Shook, Hardy & Bacon L.L.P.

Protecting Business Assets:
Unfair Competition, Non-Competes & Trade Secrets

Winning in Employment™
SHB National Employment Litigation & Policy Group

A PUBLICATION OF SHOOK, HARDY & BACON L.L.P. JANUARY 2007



SWORD & SHIELD: THE COMPUTER FRAUD AND ABUSE ACT

BY SCOTT MCLAUGHLIN AND SHANE MCCLELLAND

In today's market, employees are mobile and regularly change jobs. As a result, employers are exposed to the risk of former employees taking trade secrets and other valuable company information via the company's computer system or the Internet. Even worse, employers are vulnerable to attack from employees through the dissemination of viruses, worms or other programs that may cause significant damage to their servers, databases and electronic files.

To contain a rising tide of losses, employers are looking to the Computer Fraud and Abuse Act (CFAA) for protection and to recoup some of those losses, and such causes of action are being pursued with greater frequency. Indeed, "[e]mployers ... are increasingly taking advantage of the CFAA'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." *P.C. Yonkers, Inc. v. Celebrations the Party Superstore, LLC*, 428 F.3d 504, 510 (3rd Cir. 2005).

Elements of a CFAA Cause of Action

To recover under the CFAA, an employer must show that an individual:

(1) accessed a protected computer;

(2) without or exceeding authorization;

(3) knowingly and with intent to defraud; and

(4) as a result, furthered the intended fraudulent conduct and obtained anything of value.

In addition to establishing these elements, the statute provides a $5,000 floor for losses sustained by a victim within a one-year period.

A "protected computer" is a computer used in interstate or foreign commerce or communication. "The term 'exceeds authorized use' means to access a computer without authorization and to use such access to obtain or alter

About SHB

Recognized by *Business Week* as "the law firm of choice for many companies plagued by high-stakes [litigation] woes," SHB is internationally known as the litigation firm to hire to defend complex commercial, antitrust, employment, environmental, ERISA, products liability, and mass tort litigation.

The SHB Employment Litigation & Policy Practice Group represents corporate employers exclusively. In *Chambers USA America's Leading Business Lawyers — A Clients' Guide*, the group is "lauded for both its class action work and its effective advice to employers on federal compliancy issues." The group represents a number of *Fortune* 500 companies throughout the United States.

The group is distinguished by a highly imaginative and innovative approach based on the wealth of the firm's litigation experience (class action issues, expert witness development, e-discovery, effective case-management technology, award-winning diversity efforts and professional development programs, a national local counsel network, and the best practices of convergence programs).

information in the computer that the accesser is not entitled so to obtain or alter." Interestingly, perhaps because the CFAA is in large part a criminal statute, the Act requires that the violator act *knowingly* and with the *intent* to defraud.

"Interestingly, perhaps because the CFAA is in large part a criminal statute, the Act requires that the violator act knowingly and with the intent to defraud."

The CFAA defines damage as "any impairment to the integrity or availability of data, a program, a system, or information." Disclosure of trade secrets may also be considered damages under the Act. There is no requirement, however, that physical damage be present to prevail under the statute. Economic damages may also include salaries of individuals who resolve problems created by violations of the Act or consulting fees to determine the amount of damage caused to a computer system.

Under the Act, a loss includes "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data . . . to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." Losses may include loss of business and loss of business goodwill, if it results from impairment or unavailability of data or a computer system.

"Losses may include loss of business and loss of business goodwill, if it results from impairment or unavailability of data or a computer system."

The Circuit Courts Provide Protection for Employers' Trade Secrets and Other Proprietary Information Through the CFAA

First Circuit

In *EF Cultural Travel BV, EF v. Explorica, Inc.*, 274 F.3d 577, 585 (1st Cir. 2001), the First Circuit Court of Appeals affirmed a preliminary injunction preventing a student tour company from using a "scraper" software program to glean another company's tour prices from its Web site. Several employees left EF Cultural Travel to begin their own student tour company. Before leaving, the vice president of the new company, Explorica, Inc., entered a broad confidentiality agreement with his former employer that prevented him from disclosing proprietary or competitive information. To gain an advantage in the market, the former vice president retained a software consulting company to develop software that would obtain his former employer's pricing information from its Web site. The court held that "because of the confidentiality agreement appellants' action 'exceeded authorized access,'" to the former company's proprietary information. Consequently, when the former employee obtained the pricing information from the public Web site via the software scraper, he violated the CFAA.

Second Circuit

In *Nexans Wires S.A. v. Sork-USA, Inc.*, 166 Fed. App. 559, 562 (2d Cir. 2006), the Second Circuit Court of Appeals considered whether a manufacturer of silver-plated copper wire presented sufficient evidence to demonstrate that the defendant's alleged misappropriation of trade secrets and data caused a "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000." The plaintiff had alleged that the misappropriation of confidential data caused the company to lose $10 million in revenue. The court recognized that the CFAA only permits damages for lost revenue if there is an "interruption in service." Additionally, travel expenses incurred in investigating potential misappropriations unrelated to actual computers or computer services is not

cognizable under the Act. The court noted, however, that these expenses may be recognized under the Act if a plaintiff could show a "connection between the travel costs incurred . . . and 'any type of computer investigation or repair,' or any preventative security measures or inspections" taken.

