THE
NATIONAL LAW REVIEW

Accessing Database Violates Computer Fraud and Abuse Act and Economic Espionage Act – Ninth Circuit Affirms Criminal Conviction of Former Employee

jackson lewis.

Article By Dylan B. Carp
Clifford R. Atlas Ravindra K. Shaw
Jackson Lewis P.C.
Non-Compete & Trade Secrets Report Blog
Labor & Employment
Litigation / Trial Practice
Criminal Law / Business Crimes
9th Circuit (incl. bankruptcy)

Tuesday, July 19, 2016

The ***Ninth Circuit*** recently filed its latest installment in the saga involving *David Nosal* and his former employer, Korn/Ferry International, an executive search firm. Korn/Ferry maintains a proprietary database of executive candidates for its paying customers. Nosal, a former Korn/Ferry executive, set up a competing business. Allegedly desiring the information in Korn/Ferry's database for his competing business, Korn/Ferry alleged that Nosal tried two methods to access it: (1) using his own user name and password to download information before his departure; and (2) after his departure, using the user name and password of a willing accomplice who was still employed by Korn/Ferry.

Nosal was charged with violating a criminal provision of the federal ***Computer Fraud and Abuse Act,*** 18 U.S.C. § 1030 ("CFAA"), which states, "[w]hoever…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…shall be punished." This provision also provides for civil liability. In a prior decision, ***United States v. Nosal*** *("Nosal I")*, 676 F.3d 854 (9th Cir. 2012) (en banc), the appellate court held the CFAA does not prohibit Nosal's first act—using his user name and password to obtain Korn/Ferry's information during his employment—because using information in an unauthorized way is not "exceed[ing] authorized access."

In *United States v. Nosal*, No. 14-10037 (9th Cir. July 5, 2016) ("*Nosal II*"), the court held Nosal's second act—obtaining Korn/Ferry's information by logging in to the database with the user name and password of a willing currently-employed accomplice—*does* violate the CFAA. The panel, by a vote of 2-1, held such activity violated the unambiguous meaning of the phrase "access a protected computer without authorization." The court noted its holding is in accord with all other circuits to have addressed this issue: the Second, Fourth and Sixth Circuits. Accordingly, the court affirmed Nosal's conviction.

The dissent, which the majority largely ignored, would have held that because Nosal had the "authorization" of the willing accomplice, he did not violate the CFAA. The dissent was concerned that the majority's broader reading of "authorization" may criminalize innocent acts—including what the dissent termed "password sharing," such as a former employee who accesses his former employer's database using a current employee's credentials to assist his former colleague for a legitimate reason.

In a portion of the opinion that may be overlooked given the long-running drama over whether the CFAA should be interpreted broadly or narrowly, the Ninth Circuit also affirmed Nosal's conviction for trade secret theft under the Economic Espionage Act, 18 U.S.C. § 1832 ("EEA"). Nosal appealed his conviction in part on the ground the information contained in the Korn/Ferry database was not a trade secret because it contained publicly-available information and was akin to a customer list. The appellate court rejected Nosal's contentions, and held – significantly – that a list of customers may qualify for trade secret protection. Moreover, the court noted the database was more than a mere list of executive candidates. The database contained information on over one million executives, including contact information, employment history, salaries, biographies and resumes, all

compiled since 1995. When launching a new search to fill an open executive position, Korn/Ferry could compile a "source list" of potential candidates, which was the result of a query run through a proprietary algorithm that generated a custom subset of possible candidates. The court held the jury was permitted to find the database contained Korn/Ferry's trade secrets.

Nosal II has two implications for the civil remedies available to employers to protect their trade secrets and other property. First, because the CFAA provides for civil causes of action, the decision affirms an employer's right to sue a former employee who accesses its data by using someone else's credentials. Second, in light of the Defend Trade Secrets Act—which provides a civil claim for trade secret misappropriation under the EEA and relies on the same definitions supporting the EEA—*Nosal II* affirms that customer lists and related information deserve legal protection.