SCHWARTZ COOPER CHARTERED
180 North LaSalle Street, Suite 2700, Chicago, Illinois 60601
T 312.346.1600 F 312.782.8416 www.schwartzcooper.com

FORMER EMPLOYEE'S DATA DELETION AFTER QUITTING JOB VIOLATES COMPUTER FRAUD AND ABUSE ACT

By: Joan M. Eagle

Employers frequently ask what, if anything, they can do when a former employee deletes data on a company computer in such a way as to guarantee that the deleted files cannot be retrieved. The Seventh Circuit Court of Appeals has just provided an answer.

In *International Airport Centers v. Citrin,* Citrin, managing director of IAC, was responsible for identifying properties that IAC, a real estate company, might want to acquire and assisting in any ensuing acquisition. IAC lent Citrin a laptop for him to record data he collected in the course of his work. Citrin subsequently quit IAC to go into business for himself, in violation of his employment contract; however, before returning the laptop to IAC, he deleted all files and installed a secure-erasure program to ensure that the files could not be retrieved. In doing so he deleted not only the data he had collected for IAC but also data that would have revealed to IAC improper conduct in which he had engaged before he decided to quit.

IAC sued Citrin under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. §1030, and for breach of contract, breach of fiduciary duty, trade secrets, and other claims. In its lawsuit, IAC relied on the provision of the CFAA that provides that whoever "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct intentionally causes damage without authorization, to a protected computer [a defined term that includes the laptop Citrin used]," violates the Act.

Although Citrin successfully argued to the District Court that merely erasing a file is not a "transmission" under the CFAA because all he did was hit the "delete" button, the Seventh Circuit disagreed. The Seventh Circuit found that the loading of the secure-erasure program satisfied the "transmission" requirement and fulfilled congressional intent to protect against computer viruses *and* disgruntled, internal programmers.

The Seventh Circuit also addressed precise modes of transmission of the secure-erasure program to the computer, but basically didn't see what difference that would make, and the difference between "without authority" and "exceeding authorized access," which it found to be "paper thin." The bottom line is that the Seventh Circuit reinstated all of IAC's claims against Citrin.

If you have any questions about this case or how it may apply to a similar situation at your company, please contact Joan M. Eagle at (312) 845-5439 or jeagle@schwartzcooper.com or any member of Schwartz Cooper's Employment Practice Group.