FISHER & PHILLIPS LLP
ATTORNEYS AT LAW
Solutions at Work®

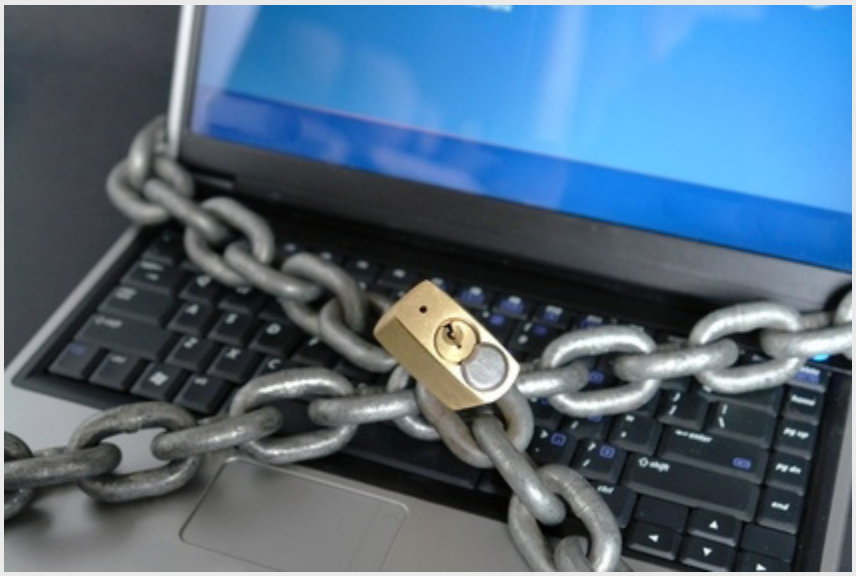
Ninth Circuit Reverses Course on Computer Fraud & Abuse Act

May 16, 2011

by John D. McLachlan

More often than not when a management law firm informs its clients of recent case developments, the news is not good. This is an exception.

In a decision more in line with decisions from other circuits, the U.S. Court of Appeals for the 9th Circuit recently decided a Computer Fraud & Abuse Act ("CFAA") case which offers significant assistance to employers' efforts to protect their trade secrets and confidential information from theft or misuse by employees, so long as employers do it correctly. The case was entitled U.S. v. Nosal, and a copy of the decision is available in pdf format below.



Case Background

David Nosal was a former employee of Korn/Ferry, an executive search firm. Nosal resigned his employment and convinced certain employees who were still employed by Korn/Ferry to provide him with information from the company's confidential Searcher database – considered by Korn/Ferry to be one of the most comprehensive databases of executive candidates in the world. Nosal was not authorized to access the Korn/Ferry database, and he did not do so. The currently employed individuals engaged by Nosal were authorized to access the Searcher database as part of their jobs, and they passed Searcher database information to Nosal.

An indictment followed, with the government claiming Nosal and his co-conspirators were criminally liable for violation of the CFAA which subjects to punishment under criminal statutes anyone who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value." Employers should take note of this case as well because the CFAA also provides civil remedies for violations of its provisions. These civil remedies include damages and injunctive relief.

The defendants argued they could not possibly be guilty of a violation of CFAA because the employer authorized them to access the Searcher database. They claimed the CFAA was designed to penalize hackers who illegally entered company computer systems without authorization and not individuals like themselves who were authorized to access the database, regardless of what use they made of the company's database information.

The court agreed with the government that the employees violated the statute because they: 1) accessed the database; 2) obtained information from the computer; and, 3) used it for a purpose that violates the employer's restrictions on the use of the information. The case turned on the employer's restrictions on the use of information stored in its Searcher database and the meaning of authorized access.

A Dramatic Change In Direction

This distinction is more significant in light of an earlier 9th Circuit holding in a case titled LVRC Holdings LLC v. Brekka. In that case, Christopher Brekka, while an employee of LVRC Holdings, sent a number of the employer's business documents to his private email account. At the time he sent the documents, he was also engaged in negotiations for the purchase of the company. The negotiations did not result in agreement, and he left the company. Later LVRC learned of Brekka's transfer of its documents and proceeded against him for violation of the CFAA.

In that case, the court found no violation because the employer had not notified Brekka of any restrictions on his access to the computer. The Brekka court held: "Therefore, as long as an employee has some permission to use the computer for some purpose, that employee accesses the computer with authorization even if the employee acts with a fraudulent intent."

The Significance Of The Difference In The Two Approaches

The primary lesson from these two decisions is that it is imperative that an employer precisely define the limits of an employee's access to its computer systems and databases. If an employee's improper computer access is ever to be found to be illegal, the employer must have first placed limitations on the employee's permission to use the computer and the employee must have violated or exceeded those limitations. As seen

from the Brekka decision above, failure to set limits means you may have little protection, even against fraudulently inclined employees.

In a classic summation of the principle, the Nosal court held: "Therefore, as long as the employee has knowledge of the employer's limitations on that authorization [to use the company computers and access company databases] the employee exceeds authorized access [under the statute] when the employee violates those limitations. It is as simple as that."

Despite the Ninth Circuit's wording, it may not be quite that simple, but it is clearly imperative that employers carefully define the scope of the permission they grant their employees to access and to use their information. If nothing is said, employees who access the information, even for fraudulent purposes, may not be found to have violated the CFAA. But if employers have defined the limits of the permission granted to employees to use their computer systems and databases, employees who violate that permission may be successfully prosecuted.

It's also important to note that Korn/Ferry had taken a number of steps before this lawsuit to protect its Searcher database – such as controlling electronic access to the database and controlling physical access to computer servers that contained the database. Korn/Ferry employees had unique usernames and created passwords for use on the company's computer system, including for use in accessing the Searcher database. Korn/Ferry included a phrase emphasizing the proprietary and confidential nature of the data on every report generated from the Searcher database. The company also had policies and agreements that explained the proprietary nature of information made available to employees and restricted use and communication of all such information, except for legitimate Korn/Ferry business.

Protect Your Assets

The specific methods an individual employer uses to protect its confidential, proprietary and trade secret information will vary depending on the nature of the information and the nature of the business operation. This is a situation in which one size does not fit all. Employers may be wise to speak with their labor and employment counsel before the horse bearing the company's crucial information leaves the barn.

Courts regularly tell employers, generally after they have unsuccessfully attempted to get the court's help in retrieving important information, that it is not the court's job to protect their confidential and proprietary information. It is the employer's job to do that in the first instance by implementing carefully thought out safeguards to protect its own systems. If employers have to seek a court's intervention, they want to make the court's job as easy as possible by being able to demonstrate that they have first taken reasonable steps to safeguard the information they are now telling the court is so crucial to the future success of the company.

This is an area where the employer has the right and the ability to set the rules for employee access to its important and crucial information. The takeaway: employers should establish systems and rules which will permit them to protect their valuable information to the maximum extent possible. Here's a simple equation to put this in perspective:

No Rules = Possibile Inability to Take Action Against Employees Who Steal Information From Computers.

Rules = Enhanced Ability To Protect Company Against Employees Who Might Be Tempted to Steal Company Secrets.

US v. Nosal.pdf (92.31 kb