

Total Rewards on Guard

By Nick Akerman, Dorsey & Whitney

Computerization has evolved to the stage in which nearly every business maintains its vital information on computers. Fortunately, the federal Computer Fraud and Abuse Act (CFAA) has emerged as a powerful tool to protect that information. (See Figure 1 on page 48.)

While one may assume that responsibility for protection of corporate technological assets lies with the information technology (IT) department or security personnel, the total rewards department also can play a critical role. Many measures relating to employee policies and procedures are directly controlled by the total rewards department. Total rewards has control over promulgating companywide policies on employees' use of e-mail and the Internet, requiring employees to sign agreements at the beginning of employment, and is in charge of termination procedures.

Two cases, *Igenix Inc. v. Lagalante* and *Shurgard Storage Centers v. Safeguard Self Storage Inc.*, involved employees stealing employers' confidential and proprietary information to compete against the employers in new jobs. Two other cases, *EF Cultural Travel BV v. Explorica Inc.* and *Register.com Inc. v. Verio Inc.*, enjoined companies from using automatic robots to download data through their competitors' public Web sites. All four of these cases have far-reaching consequences with regard to how companies can use the CFAA to protect business information stored on computers.

Each case also significantly challenges businesses to prepare themselves to take advantage of the remedies the CFAA offers.

QUICK LOOK

- ⇒ The Computer Fraud and Abuse Act (CFAA) is a powerful tool to protect sensitive corporate information, but it's up to the plaintiff to prove the law was broken.
- ⇒ Even if information stolen from a computer is not protected by trade secret or copyright laws, perpetrators can still be caught — and punished.
- ⇒ Taking certain steps *before* a problem arises makes the burden of proof much easier.
- ⇒ Total rewards can play a critical role in protecting an organization's important information.

Virtual Hand in the Cookie Jar

Shurgard dealt with a factual scenario that almost every total rewards department in the nation has, at some point, confronted: an employee sending valuable company information through the Internet immediately before the employee terminates his or her employment with the company.

FIGURE 1: CFAA TIMELINE

The CFAA embraces multiple civil causes of action for damages and injunctive relief that fall into four main categories:

- Obtaining information from a computer through unauthorized access
- Trafficking in a computer password that can be used to access a computer
- Transmitting junk mail known as “spam”
- Damaging computer data.

Despite the fact that the CFAA has provided for civil relief since 1994, it was not until recently that federal courts around the country relied upon the CFAA to uphold the right of businesses to protect

1984	Computer Fraud and Abuse Act (CFAA) (18 USC § 1030) is enacted as an exclusively criminal statute, designed to protect classified information on government computers and financial records or credit information on financial institution computers.
1994 and 1996	Congress amends the statute, broadening it to cover all computers used in interstate commerce. At the same time, Congress provided for private civil actions to help anyone injured by the criminal activity prohibited by the statute.
2001	Congress further broadens the CFAA to include any computer “located outside the United States that is used in a manner that affects interstate or foreign commerce or communication in the United States.”

Shurgard employees sent trade secret information via e-mail from a Shurgard computer to their new employer, a direct competitor. The defendant competitor argued that the CFAA was inapplicable since, as employees, they had the right to access the company’s computer and, as a result, could not have exceeded the authorized access required by the CFAA.

The federal district court held that the employees’ authority ended when they acquired “adverse interests” or committed “a serious breach of loyalty” to their employer. Thus, “they lost their authorization and were ‘without authorization’ when they allegedly obtained and sent the proprietary information to the defendant via e-mail.” The court also held that the legislative history of the CFAA supported Shurgard’s position. Quoting from the 1996 *Senate Report*, the court found that the CFAA’s scope “ensure(s) that the (virtual) theft of ... intangible information by the unauthorized use of a computer is prohibited in the same way (that the real) theft of physical items (is) protected,” and that “(the) crux of the

offense ... is the abuse of a computer to obtain information.” The district court also relied on the *Senate Report* for its statement that one of the intended purposes of the CFAA is “to punish those who illegally use computers for commercial advantage.”

A Louisiana federal district court also adopted this application of the CFAA in *Ingenix*. The company’s regional sales director downloaded confidential and proprietary customer and marketing information and deleted other customer information from his Ingenix company computer immediately before he took a new job with a competitor. The court granted Ingenix’s motion for a temporary restraining order that, among other things, prohibited the former employee from conducting business with Ingenix customers, though he was not bound by a noncompete agreement or a post-employment restrictive covenant.

Techno Spies

In both *EF Cultural Travel* and *Register.com*, the federal courts enjoined the defendants from using specially

designed robots to download large quantities of data from public Web sites. The data was not trade secret protected and could be obtained on a limited basis from the public Web site.

The data at issue in *EF Cultural Travel* consisted of more than 150,000 prices for high school educational tours. The court found that the defendants used the pricing data to “gain a substantial advantage over all other student tour companies, and especially EF, by undercutting EF’s already competitive prices on student tours.”

