Nick Akerman
(212) 415-9217 ▪ akerman.nick@dorsey.com

Nick is a partner in the New York office of Dorsey & Whitney.

For additional articles like this one or to watch my one hour CLE seminar video go to:
http://computerfraud.us

DORSEY
DORSEY & WHITNEY LLP

CAN YOU RELY ON YOUR CORPORATE COMPUTER POLICIES TO SUE EX-EMPLOYEES WHO STEAL COMPANY DATA?

Two recent district court opinions add to the caselaw providing judicial guidance on how employers might update their corporate computer policies to be able to sue ex-employees for stealing company data based on the Computer Fraud and Abuse Act ("CFAA"), the federal computer crime statute. Title 18, U.S.C. §1030. This is a particularly significant problem when employees leave their current jobs to join competitors and attempt to gain an unfair advantage by stealing data from the company computers prior to their departure. 4 of the 7 sections of the CFAA that are the basis for a civil cause of action require that the employer prove that the employee's access to the company computer was "without authorization or exceeds authorized access."

One way the courts permit an employer to establish lack of authorized access is by showing that the employee violated a company policy defining the scope of the employee's permission to access the company computers. Courts have sanctioned the use of corporate computer policies to prove unauthorized access because the "CFAA...is primarily a statute imposing limits on access and enhancing control by information providers." *EF Cultural Travel B.V. v. Zefer Corp*., 318 F.3d 58, 63 (1st Cir. 2003). Thus, a company "can easily spell out explicitly what is forbidden," through employee agreements, policies and access-limiting technology.

For example, *U.S. v. John*, 597 F.3d 263, 269, 272 (5th Cir. 2010), upheld the CFAA conviction of Citigroup account manager Dimetriace Eva-Lavon John, who accessed Citigroup's internal computer system to provide her brother with customer account information that he used to perpetrate fraudulent charges. The court found that John had exceeded authorized access based on "Citigroup's official policy, which was reiterated in training programs that John attended, [that] prohibited misuse of the company's internal computer systems and confidential customer information." *Id*. at 272.

The two recent decisions -- *Sloan Financial Group, LLC v. Coe*, 2010 WL 4668341 (D.S.C., Nov. 18, 2010) and *Clark Street Wine And Spirits v. Emporos Systems Corp*., 2010 WL 4878190 (Nov. 24, 2010) – directly address the issue of corporate computer policies in the context of the employer suing the employee for violating the CFAA. According to Sloan Financial Group LLC's ("Sloan") complaint, Marcus Coe had been an insurance agent employed by Sloan who left to set up a competing insurance agency. Sloan alleged that its former employee violated the CFAA by "(1) transmitting two spreadsheets of Sloan's client information from his work email address to his home email address; (2) conducting searches on the Harleysville database [that contained confidential information on Sloan's insurance clients] for his own benefit; and (3) at

Sloan's expense, ordering Choice Point reports on individuals who never became clients of Sloan's, but later became clients of Coe's new Agency." *Id*. at *3.

Sloan claimed that Coe accessed its computers without authorization or in excess of authorized access based on its company policies. Those policies were in a memorandum circulated to its employees and in an employee handbook. The memorandum restricted "employees' use of client information" and "stated, "[i]t is imperative that all office personnel understand that no client information be taken out of the office.... This information includes electronic data (laptops, CDs, disks, flash-drives, emails), files, paperwork, etc." . . . Coe acknowledged receipt of this policy." Id. at *2.

Thereafter, "Sloan established a more detailed confidentiality policy relating to client and proprietary information . . . when it issued a new employee handbook" that "provides, in pertinent part, that "[i]nformation concerning [Sloan's] clients is confidential.... Confidential information *may not* be released by anyone without proper authority, nor may it be used for personal gain." . . . The handbook also includes a section on access to and use of Sloan's computer systems, providing that "[a]ll computers, related equipment and computer accounts ... are provided as tools to assist [employees] in performance of [their] job-related duties and responsibilities." *Id.*

Despite these policies, the court dismissed the CFAA claims and granted Coe summary judgment, finding 'that Sloan has not proffered evidence that Coe exceeded authorized access by performing any of the alleged actions." *Id*. at *5. The court's dismissal was based on its conclusion that Sloan's company policies only "limit an employee's use of information" rather than limiting "an employee's right to access or obtain information" from the Sloan's computers. *Id*.

Clark Street Wine And Spirits v. Emporos Systems Corp also focused on the employee's right to access the information in question. The complaint alleged "that the defendant and its employees breached plaintiffs' electronic credit and sales system (supplied largely by defendant), resulting in the stealing of credit card information and losses to plaintiffs' customers, and ultimately, to plaintiffs." *Id*. at *1. The district court denied defendants' motion to dismiss the CFAA claim because the case required factual development in discovery on the issue of authorized access -- "[i]f Emporos employees had permission to access Plaintiffs' computers, but not their customers' credit card information, [the CFAA] Count . . . might survive even a strict interpretation" of the element of authorized access. *Id*. *11.

However, that not all courts make such a fine distinction between access and subsequent use. For example, *U.S. v. Salum*, 257 Fed. App'x 225, 230-31 (11th Cir. 2007), interpreted "without authorization" based on the defendant's intended use of the data at the time he accessed his employer's computer. In *Salum*, a police officer with the Montgomery, Alabama, Police Department was charged with a criminal violation of the CFAA for providing information from the FBI's criminal record database to a private investigator. Although Salum, as an employee,

"had authority to access the [National Crime Information Center] database," the court held that there was sufficient evidence for the jury to conclude that Salum had accessed the computer "without authorization "because at the time he accessed the computer Salum knew that he was accessing the information "for an improper purpose." *Id.* at 230.

Based on the current state of the law, employers are well advised to establish corporate computer policies specifically for the CFAA to ensure their ability to use the statute against an ex-employee who might steal valuable data from the company computers to use unfairly in a competing venture. The policies must address the scope of employee's permitted access to the company computers including 1) what information the employee is permitted to access and 2) for what purposes. These policies need to be precisely drafted to the unique circumstances of each company.