

Protecting Against Employee Theft

Cases of employee-related data theft more than doubled between 2006 and 2008, with more expected in this down economy. Companies have found some success using the Computer Fraud and Abuse Act, but HR leaders should be aware of some proactive steps that will make victory more likely in such cases.

By Leslie Paul Machado

Businesses face all kinds of challenges in today's competitive environment, but one of the most insidious is the threat of an enemy within.

In a typical scenario, a less-than-loyal employee decides to jump ship to a competitor or start a competing operation. Unless you have in place a noncompete agreement specifically prohibiting such activities, the employee's behavior may be distasteful but probably not illegal.

However, if the departing employee decides to download company files containing sensitive information – such as customer lists, pricing schedules, marketing plans, etc. – and take those files with them, a line has been crossed. One powerful weapon employers can use to protect their interests in such cases is the Computer Fraud and Abuse Act.

Unfortunately, the scenario described above is far from hypothetical.

Last year, Starwood Hotels & Resorts Worldwide filed suit against Hilton Hotels and two former Starwood executives who went to work there. The suit claims the two former executives stole information about Starwood's W hotel brand and were using that information to help Hilton develop Denizen hotels, a competing format.

The lawsuit charges that the two departing employees took more than 10,000 electronic and hard-copy files, "many containing highly confidential and proprietary Starwood information and trade secrets."

On top of this civil action, it was revealed earlier this year that federal prosecutors and agents are investigating possible charges, including fraud and theft of trade secrets, in a criminal probe of Hilton and the two former Starwood executives.

While it's impossible to know exactly how widespread a problem theft of trade secrets by former employees really is, there is strong statistical and anecdotal evidence that it has become a growing issue for employers.

According to "A Statistical Analysis of Trade Secret Litigation in Federal Courts," that was recently published in the *Gonzaga Law Reform*, the number of trade secret cases has grown "exponentially" in recent years.

"Most alleged misappropriators are someone the trade secret owner knows," the authors write. "Specifically, in over 85 percent of cases, the alleged misappropriator was either an employee or business partner."

Cases of employee-related data theft more than doubled between 2006 and 2008, according to a study conducted by accounting and consulting firm KPMG. Based on its findings, the firm concluded that the number of such incidents is "almost certain" to increase further, especially in a difficult economic environment.

While thefts analyzed in the KPMG study were carried out primarily by individuals, teams of employees working against their employers were the perpetrators in about 10 percent of cases. In one case, up to

15 employees conspired to defraud their employer by stealing proprietary information. In more than 90 percent of cases, the thefts were not discovered until after the employees had left the company.

In about 70 percent of cases, the employees moved to a rival company, but in about a quarter of cases, they used the stolen data to start a competing business. The most common methods of data theft were e-mail (46 percent), followed by hard copies of the data (22 percent), electronic storage devices (9 percent) and suspicious database searches (7 percent). Another 22 percent of the methods were uncategorized.

Needless to say, the best way to neutralize the potential damage of trade secret theft by employees is to prevent it in the first place.

However, given the interconnected nature of the modern business environment and the need for employees at all levels of an organization to have timely access to data, an ironclad prevention policy is a virtual pipedream. That being the case, it is imperative that employers be aware of all the means they have at their disposal to redress such transgressions when they occur.

From a legal standpoint, the former employer of an individual who has stolen company information and used it to start a competing business or to help their new employer compete against their old one has several potential paths to pursue. The former employer may have a claim for breach of an employment agreement, tortious interference with ongoing and/or prospective opportunities, misappropriation of trade secrets, civil conspiracy or conversion.

Depending on the former employee's position, it may also have a claim for breach of fiduciary duty.

The former employer may also be able to pursue its claim under the Computer Fraud and Abuse Act, which allows the employer to bring the suit in federal court against disloyal employees who access a computer "without authorization" and obtain something of value.

Additionally, because the CFAA also includes criminal penalties, a viable CFAA claim significantly increases a defendant's exposure and thus may encourage an expeditious settlement on terms most favorable to the former employer.

However, filing a CFAA claim is no guarantee of a favorable outcome. While several courts have endorsed claims under this law, other courts have rejected them in virtually identical cases. Generally, it comes down to a matter of interpretation, but there are steps employers can take to help tilt the odds in their favor.

The expansive view of the CFAA was established in a 2006 case, *International Airport Center vs. Citrin*. In that case, an employer loaned its employee a laptop to record data he collected in the course of his work. When the employee decided to open a rival company, he used the information on the laptop to benefit his new venture.

The court held that when the employee decided to act in his own interest rather than his employer's, his authority to access the laptop ended because the only basis of his authority had been that relationship. As such, the *Citrin* court held, the employee was "without authorization" to access the information on his employer's laptop.

The expansive view established by the court in the *Citrin* case has been adopted by numerous other courts in similar cases.

However, other courts confronting the same or very similar sets of facts have reached quite different conclusions, holding that an employer could not assert a CFAA claim because the employee's access was authorized when the employer gave them access to the network.

For example, in a 2009 case (*LVRC Holdings LLC vs. Brekka*), an employee e-mailed confidential company documents to his personal e-mail account and used that information to compete with his employer. Adopting a narrower interpretation of the CFAA, the court in that case rejected the employer's argument that authorization to use a computer ceases when an employee resolves to use the computer contrary to the employer's intent.

Both decisions mentioned above were reached by circuit courts, and, ultimately, the glaring discrepancy between the two interpretations will have to be resolved by the U.S. Supreme Court or clarified by Congress. In the meantime, there are several steps employers can take to place themselves in a stronger position should they decide to assert a CFAA claim in case of employee theft of trade secrets or other proprietary information.

First, employers should amend their employment manuals to assert that any authorization granted to an employee to access the company's networks, files or data automatically ceases when the employee has been terminated, tenders a resignation or forms an intent to leave the employer for any reason – irrespective of whether the employer has actually blocked the employee's access.

Such language does not guarantee the employer will be able to successfully assert a claim under the CFAA, but it strengthens such a claim because it responds to questions about employee authorization to access raised in some of the court decisions embracing the narrower interpretation of the law.

Second, employers should make clear in their employment handbooks, manuals and employment agreements that any authorization to access company data is granted only in furtherance of the employer's business purposes. They should state explicitly that any other access is unauthorized. Such language has been cited by courts in several cases where employer CFAA claims have been allowed.

Finally, employers must remain vigilant to retrieve laptop computers from employees immediately after an employee gives notice. They should also immediately change passwords and close remote access upon learning of an employee's intention to leave the company.

In several of the cases where employers' CFAA claims were not allowed, courts emphasized that the employers in those cases had allowed employees to retain access to the network or laptops after separation.