

## Fighting Theft Of Company Data Through The CFAA

*Law360, New York (July 16, 2010)* -- Many employers would be surprised to know that almost 60 percent of employees who are either terminated or quit are taking company data with them when they leave that employment. Such theft comes at a high price for companies. It has been recently estimated that data and trade secret theft cost individual companies an average of \$2 million each year.

Because of this increase in data theft by company insiders, employers must search for new ways to combat these malevolent efforts by employees and former employees.

Traditional means to address theft of company information have included criminal prosecution under the Economic Espionage Act under 18 U.S.C. § 1831, theft of trade secrets under 18 U.S.C. § 1832, and civil suits for trade secret misappropriation under state law. Another effective tool has emerged for combating electronic theft through the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030.

Enacted in 1984, the CFAA, a statute providing for both criminal and civil claims, began as an effort to protect against the access of specific protected computers. Faced with increasing computer crimes, Congress enacted the CFAA to provide an important tool to prescribe theft of information over computers.

As criminals have become more sophisticated and computer theft has increased, Congress has expanded the CFAA to try to stem the tide of such



*Eric D. Welsh*



*Sarah A. Fulton*

illegal conduct. The CFAA has been expanded to address a number of limitations that were perceived as unduly restricting the use of this statute.

For example, in September of 2008, the CFAA, through the enactment of the Identity Theft Enforcement and Restitution Act, Pub. Law 110-326, 122 Stat. 3560, no longer requires a showing that the culprit's actions result in over \$5,000 of loss under certain sections. In addition, the CFAA's jurisdiction has been expanded to reach the theft of information from computers even if the theft did not involve interstate or foreign commerce. The act has also been broadened to include within the definition of a "protected computer" any computer used in or affecting foreign or interstate commerce.

With these amendments, the CFAA has become another tool for companies to combat computer theft.

While the CFAA has been strengthened as a tool for addressing cyber crime, a significant issue has emerged in the interpretation of the CFAA that could undermine its usefulness as a tool in fighting the theft of computer data by departing employees. This issue surrounds the appropriate interpretation to be given to one phrase in one commonly used section of the statute. While it may seem that a debate over one phrase in the CFAA is minor, it actually bears great significance, in many cases determining the applicability of the statute in civil contexts.

Section (a)(5) of the CFAA allows for private action against one who "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; [or] intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss."

In the context of an employee that steals data from a computer, the question under this statute is whether that person's access to the computer was "without authorization" or not. Unfortunately, the CFAA does not define "without authorization," although it does define "exceeds authorized access." 18 U.S.C. § 1030 (e)(6). In the absence of a clear definition, courts in the United States have struggled to define the circumstance where a person acts "without authorization."

The dilemma posed by the current debate is perhaps best understood through a hypothetical. Consider the example of an employee (referred to as Trusted Employee), who on the eve of ending his employment with the company, accesses the company database and downloads from his terminal highly sensitive company data, which he then copies to a computer hard drive and takes with him to his new employment.

In this situation, did Trusted Employee, in accessing the same information he was able to access during his employment through the computer terminal assigned to him, act beyond his permitted usage under the CFAA? Trusted Employee was allowed, no doubt, to access that computer and those files or programs as part of his job description. Certainly, the Trusted Employee's copying and pilfering of proprietary business information was not authorized by his employer and certainly this conduct must violate the CFAA.

### **The Two Views of the Statute**

Surprisingly, the courts have approached the scenario set forth with Trusted Employee in two different ways. Some courts have interpreted the definition of "without authorization" to include "exceeding authorized access."

With this view, the courts consider the CFAA to reach instances where the employee's motives become contrary to the goals of the employer. This is viewed as a more flexible application of the CFAA. Alternatively, other courts view acting "without authorization" more rigidly, as being limited to situations where an employee accesses information or files outside the bounds of his job description.

In the example above, under the second view, the Trusted Employee would have to hack into a database he was not previously given access to in order to find a violation under the CFAA.

For the employer, this distinction is significant. In instances where the employer wishes to pursue action Section (a)(5) of the CFAA the potential outcome is completely uncertain because what constitutes unauthorized access is unknown.

Cases under the first line of thought reason that an individual acts without authorization any time the person exceeds the authority granted to him. Courts that follow this school of thought focus on the employee's breach of his duty of loyalty, thus terminating the agency relationship upon which the employment relationship was built. *Int'l Airport Centers LLC v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006). See also, *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.* 119 F.Supp.2d 1121, 1123 (W.D. Wash. 2000).

Under this school of thought, an agency relationship is terminated once the "agent acquires adverse interests or is guilty of a serious breach of loyalty to the principal." Restatement (Second) of Agency § 112 (1958). Because an employee only has access to a computer as a result of the agency relationship, that access is no longer authorized once the agent breaches the terms of the relationship. Thus, this line of thought clearly allows for the employer to withdraw authorization, either through explicit or implied means.

Furthermore, this viewpoint clearly applies to circumstances where an employee is still employed by a company but acts against the interests of a company by accessing a computer and stealing information or deleting files. See *ViChip Corporation v. Lee*, 438 F. Supp. 2d 1087 (N.D.C.A. 2006).

Under this view, Trusted Employee's behavior would most certainly be termed acting "without authorization" because Trusted Employee's actions are in contrast with the agency relationship and the implied duty of loyalty to Company X that comes with it.

Though this first view considers the language "exceeds authorized access" and acting "without authorization" as very similar, there is still a distinction to be made. Followers of the first viewpoint have differentiated circumstances where an employee "exceeds authorized access" without acting "without authorization."

