THE NATIONAL LAW JOURNAL
JULY 6, 2009
Daily Updates at NLJ.COM

When workers steal data to use at new jobs

Despite some negative case law, the Computer Fraud and Abuse Act is an effective tool for employers.

BY NICK AKERMAN

In response to the economic crisis, companies have downsized, resulting in some terminated employees' stealing vital data to improve their job opportunities with a new employer. In addition to traditional state remedies such as misappropriation of trade secrets, employers have been "increasingly taking advantage of...[the federal Computer Fraud and Abuse Act's] civil remedies 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." *Pacific Aerospace & Electronics Inc. v. Taylor,* 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003).

THE PRACTICE
Commentary and advice on developments in the law

The Computer Fraud and Abuse Act, a federal criminal statute outlawing the theft of data, permits a company that "suffers damage or loss" by reason of a violation of the CFAA to "maintain a civil action against the violator" for damages and injunctive relief. 18 U.S.C. 1030(g). Since *Taylor*, there has developed a body of district court opinions that refuse to apply the CFAA against employees who steal their employers' data. This article will explain why these opinions are not likely to survive appellate review; it will also provide a strategy to avoid the application of these decisions.

'CITRIN' IS LEADING AUTHORITY

Four of the seven violations of the CFAA that provide a basis for a civil action require the employer to show that the employee's access to the company computers was "without authorization" or "exceeds authorized access." The leading authority for using the CFAA against employees who steal their employers' data is *Int'l Airport Centers LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006). Based on the Restatement (Second) of Agency § 112 (1958), the U.S. Court of Appeals for the 7th Circuit held that an employee's authorization to use the company computers is predicated on his agency relationship with his employer and that, when the employee violates "his duty of loyalty," i.e., accesses his employer's computer to steal its data, he voids this relationship and thereby terminates his authority to access the computer.

There are now 11 reported district court decisions that disagree with *Citrin* and refuse to apply the CFAA to employee data thieves. These courts hold that the intent of the employee in accessing the computer is irrelevant to the question of authorization because employees do have permission to access the company computers. See, e.g., *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962 (D. Ariz. 2008). These cases conclude that the CFAA is "generally aimed towards outside, third parties or other 'high-tech' criminals, rather than the rogue employee." *Lasco Foods Inc. v. Hall And Shaw Sales, Marketing, & Consulting LLC*, 600 F. Supp. 2d 1045, 1049 (E.D. Mo. 2009).

Nine of the 11 opinions rely on *Lockheed Martin Corp. v. Speed*, 2006 WL 2683058 (M.D. Fla. 2006), which, along with *Diamond Power Int'l Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1341 (N.D. Ga. 2007), is within the 11th Circuit and has been effectively overruled by *U.S. v. Salum*, 257 Fed. Appx. 225, 230-31 (11th Cir. 2007). In *Salum*, a police officer with the Montgomery, Ala., 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

NICK AKERMAN *is a partner in the New York office of Dorsey & Whitney who specializes in the protection of trade secrets and computer data. He represented the plaintiffs in* Lockheed Martin Corp. v. Speed *and* EF Cultural Travel B.V. v. Explorica Inc., *two cases discussed in this column.*

an employee, "had authority to access the [National Crime Information Center] database," the circuit court held, without citing the lower court opinions of *Lockheed Martin* or *Davidson*, that there was sufficient evidence to convict on the element of lack of authorization because Salum knew that the information he accessed was to be used "for an improper purpose." The five district courts that adopted the holding in *Lockheed Martin* and were decided after *Salum* ignore *Salum*. See, e.g., *US Bioservices Corp. v. Lugo*, 595 F. Supp. 2d 1189, 1191-96 (D. Kan. 2009).

Lockheed Martin faulted *Citrin* for relying "heavily on...the Second Restatement of Agency...to derive the meaning of 'without authorization.' " 2006 WL 2683058, at *4. The court complained that "the breadth of the statute given under the *Citrin* reading is especially disconcerting, given that the CFAA is a *criminal* statute with a civil cause of action." Id at *7.

In *Carpentar v. U.S.*, 484 U.S. 19 (1987), however, the U.S. Supreme Court, employed the Restatement (Second) of Agency to affirm the mail and wire fraud convictions of a *Wall Street Journal* reporter who, prior to publication, had provided his upcoming financial columns to confederates, who bought or sold stock "based on the probable impact of the column on the market." Relying on the Restatement, the Court held that "an employee has a fiduciary obligation to protect confidential information obtained during the course of his employment" and that intentionally exploiting that information for his own personal benefit was a scheme to defraud his employer of confidential information outlawed by the mail and wire fraud statutes. Just as the Restatement prescribes the duty of an employee in the context of these fraud statutes to safeguard his employer's confidential information, it also prescribes the scope of an employee's authority to access his employer's computer in the context of the CFAA.

IN THE CRIMINAL CONTEXT

The first criminal case to deal with the CFAA in the employment context, *U.S. v. Nosal*, 2009 WL 981336, at *7 (N.D. Calif. 2009), refused to dismiss CFAA charges against a former "high level executive at an international executive search firm" who quit his position "with plans to start a competing executive search firm." Prior to leaving the firm, he stole competitively sensitive data from his employer's computer. The court rejected the defendant's argument that "the CFAA was aimed primarily at computer hackers and that the statute does not cover employees who misappropriate information."

The court adopted *Citrin*, finding that "ample authority exists to permit criminal actions to proceed based on violations of [§ 1030(a)(4)] by employees, as interpreted by civil cases, and there is simply no statutory basis to suggest otherwise." The court also emphasized that the defendant was wrong in "focusing exclusively on the later misuse of information by an employee against an employer's interests," when the "gravamen of the charge" is that the employee accessed the computer "with the intent to defraud." Thus, the critical element is that, at the time the employee accessed the company computer, he intended to use it in a fraudulent way.

Finally, *Citrin* is not the only circuit court decision sanctioning use of the CFAA against employees. The 3d Circuit recognized that its reach includes actions against employees who steal data from their employers' computers. *P.C. Yonkers Inc. v. Celebrations The Party and Seasonal Superstore LLC*, 428 F.3d 504, 510 (3d Cir. 2005). The 5th Circuit, citing *Citrin*, has recognized that "authorized access typically arises...out of a[n]...agency relationship," *U.S. v. Phillips*, 477 F.3d 215, 221, n. 5 (5th Cir. 2007). In short, although there are 11 district courts that preclude CFAA civil actions against employees, four circuit courts and Supreme Court law strongly suggest that these 11 opinions will ultimately lack precedential value.

Until this issue is resolved by the circuit courts or the Supreme Court, a simple strategy to avoid relying solely on the agency theory in filing a civil CFAA action is to establish unauthorized access through company polices and employee agreements. An employer "clearly has a right to control and define authorization to access its own computer systems" through its company policies. *Cont'l Group Inc. v. KW Property Mgmt.*, 2009 WL 1098461, at *12 (S.D. Fla. 2009). Thus, "written computer access policies maintained by...[the employer] in its Employee Handbook" can "determine whether" the employee "exceeded her authority to access."

Unauthorized access can also be established through employee agreements. In *EF Cultural Travel B.V. v. Explorica Inc.*, 274 F.3d 577 (1st Cir. 2001), the court upheld a preliminary injunction based on a violation of the CFAA because the defendants, all former employees of the plaintiff, had accessed and downloaded pricing data on EF Cultural's Web site by violating their confidentiality agreements with EF Cultural. It is therefore critical for employers to review and amend company rules and agreements to maximize their ability to use the CFAA. ■