Employees Beware: The 9th Circuit Finds That Unauthorized Access To An Employer's Computer May Create Criminal Liability Under The Computer Fraud & Abuse Act

Publication
5.03.11

The 9th Circuit in *United States of America v. Nosal* (No. 10-10038, opinion by Judge Trott) for the purposes of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. section 1030, an employee's use of an employer's computer "exceeds authorized access" when he or she obtains information from the computer and uses it for a purpose that violates the employer's restrictions regarding the use of such information. Under the CFAA, criminal liability attaches where such use is accompanied by an intent to defraud, furthers the intended fraud, and obtains *anything* of value.

The CFAA was enacted in 1986 and criminalized unauthorized use of computer systems and federal computer-related offenses. The CFAA subjects to punishment 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."

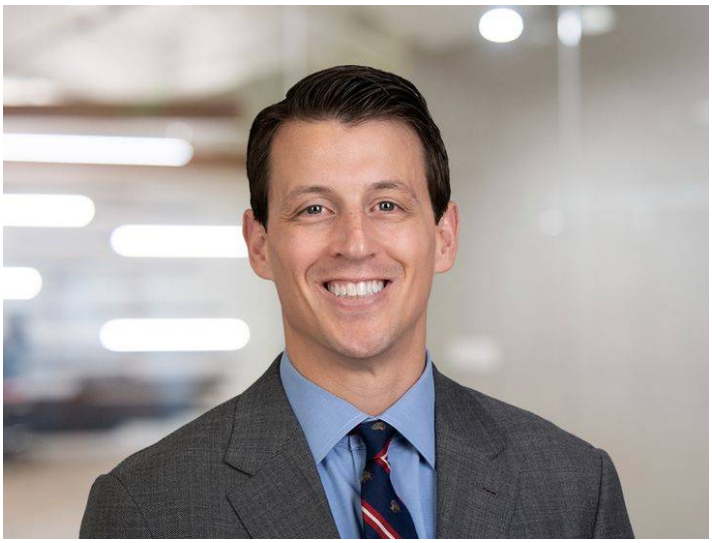
In *Nosal*, the employee David Nosal, worked as an executive for Korn/Ferry International ("KFI"), an executive search firm. When Nosal left KFI in 2004, he signed a Separation and General Release Agreement and an Independent Contractor Agreement. Under these agreements, Nosal agreed to serve as an independent contractor for KFI for a period of one year. However, shortly after leaving KFI, Nosal engaged three KFI employees to help him start a competing business. According to the indictment, Nosal next obtained trade secrets and other proprietary information (source lists, names, and contact information) from KFI through the use of the employees user accounts and access to the KFI computer system.

KFI considered the information contained on the database "to be one of the most comprehensive databases of executive candidates in the world." In order to safeguard the information, KFI: limited electronic and physical access to the database; required all employees to enter into agreements explaining the proprietary nature of the information and restricting use to legitimate KFI business; declared the confidentiality of the information on the database by placing the phrase "Korn/Ferry Proprietary and Confidential" on every "Custom Report;" and displayed a notification to all users upon log-in confirming the proprietary nature of the database and warning of possible disciplinary action or criminal prosecution.

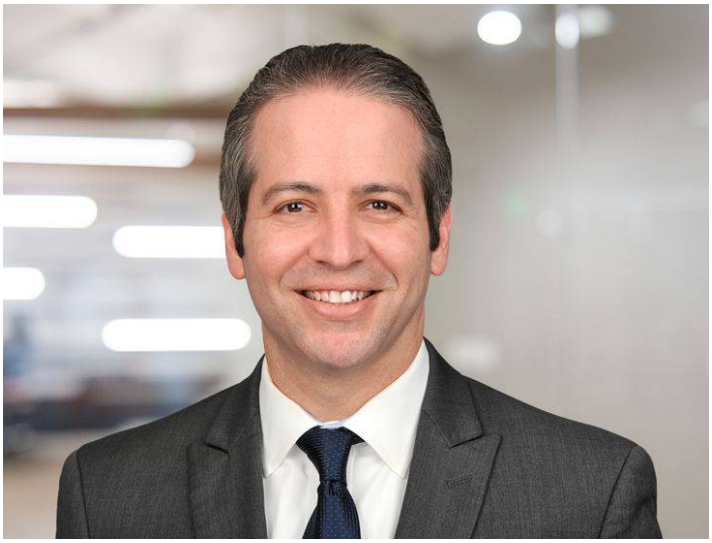
In response to Nosal's actions, the government filed a twenty-count superseding indictment. In the indictment, counts 2 through 9 of alleged violations of the CFAA.

This article was posted on May 3, 2011 on *The Ninth*.

Related People



Colin P. Calvert
Partner
949.798.2160
Email



Todd B. Scherwin
Regional Managing Partner
213.330.4450
Email