

## BUSINESS INFORMATION

### Evidence Under the CFAA

**T**HE FEDERAL Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030, et. seq., provides companies with a powerful legal tool to protect their computer data. As its inclusion in Title 18 demonstrates, the CFAA was originally enacted as a criminal statute in 1984, but was amended in 1994 to provide victims of computer crime with a civil remedy for both damages and injunctive relief. § 1030(g). The CFAA contains seven potential causes of action based on theft and destruction of data, fraudulent use of passwords, hacking and schemes to defraud through unauthorized access to computers.

While damages are not to be minimized, the statute's most useful civil remedy is injunctive relief, which permits a federal court to order the immediate return of stolen data and to direct a halt to their dissemination. An injunction can be critically important to a company that is seeking to prevent its confidential and trade secret information from being used against it in the marketplace or trying to stop a data thief from perpetrating identity theft on its customers or employees. The key to success under the CFAA is identifying and marshaling the evidence to prove a violation of the statute.

#### Advanced planning can lead to proof of theft

The recent decision by the 3d U.S. Circuit Court of Appeals in *P.C. Yonkers Inc. v. Celebrations the Party and Seasonal*

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

By Nick Akerman



*Superstore LLC*, 428 F.3d 504 (3d Cir. 2005), underscores just how important it is to be able to develop sufficient admissible

**Taking steps before a theft occurs can help a company capture proof of a theft, which is the key to obtaining an injunction.**

evidence from the company's computers to obtain a preliminary injunction. Based on a failure of proof, the *P.C. Yonkers* plaintiffs lost their motion for a preliminary injunction. This article will review that decision and its prime lesson: Advance planning and proactive steps before a theft occurs can facilitate a company's ability to capture proof of a theft, which in turn maximizes

the likelihood that a court will grant a preliminary injunction.

The *P.C. Yonkers* plaintiffs were all franchisees who each operated "a retail store selling discount party goods and related products." *Id.* at 506. The two defendants, a former officer and employee for the company that managed the various franchise locations, left the managing company to create a competing business, *Celebrations*. The proof predicated the plaintiffs' motion for a preliminary injunction, based on violations of the CFAA, focused on one employee, Andrew Hack. Hack had accessed the franchisor's computer shortly before and after resigning from the managing company. The plaintiffs claimed that, of the 125 incursions into the computer system over seven days in October and November 2003, eight occurred after Hack was no longer an employee.

The plaintiffs also claimed that Hack accessed the computers two additional times after leaving the plaintiffs' employ, once two months later "in December 2003 and a final time in April 2004." *Id.* at 507. "The access in December 2003 lasted a total of 19.4 minutes," and "[t]he April access was for a total of 5 minutes and 49 seconds." *Id.* The plaintiffs claimed that the defendants obtained information from these computer incursions that resulted in *Celebrations* opening competing stores "in late July and August of 2004" in time to compete against the plaintiffs in their busiest and most profitable season "leading up to Halloween." *Id.* The information taken from the computers, according to the complaint, allowed the defendants to determine "where to locate their stores, where to focus marketing efforts and budgets,

and to obtain valuable information as to sales during the Halloween season.” Id.

The plaintiffs moved the court for a preliminary injunction “prohibiting Celebrations from operating the Celebrations stores and from using the PC plaintiffs’ trade secrets and confidential and proprietary information, and ordering the return of such information.” Id. The 3d Circuit, however, affirmed the district court’s denial of the preliminary injunction, finding that there was “absolutely no evidence as to what, if any, information was actually viewed, let alone taken” from the plaintiffs’ computers. Id. at 508. As a matter of law, to obtain a preliminary injunction the plaintiffs were required to demonstrate a likelihood of success on the CFAA claim.

## Plaintiffs could not show that any data were taken

The court held that the plaintiffs failed to demonstrate a likelihood of success because “without a showing of some taking, or use, of information, it is difficult to prove intent to defraud,” a critical element of the CFAA violation alleged against the defendants. Id. at 509. Absent the plaintiffs’ speculation of thefts based solely on the incursions into the company computer, the court was left with no choice but to conclude that the defendants’ decisions about where to locate their stores and where to focus their marketing budgets were based on their “expertise gained through years of experience in the retail party goods business, unaided by any information obtained through access to the... plaintiffs’ computer system.” Id. at 509-10.

