http://www.laboremploymentlawblog.com/

SHEPPARD MULLIN
SHEPPARD MULLIN RICHTER & HAMPTON LLP
ATTORNEYS AT LAW

Labor & Employment Law BLOG
Up-to-date Information on Labor & Employment

05 | 3 | 2011

The Ninth Circuit Clarifies Application Of The Computer Fraud And Abuse Act Favorably For Employers

The Computer Fraud and Abuse Act ("CFAA") may now give employers some teeth to enforce a well-crafted computer use policy. The CFAA punishes 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." 18 U.S.C. § 1030(a)(4). Although primarily a criminal statute, the CFAA also includes civil remedies and a private right of action and, therefore, has broad implications for employers who want to protect trade secrets and confidential data from unauthorized access and abuse.

In *United States v. Nosal* (April 28, 2011), the Ninth Circuit clarifies the reach of the CFAA in the employment context and provides some insight as to how employers may draft computer and data use policies to invoke the protections of the Act. Specifically, the Ninth Circuit held that employees not only violate the CFAA when they access a computer or database that they did not have authorization to access, but also where employees exceed authorized access by accessing information they were only entitled to access under limited circumstances.

The facts of *Nosal* are instructive and, unfortunately, not unique. Nosal was an executive for the executive search firm Korn/Ferry International. When Nosal left his employment with Korn/Ferry, he signed a separation and release and an independent contractor agreement. As part of the agreements, in exchange for considerable monthly payments over a twelve-month period, Nosal agreed not to compete with Korn/Ferry for one year. However, shortly after leaving his position with Korn/Ferry, Nosal decided to start a competing business. To help him get started, Nosal enlisted some Korn/Ferry employees to use their computer accounts to access Korn/Ferry's computer system and retrieve data, including executive candidate information that Korn/Ferry regarded as highly confidential proprietary information. The employees had authorization to access the executive candidate data, but only for legitimate Korn/Ferry business. According to the indictment, the employees gathered names and contact information of executive candidates maintained in Korn/Ferry's database and transferred the data to Nosal.

The Court recognized that Korn/Ferry had taken considerable measures to protect the confidentiality of the data in its database. One of the key points noted by the Court is that Korn/Ferry controlled physical access to its database using unique employee usernames and passwords. Korn/Ferry also had a strict rule that usernames and passwords were only to be used by the assigned Korn/Ferry employee. In addition,

Korn/Ferry had its employees enter into agreements that explained the proprietary nature of the data in its databases and restricted the use and disclosure of the data to legitimate Korn/Ferry business. Thus, when the employees transferred data to Nosal, they not only violated Korn/Ferry's restricted use policy, but they also violated the CFAA because they exceeded their use authorization.

In his defense, Nosal argued that if the CFAA was interpreted to include employee use that exceeds authorization, it would lead to prosecution of employees for innocent misuse or for merely violating the employer's use policies. For example, a violation of the CFAA would occur when an employee who has been granted access to sensitive data out of curiosity looks at additional data. The Ninth Circuit rejected this argument and was persuaded that the specific intent and causation requirements of the statute provide sufficient protection from prosecution for innocuous violations of an employer's use policy.

Moreover, under the Ninth Circuit's interpretation, for a violation of the CFAA to occur, the employer must have placed restrictions on the employee's permissible use. Therefore, to receive the full benefit of the CFAA, a use restriction policy should carefully explain what is and is not permissible use.

Now is an excellent time for employers to review their computer use policies or consider adopting one. To take full advantage of the protections of the CFAA, a policy should contain clear and conspicuous use restrictions. At minimum, the policy should make it clear that employees may access and use information available on or through work computers only for legitimate and authorized business purposes, and that employee access and use rights will be deemed revoked if they use work computers for unauthorized purposes.

Authored by Sheppard Mullin's Labor & Employment Practice Group.