For example, when a former employee accesses a public website, he is authorized to use that website, but the employee exceeds his authorization by using confidential information to gain better access. *EF Cultural Travel BV v. Explorica, Inc.* 274 F.3d 577, 583-84 (1st Cir. 2001). Again, this first school of thought affords flexibility in addressing computer crimes.

Under the second school of thought, there is a strong delineation between actions that are "without authorization" and those that simply "exceed authorized access." The second school of thought believes that once someone is granted access to a computer or database, that person cannot then access that computer or database without authorization because authorization has already been given.

Thus, the CFAA only prohibits improper accessing of computer information — not improper motives. *Jet One Group, Inc. v. Halcyon Jet Holding Inc.*, 2009 WL 2524864 (E.D.N.Y 2009). The leading case of this point of view is *LVR Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009). *LVR Holdings* found that "no language in the CFAA supports [the] argument that authorization to use a computer ceases when an employee resolves to use the computer contrary to the employer's interest." *LVR Holdings*, 581 F.3d at 1133.

Because Trusted Employee once had permission to access the computer, that authorization is not lost even when the motives behind the access are in contrast with the goals of the employer.

The LVRC Holding court, and the other courts following this school of thought, have found that the CFAA “does not prohibit the use of a protected computer for any prohibited purpose; instead it prohibits one from intentionally accessing a computer “without authorization.” *Southwest Airlines Co. v. Boardfirst, LLC*, 2007 WL 4823761 (N.D. Tex).

The courts subscribing to this point of view have shifted the focus from a duty of loyalty to a focus centered on the plain meaning of the statute. For these courts, the fact that Congress delineated between “exceeds authorized access” and the phrase “without authorization” has particular significance. See § 1030 (a)(1) and (a)(2).

Because Congress defined “exceeds authorized access” to mean to access a computer with authorization and obtain information, and because Congress did not include the term “exceeds authorized access” in Section (a)(5), subscribers to the second view believe Congress did not contemplate private action under the CFAA for exceeding permitted use.

Under this new line of thinking, “without authorization” simply means instances in which use of the computer was not ever permitted. *Lockheed Martin Corp. v. Speed*, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at \*5(M.D. Fla. Aug. 1, 2006); *Int’l Ass’n of Machinists & Aero. Workers v. Werner-Masuda*, 390 F. Supp. 2d 479, 498 (D. Md. 2005).

A major criticism of this second view is that it does not easily demonstrate the circumstances in which an employee’s actions are no longer authorized — once permission is given, it is not clear that an employee’s actions can ever become “unauthorized,” especially when the employee acts while still employed by the company and absent pre-set limitations established by the employer.

This line of thinking may limit the applicability of the CFAA only to circumstances where an employee acts where authority has never been given and not to circumstances where an employee’s permission has been impliedly or explicitly revoked.

### **Steps Can Be Taken to Benefit Under the CFAA**

As instances similar to that involving Trusted Employee arise as a result of a struggling economy and increased reliance on computers, the meaning of “without authorization” under the CFAA will become even more significant, especially for courts where this is a matter of first impression. This judicial split over the meaning of the CFAA clearly adds a complication to a company’s ability to use the CFAA as tool to protect proprietary information and trade secrets, and highlights the need for explicit employment agreements and computer access policies. Given this uncertainty, and in order to protect themselves from internal data theft, employers should consider taking a number of measures to better align themselves to the protections afforded by the CFAA, irrespective of which school of thought may later be applied by a court addressing the wrong, including:

—Employers should include clear delineations in the employment handbooks or guidelines of what is or is not permissible access under an employee’s job title, and efforts must be made immediately upon termination to halt an employee’s access to company computers.

—Computer policies must be clearly defined and specific as to the types of technologies that they encompass.

—The programs and computers that an employee is allowed to access in the scope of his or her employment should be explicit and limited. Additionally, access to these programs should be explicitly contingent upon employment or an assignment for the benefit of the employer.

—Employers must also take appropriate steps to guard against continued access to a computer after the employment relationship has ended.

Until the issue concerning the reach of Section (a)(5) of the CFAA is resolved, either by legislative amendment or by the U.S. Supreme Court, employers should take steps to ensure that they can minimize the potential for computer theft and, if it occurs, maximize their abilities to counteract such conduct through all available means, including through the CFAA.

--By Eric D. Welsh and Sarah A. Fulton, Parker Poe Adams & Bernstein LLP

*Eric Welsh is a partner with Parker Poe Adams & Bernstein in the firm's Charlotte, N.C., office and practices in complex commercial litigation and intellectual property litigation. Sarah Fulton is an associate with the firm in the Charlotte office and practices in complex commercial litigation and intellectual property litigation.*

*The opinions expressed are those of the authors and do not necessarily reflect the views of the firm, its clients, or Portfolio Media, publisher of Law360.*

[1] Brian Krebs, Data Theft Common By Departing Employees, The Washington Post, Feb 26, 2009.

[2] A Matter of Life or Death, Bloomberg and AFP, Washington, Feb. 24, 2010.

[3] Though more recent, the second viewpoint portrayed in LVRC Holdings has still been subject to criticism by those who follow the first school of thought. In U.S. v. Dimetriace Eva-Lavon John, the Fifth Circuit, noting LVRC Holdings opinion, maintained that an employee who was aware of the “intended-use” of the employer, but exceeded the intended use, exceeded authorized access under the CFAA. U.S. v. Dimetriace Eva-Lavon John, 597 F.3d 263, 271-272 (5th Cir. 2010).