The factual scenario alleged in *P.C. Yonkers* is not unique. According to the plaintiffs, this is the classic “inside job,” where disloyal employees steal competitively sensitive computer data as part of their plan to resign and compete against their current employer. Inside data thefts, as Judge Richard E. Posner observed in *Int’l Airport Centers LLC v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006), are both “easier to detect [than attacks by an outside hacker and] may also be easier to accomplish.” Id. There is no dispute that the inside incursions into the *P.C. Yonkers* Inc. computers were easy to accomplish. The incursions were also easy to prove.

What the plaintiffs could not show was which, if any, of their data records were

accessed and whether any of their data records had been downloaded, copied or printed. The court faulted the plaintiffs for not providing noncomputer evidence from which Celebrations’ acquisition of the plaintiffs’ trade secrets could have been reasonably inferred. For example, the court pointed out that “[p]erhaps they could have produced evidence...[that] vendors [had been] contacted by...[the defendants] in temporal proximity to the unauthorized access.” Id. While such proof might have saved the day for the preliminary injunction, there was no excuse for the plaintiffs not being able to provide sufficient proof from their own computers of what was accessed.

## Companies need to capture proof of what was accessed

Current technology permits a company to capture proof from its computer network establishing the details of each document accessed. *P.C. Yonkers* should be a wake-up call for companies, alerting them to employ that technology. Access itself, as demonstrated by *P.C. Yonkers*, is usually not difficult to prove, since most companies use passwords that identify the date and the time a particular employee enters and leaves the network. What many companies do not have is an auditing function that automatically records what specific document is accessed and what happens to a document each time it is accessed.

For example, commercially available software exists that automatically creates a record detailing the history of who accessed a predesignated sensitively competitive document and whether the document was physically retrieved. In *P.C. Yonkers*, the software would have demonstrated what documents, if any, Hack viewed and what actions, if any, he took with respect to each document.

Such an audit trail would be admissible in court to support a motion for a preliminary injunction as a record maintained in the regular course of business under Fed. R. Evid. 803(6). Whatever software or method is used to create an audit trail for individual documents, it is important to keep in mind that for the audit trail to be admitted under the business-record exception to the hearsay rule, the company must be able to convince a court that the

audit trail is reliably created and is “an accurate representation of the record that originally was created” each time the user accessed the document in question. *In re Vee Vinhnee*, 336 B.R. 437, 444 (B.A.P. 9th Cir. 2005).

## Inspection of home computers may be needed

Another aspect of the *P.C. Yonkers* case that underscores the importance of advance planning is that all of the incursions into the plaintiffs’ computer network were made from Hack’s home computer. What is conspicuously absent from the reported case is any reference to the evidence that should have been available from Hack’s home computer that might have shown which of the plaintiffs’ documents were observed or downloaded. Again, proper advance planning could have facilitated the obtaining of proof from the home computer in addition to the regular discovery that the plaintiffs were entitled to take in the lawsuit. At the time that the company permitted Hack to work from his home computers, the company should have required him to sign an agreement allowing it to inspect his home computers at the time of his termination of employment and to remove data belonging to the company.

In sum, the two lessons for protecting computer data from *P.C. Yonkers* are obvious and compelling. Addressing both will make it more likely that if data are stolen, evidence will be available to support a preliminary injunction. First, company computer networks should be programmed to create an automatic audit trail of all sensitive documents that is admissible in a court of law as a regularly conducted business record. Second, when the company allows employees to work at home on their own computers, protocols and policies should be established to ensure the return of all company data remaining on the home computers. **NLJ**

This article is reprinted with permission from the July 17, 2006 edition of THE NATIONAL LAW JOURNAL. © 2006 ALM Properties, Inc. All rights reserved. Further duplication without permission is prohibited. For information, contact ALM Reprint Department at 800-888-8300 x6111 or visit [almreprints.com](http://almreprints.com). #005-07-06-0014