. The Court affirmatively stated it was reluctant to convert an anti-hacking statute "into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy."

The Fourth Circuit expressly rejected the "cessation-of-agency theory" used in the Seventh Circuit (Illinois, Indiana, Wisconsin), which holds that authorization is revoked when an employee uses his access for a purpose contrary to the employer's interests:

Such a rule would mean that any employee who checked the latest Facebook posting or sporting event scores in contravention of his employer's use policy would be subject to the instantaneous cessation of his agency and, as a result, would be left without any authorization to access his employer's computer systems.

While some companies may be disappointed to lose the CFAA as a tool, many other remedies exist under state law, including theft or misappropriation of trade secrets, conversion, breach of employment contracts, breach of confidentiality provisions, breach of a non-compete agreement, breach of non-solicitation agreement, tortious interference and civil conspiracy.

There are some modifications to company employment policies that may place unauthorized use of information within the CFAA. If you need your policy reviewed, please contact an **employment attorney**.