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 go to http://computerfraud.us

DORSEY
DORSEY & WHITNEY LLP

MARYLAND COURT: EMPLOYEES WHO STEAL DATA FROM THE COMPANY COMPUTER DO NOT VIOLATE THE COMPUTER FRAUD AND ABUSE ACT

A federal district court in Maryland held that an employee who stole proprietary data from his prior employer did not violate the Computer Fraud and Abuse Act ("CFAA") because he was authorized to access the data and use the data on the job before he terminated his employment with his prior employer. *Océ North America, Inc. v. MCS Services, Inc*., 2010 WL 3703277 *3-*5 (D. Md. Sept. 16, 2010).

Océ North America (Océ) "designs, manufactures, sells, and services high volume production printing systems . . .for commercial printing functions." *Id*. at *1. A former Océ employee went to work for a direct competitor, the defendant MCS Services, Inc. ("MCS"). Océ claimed that before leaving its employ the former employee copied from its computers its proprietary "diagnostic software, a parts manual, and a maintenance manual" and that MCS distributed this stolen material to "its engineers who are using these copies in their daily work." *Id.*

The court dismissed the CFAA claim based on Océs failure to allege facts showing that its former employee accessed its computers "without authorization," an essential element of the CFAA. The court held that Océ's former employee could not have accessed its computers without authorization when he stole the proprietary material because "it was part of his job to use . . . [Océ's] computers and the software on the computers." *Id.* at *4.

In support of its decision the court did not address the division in the Circuit courts on this issue created by the 9th Circuit in *LVRC Holdings LLC v. Brekka,* 581 F.3d 1127, 1130-31 (9th Cir.2009) or explain why it believed its position was more correct than the other courts which have found that employees are can violate the CFAA. The court did not address *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006) which held that an employee's authorization to access the company computer is predicated on the agency relationship with his employer such that when an employee violates his duty of loyalty by stealing his employer's data, his authorization to access the company computers terminates.

The court also found that the copying of the software "may have been a violation of . . . [the former Océ employee's] employment agreement but did not address the case law in First and Fifth Circuits which allow the employer to place limits on the scope of the employee's authorization to access the company computers. *U.S. v. John*, 597 F.3d 263, 271 (5th Cir. 2010) and *EF Cultural Travel BV v. Explorica, Inc*., 274 F.3d 577, 582-84 (1st Cir. 2001). Instead, the court simply cited three district court opinions that support its position.