

# Co. can go after exec over use of computer

By Eric T. Berkman

An employer could sue a former executive under the Computer Fraud and Abuse Act for misuse of proprietary information he allegedly took from a company computer in order to launch a competing business after he quit, a U.S. District Court judge has decided.

The defendant executive argued that the CFAA — which covers parties who access a computer “without authorization” — only applies to those who misuse information from a computer that they had no authority to access in the first place, not parties who subsequently misappropriate information from a computer they were authorized to access at the time.

But Judge Nathaniel M. Gorton disagreed and denied a motion to dismiss filed by the executive and his newly formed business.

“Although the [1st U.S. Circuit Court of Appeals] has not directly addressed the meaning of ‘without authorization’ or ‘exceeded authorization’ [under the CFAA], it has favored a broader reading of the CFAA than that which the defendants now urge,” wrote Gorton. “Although the majority of CFAA cases still involve ‘classic hacking activities,’ the CFAA’s reach has been expanded in the past two decades.”

The 12-page decision is *Guest-Tek Interactive Entertainment Inc., et al. v. Pullen, et al.*, Lawyers Weekly No. 02-260-09. The full text of the ruling can be found at [www.masslawyersweekly.com](http://www.masslawyersweekly.com).

## Additional avenue

Plaintiffs’ counsel David M. Cogliano of Davis, Malm & D’Agostine in Boston said the

decision gives employers another potential avenue of recovery against employees who use computers to misuse company information.

“So much of everything we do is with computers these days, and this ruling provides an additional form of relief,” he said. “Lots of employees now have laptops and easy access to confidential information [that] they can transmit.”

Cogliano said the decision is also significant because it is the first time a court within the 1st Circuit addressed head-on whether an employee could be liable under the CFAA for misappropriating information he had been permitted to access from a computer he had also been allowed to access.

“The 1st Circuit had recognized a more expansive view of the CFAA in other cases [not specifically on point],” he said. “This decision seems to follow those and is consistent with the statute.”

In doing so, Cogliano said, the court seemed to adopt his client’s view that once an employee breaches his fiduciary duty of loyalty to his employer, as the defendant employee allegedly did in this case, any prior authorization to access and use proprietary information terminates.

Stephen T. Paterniti, a lawyer at Jackson & Lewis in Boston who represented the defendants, declined comment, citing the ongoing nature of the litigation.

## Plotting with the competition

Defendant Thomas Pullen worked for



COGLIANO  
Says judge’s ruling is  
consistent with CFAA

plaintiff Guest-Tek Interactive Entertainment as vice president of North American Sales for more than two years, until his resignation in May 2009.

During his employment, the defendant was involved in all aspects of the plaintiff’s sales and marketing initiatives and was given access to its confidential and proprietary information and trade secrets.

The plaintiff employer asserted that for an eight-month period leading up to his resignation, the defendant surreptitiously transferred thousands of files from a company computer that he apparently had permission to access onto his personal USB device. Using this proprietary information, he allegedly plotted with one of the plaintiff’s largest competitors to launch a new company, PureHD Ltd., of which the defendant is now president and which competes directly with the plaintiff.

In July 2009, the plaintiffs brought CFAA and G.L.c. 93A claims against the defendant in U.S. District Court. The plaintiffs also filed a 93A claim against PureHD.

The defendants moved to dismiss the claims.

## Broad reading

The defendants argued that, under the “plain language” of the CFAA, a party only accesses a computer “without authorization” when initial authorization is not permitted and only “exceed[s] authorized access” when the party is given general access to a computer, but not to

certain information on the computer.

The plaintiffs, on the other hand, contended that the defendant employee's initial authorization to access company computers and information was conditioned on the agency relationship between him and the company. Once he breached his duty of loyalty to the company by copying files and planning a competitive venture, the relationship ended, as did his authorization to access the files, according to the plaintiffs.

Gorton said that some federal courts around the country have adopted the plaintiffs' broader interpretation of the phrase "without authorization" while others have adopted the defendants' narrower interpretation.

And while the 1st Circuit has not directly addressed the meaning of the phrase, it has favored a broader reading of the CFAA in general, the judge said, pointing to the court's 2001 decision in *EF Cultural Travel BV v. Explorica, Inc.*

In that case, the 1st Circuit upheld a CFAA claim against employees who relied on

**CASE:** *Guest-Tek Interactive Entertainment Inc., et al. v. Pullen, et al.*, Lawyers Weekly No. 02-260-09

**COURT:** U.S. District Court

**ISSUE:** Could a company sue a former executive under the Computer Fraud and Abuse Act for misuse of proprietary information he allegedly took from a computer while employed by the company in order to launch a competing business after he left?

**DECISION:** Yes, because he constructively extinguished his authorization to use the company's computer when he breached his duty of loyalty by allegedly misappropriating the information

pricing information on their former employer's website to develop a competing company with lower prices.

The 1st Circuit found that such use of the employer's information "reek[ed] of use — and indeed, abuse — of proprietary information that goes beyond any authorized use of [the employer's] website," Gorton observed. "The court's analysis of the employees' 'authorized use' and 'abuse' of [their employer's] proprietary information rather than their initial authorization to access the website undercuts the defendants' plain language argument."

Additionally, the judge said, the CFAA's reach has been expanded in the past two

decades by the congressional enactment of a private cause of action and a more liberal judicial interpretation of the statutory provisions.

As a result, "[e]mployers ... are increasingly [using the CFAA] to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system," he said.

Thus, Gorton ruled, the defendants' motion to dismiss should be denied.

The judge went on to dismiss the plaintiffs' Chapter 93A claim against the defendant employee on the ground that the statute does not cover conduct arising from an employment relationship. He did, however, allow the 93A claim against PureHD to proceed. **MLW**

*Eric T. Berkman, an attorney and former reporter for Massachusetts Lawyers Weekly, is a freelance writer.*

*For more information about the judge mentioned in this story, visit the Judge Center at [www.judgecenter.com](http://www.judgecenter.com).*