

Protecting Your Critical Business Information With The Computer Fraud and Abuse Act

Computerization has evolved to the stage where nearly every business maintains its vital information on computers. Fortunately, the federal Computer Fraud and Abuse Act (CFAA)¹ has emerged as a powerful tool to protect that information. Enacted in 1984, the CFAA began as an exclusively criminal statute, designed to protect classified information on government computers and financial records or credit information on financial institution computers. In 1994 and 1996, Congress amended this 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 this statute prohibits. In October 2001, Congress broadened 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."

The CFAA embraces multiple civil causes of action for damages and injunctive relief. These fall into four main categories: 1) obtaining information from a computer through unauthorized access, 2) trafficking in a computer password that can be used to access a computer, 3) transmitting junk mail known as "spam" and 4) 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 their business information from competitors.

Two cases dealt with employees who stole their employer's confidential and proprietary information in order to compete against their employers in new jobs. *Ingenix, Inc. v. Lagalante*;² *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*³ Two other cases enjoined companies from using automatic robots to download data through their

competitor's public websites. *EF Cultural Travel BV v. Explorica, Inc.*;⁴ *Register.Com, Inc. v. Verio, Inc.*⁵ All four cases have far-reaching consequences as to how companies can use the CFAA to protect business information stored on computers. All four cases also significantly challenge businesses to prepare themselves to take advantage of the remedies this potent statute offers.

Employee Thefts

In *Shurgard*, employees sent trade secret information via e-mail from a *Shurgard* computer to their new employer, a direct competitor of *Shurgard*. 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 authorized access, as the CFAA requires. The federal district court, relying on the Restatement (Second) of Agency, 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 district court also held that the legislative history of the CFAA supported Shurgard’s position. Quoting from the 1996 Senate Report, the district 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.”

This application of the CFAA was also adopted by a Louisiana federal district court in *Ingenix*. *Ingenix*’s Regional Sales Director downloaded *Ingenix*’s confidential and proprietary customer and sensitive marketing information and deleted other customer information from his *Ingenix* company computer immediately before he took a new job with a competitor. The federal district court granted *Ingenix*’s motion for

a temporary restraining order that, among other things, prohibited *Lagalante* from conducting business with *Ingenix* customers. *Lagalante* was not bound by a non-compete agreement or a post employment restrictive covenant. Indeed, Louisiana is a jurisdiction that is hostile to such covenants.

Use of Automated Robots

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 websites. 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 approximately 154,293 prices for high school educational tours. The court found that the defendants used this 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 of *Register.com* built “an automated software program or ‘robot’” and periodically downloaded all of *Register.com*’s customer-contact information, so the defendant could solicit those customers for the same internet services offered by *Register.com*. The robot’s 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 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 website’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."

Proactive Steps

The four recent cases discussed above demonstrate that if information has been taken from a computer without authorization, the CFAA provides several significant advantages over prior law that has traditionally been used to protect a business's confidential and proprietary information. 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? Taking the following proactive steps before a problem occurs can make this task easier:

- Monitor public entries to the company web site.
- Provide terms of use on the public web site to clarify what is and is not authorized.

- Adjust the company's computer system to capture evidence of illegal entries.
- Require employees to sign confidentiality agreements to establish unauthorized access to key business and financial information.
- Routinely review company computers for improper usage, particularly when an employee resigns or is discharged. ■

¹ 18 USC § 1030

² 2002 WL 506812 (E.D.La. 2002)

³ 119 F.Supp.2d 1121 (W.D. Washington, 2000)

⁴ 274 F.3d 577(1st Cir. 2001)

⁵ 126 F.Supp2d 238 (S.D.N.Y. 2000)

About the Author



Nathaniel (Nick) Akerman
New York
(212) 415-9217
akerman.nick@dorseyllaw.com

A partner in the Trial group, Nick represents clients in trial and appellate courts and arbitrations throughout the United States. His focus is on complex commercial litigation, computer fraud, trade secret/covenant not to compete litigation, and white collar criminal matters. He also counsels clients in establishing systems and policies to protect their intellectual property and computer data.

dotCoop, the registry for the new top-level domain name .coop, has announced its Brand Safe Program to protect your intellectual property rights. The program is available to corporations, companies and individuals that are otherwise ineligible to apply for a .coop domain name. For more information, please contact one of our attorneys listed under our Trademark & Copyright Group.

Trademark & Copyright Group

Liz Buckingham, Minneapolis
buckingham.elizabeth@dorseyllaw.com
Pamela Deese, Washington, D.C.
deese.pamela@dorseyllaw.com
Lile Deinard, New York
deinard.lile@dorseyllaw.com

Patent Group

Aldo Noto, Northern Virginia
noto.aldo@dorseyllaw.com
Edward Bulchis, Seattle
bulchis.edward@dorseyllaw.com
Lee Osman, Denver
osman.lee@dorseyllaw.com

Internet & E-Commerce Group

Nelson Dong, Seattle
dong.nelson@dorseyllaw.com
David Mathus, New York
mathus.david@dorseyllaw.com
Lance Vietzke, Denver
vietzke.lance@dorseyllaw.com

Franchise & Distribution Group

Nancy Smith Pearson, Denver
smith.nancy@dorseyllaw.com
James Hermsen, Seattle
hermsen.james@dorseyllaw.com

IP Litigation Group

Peter Lancaster, Minneapolis
lancaster.peter@dorseyllaw.com
Ralph Taylor, Washington, D.C.
taylor.ralph@dorseyllaw.com

Additional Offices Offering Intellectual Property Services

Brian Laurenzo, Des Moines
laurenzo.brian@dorseyllaw.com
Shane Coleman, Missoula
coleman.shane@dorseyllaw.com
Ian Craig, London
craig.ian@dorseyllaw.com
Donald Kaul, Southern California
kaul.donald@dorseyllaw.com

For change of address or subscription:

Toni Byard, Minneapolis
byard.toni@dorseyllaw.com

© 2002 Dorsey & Whitney LLP. This newsletter is published for general information purposes only. Views herein are deemed of general interest and should not necessarily be attributed to Dorsey & Whitney LLP or its clients. This newsletter does not establish or continue an attorney-client relationship with Dorsey & Whitney LLP. The contents should not be construed as legal advice or opinion. If you have any questions, you are urged to contact a lawyer concerning your specific legal situation. For further information, please contact one of the lawyers listed on this page.

The determination of the need for legal services and the choice of a lawyer are extremely important decisions and should not be based solely upon advertisements of self-proclaimed expertise. This disclosure is required by rule of the Supreme Court of Iowa.

DORSEY & WHITNEY LLP

www.dorseylaw.com

Intellectual Property Update

Dorsey & Whitney is a full-service international law firm with core practices in the areas of intellectual property, corporate securities and finance, M&A, international law and complex litigation.

Minneapolis
Seattle
New York
Washington, D.C.
Denver
San Francisco
London
Brussels

Hong Kong
Tokyo
Shanghai
Toronto
Vancouver
Anchorage
Des Moines
Salt Lake City

Southern California
Fargo
Palo Alto
Northern Virginia
Great Falls
Rochester
Missoula

www.dorseylaw.com

Volume 2, No. 4

Dorsey & Whitney LLP
Suite 1500
50 South Sixth Street
Minneapolis, MN 55402-1498