In *Register.com*, the data at issue was customer contact information for domain names registered by Register.com. As an accredited domain-name registrar, Register.com is required to permit online access to names and contact information for its customers “to provide necessary information in the event of domain-name disputes, such as those arising from cybersquatting or trademark infringement.”

The database is set up to “allow the user to collect registrant contact information for one domain name at a time by entering the domain name into the provided search engine.” The defendant, a direct competitor, built “an automated software program or ‘robot’” and periodically downloaded all of Register.com’s customer contact information to solicit those customers for the same Internet services. The automatic downloading allowed the defendant to contact Register.com’s customers “within the first several days after their registration,” when they were most likely primed and ready to purchase the related services.

Both courts addressed the issue of whether the defendants’ use of the robots exceeded authorized access under the CFAA. In *EF Cultural Travel*, the first circuit court relied on the confidentiality agreement between the plaintiff and one of the defendants to find that the

defendants exceeded authorized access by using the plaintiffs' confidential information to build the robot so it could effectively download all of the plaintiffs' prices. In *Register.com*, the district court found that the automated search robot was not "authorized" by the Web site's terms of use, holding that even if the defendant's "means of access" to the database would otherwise be authorized, "that access would be rendered unauthorized *ab initio* by virtue of the fact that prior to entry ... (the defendant) knows that the data obtained will be used later for an unauthorized purpose."

Case law interpreting the CFAA is destined to evolve in the next few years as circuit courts interpret the statute's scope. Nonetheless, if a company expects to take full advantage of the remedies this statute provides, it is critical that the company have viable systems in place. Employers must be able to prove what information was taken and how it was taken any time a virtual thief takes a fancy to the vital business information stored in corporate computers.

Total Rewards to the Rescue

These cases demonstrate that, even if information stolen from a computer is not itself protected by trade secret or copyright laws, perpetrators can still be enjoined from taking and using the information. Moreover, because the CFAA provides for a federal cause of action, there is automatic federal jurisdiction that can be used to join additional state claims. Given these advantages the question becomes, "Can you prove a CFAA violation?"

Take the following proactive steps *before* a problem occurs and the task is made easier:

- **Establish company-wide policies on employee use of the Internet and e-mail.** For example, do company policies prohibit employees from sending company information to their homes

over the Internet? Such a policy can provide an evidentiary basis to establish that a violation of that policy was done without authorization.

- **Require employees to sign confidentiality agreements to establish unauthorized access to key business and financial information.**

Traditionally, confidentiality agreements have reinforced state law outlawing an employee from using or disclosing the company's confidential and proprietary and trade secret protected information. Under the CFAA, such agreements do much more and can form the basis for establishing the central element of lack of authorization required to be proven by the statute.

- **Routinely review company computers for improper use, particularly when an employee resigns or is discharged.**

Are employee computers reviewed as part of the termination process? Does the company permit employees to perform work on home computers? If so, are home computers reviewed as part of the termination process to ensure that valuable company computer data is not on such home computers?


- **Adjust the company's computer system to capture evidence of illegal entries.**

If an employee sends critical information to a third party over the Internet via e-mail, does the company server record it? For how long? If an employee or outsider enters the company computer and accesses vital information, does the computer system record the date, time of entry and nature of the information accessed? If it does, how long does the company maintain that information before deleting it?

- **Monitor public entries to the company Web site.** Does a built-in computer warning system alert the company to attempts to use Web site access to obtain entry to other company databases?

- Provide terms of use on the public Web site to clarify what is and isn't authorized. Employers should clarify what is and isn't authorized. For example, terms of use that prohibit automatic robots from downloading information provide an evidentiary foundation to show that a particular Web site use "exceeded authorization" as that phrase is interpreted under the CFAA.

However, it is clear that there are key components over which total rewards has no control. Thus, to ensure a comprehensive approach to this problem, it is imperative that total rewards professionals coordinate their policies and procedures with IT, company security and legal.

For example, usually IT and security personnel are equipped to monitor the efficacy of the computer systems and can adjust it to capture evidence of illegal use. The company law department is the one that can best determine which evidence must be captured to prove a case in court and what must be contained in an effective and enforceable confidentiality agreement. 

ABOUT THE AUTHOR

Nick Akerman is a partner at Dorsey & Whitney. He can be reached at akerman.nick@dorseylaw.com or 212/415-9217.

FOOTNOTES

Visit our Web site at www.worldatwork.org, where you will find a powerful database that holds nearly 10,000 full-text documents on total rewards topics.

For more information related to this article:

⇒ Go to the "Info Finder" section of the home page, click on the blue "Power Search" button and then click on "Advanced Search."

⇒ Type in this key word string on the search line: "Fraud" OR "Policy and e-mail or Internet" OR "Computer and data or information" OR "Ethics and employee"