Third Circuit

In *P.C. Yonkers, Inc.*, the court attempted to clarify the breadth of relief available under the CFAA. Two former employees of Party City opened their own retail store -- Celebrations! The Party and Seasonal Superstore, L.L.C. -- in close proximity to the plaintiffs' existing stores. During their employment with Party City, the defendants had home access to the company's computer system. Plaintiffs alleged that defendants accessed Party City's computer system from home more than 125 times in a one-week span without authorization. The "plaintiffs averred that the defendants used the information obtained from this access to decide where to locate their stores, where to focus marketing efforts and budgets, and to obtain valuable information" during the busiest sales season -- Halloween. The court held, however, that the plaintiffs did not present evidence that alleged trade secret information was taken or used in violation of the CFAA.

In fact, the court pointed out that mere access does not necessarily mean that information was taken or used in violation of the CFAA. Under *P.C. Yonkers*, to prove the intent to defraud element, a plaintiff must show some taking or use of information; access to information alone is not sufficient to show a CFAA violation.

"Under P.C. Yonkers*, to prove the intent to defraud element, a plaintiff must show some taking or use of information; access to information alone is not sufficient to show a CFAA violation."*

Seventh Circuit

In *International Airport Centers L.L.C. v. Citrin*, 440 F3d 418, 421 (7th Cir. 2006), the court reinstated CFAA claims against a former employee who allegedly deleted confidential computer files by installing a computer program on his former employer's laptop. The employee quit his job and decided to go into business for himself, which violated his employment contract. Before he returned his work laptop, he loaded a software program designed to erase all the computer's data.

The court focused on whether loading the software program on the laptop constituted a transmission under the Act. The court found the distinction between physically inserting a disk or downloading the software from the Internet to be of no consequence when considering the CFAA's definition of a transmission. Indeed, the court noted that Congress intended the CFAA to protect employers from attacks from within, such as a disgruntled employee leaving the firm who destroys information on his way out or the outside attacker who transmits a virus or worm to infect the computer files. Either way, the CFAA reaches "whoever '*intentionally* accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damages.'"

Ninth Circuit

In a case similar to *Explorica, Inc.*, the Ninth Circuit addressed what potential damages the CFAA offers aggrieved employers. In *Creative Computing v. Getloaded.com, LLC*, 386 F.3d 930 (9th Cir. 2004), the employer-plaintiff owned

and operated an industry-leading dock loading Web site for trucking companies. The court affirmed a damages award for three CFAA violations and state law misappropriations of trade secrets. The damages resulted from a competitor impersonating other trucking companies' passwords and login names to sneak onto the Web site, hacking into the Web site's operating codes, and hiring away an employee who accessed confidential information on his work computer and e-mailed it to his home account. The court noted that economic damages under the Act may include the loss of business and business goodwill, sanctions for attorney's fees and expenses associated with experts used to assess damage done to the computer system. Importantly, the court rejected the argument that the CFAA's $5,000 damage floor must be realized as to each unauthorized use. The court found that "the damage floor [of $5,000] in the Computer Fraud and Abuse Act contains no 'single act' requirement"; rather, "the $5,000 floor applies to how much damage or loss there is to the victim over a one-year period, not from a particular intrusion."

A Shield and a Sword for Businesses

Trade secret protection offers unique challenges. Assistance, however, is available. In addition to the protections afforded under state misappropriation and contract law, Congress has provided employers an avenue to redress damages they sustain when their electronic trade secrets and other proprietary information are stolen. Now, employers can look to the CFAA when former employees depart with the company's valuable trade secrets or send a virus, worm or Trojan horse that damages the computer system. As noted above, it is likely that employers will become more aggressive seeking redress for the loss of trade secrets -- through the CFAA, Congress has provided both the sword and the shield.

Checklist: The Elements of a CFAA Cause of Action

The Computer Fraud And Abuse Act is violated when an individual knowingly

- ✓ accesses a protected computer;
- ✓ without or exceeding authorization;
- ✓ knowingly and with intent to defraud;
- ✓ and, as a result, furthers the intended fraudulent conduct and obtains anything of value.

Shook, Hardy & Bacon L.L.P.

For more information, contact:

Ena Diaz
Miami
305.960.6920
ediaz@shb.com

Bill Martucci
Kansas City
816.559.2196
wmartucci@shb.com

Scott McLaughlin
Houston
713.546.5684
smclaughlin@shb.com

Jim Murphy
Tampa
813.202.7121
jbmurphy@shb.com

Lori Schultz
Kansas City
816.559.2039
lschultz@shb.com

Kevin Smith
Kansas City
816.559.2238
ksmith@shb.com

Walter Stella
San Francisco
415.544.1905
wstella@shb.com

Peter Strand
Washington, D.C.
202.639.5617
pstrand@shb.com

Mark Tatum
Kansas City
816.559.2383
mtatum@shb.com

Marlene Williams
Houston
713.546.5603
mcwilliams@shb.com