9th Circuit Rules For Employers In Protecting Trade Secrets

Insights
5.12.11

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.

The U.S. Court of Appeals for the 9th Circuit recently decided a case which offers significant assistance to employers' efforts to protect their valuable trade secrets and confidential and proprietary company information from theft or misuse by employees, so long as employers do it correctly. *U.S. v. Nosal*

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 â€“ 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 Computer Fraud and Abuse Act (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." Note that CFAA also authorizes civil penalties for violations of its provisions.

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

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.

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 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."

We are not sure it is all that simple, but it is clearly imperative that you carefully define the scope of the permission you grant your employees to access and to use your information. If nothing is said, employees who access the information, even for fraudulent purposes, will not violate this statute. But if you have defined the limits of the permission granted to employees to use your computer systems and databases, employees who violate that permission can 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 â€“ 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

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.

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. We urge employers 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 you have to seek a court's intervention, you want to make the court's job as easy as possible by being able to demonstrate that you have first taken reasonable steps to safeguard the information you 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. Our advice: establish systems and rules which will permit you to protect your valuable information to the maximum extent possible. Here's a simple equation to put this in perspective:

No Rules = No Recourse Against Employees Who Steal Your Information From Your Computers.

Rules = Many More Ways To Protect Your Company Against Employees Who Might Be Tempted to Steal Company Secrets.

For more information contact your regular Fisher Phillips attorney.

This Legal Alert provides an overview on one specific court ruling. It is not intended to be, and should not be construed as, legal advice for any particular fact situation.

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.