THE NATIONAL LAW JOURNAL
NOVEMBER 28, 2016
An ALM Publication
THE PRACTICE | Commentary and advice on developments in the law

It's Easier for Employers to Sue for Data Theft

Why a Ninth Circuit decision and an amendment to the Economic Espionage Act change the landscape.

BY NICK AKERMAN

BEEBRIGHT/SHUTTERSTOCK.COM

Two new developments this past year have made it easier for employers to sue employees in federal court for stealing data from company computers.

The most recent is the U.S. Court of Appeals for the Ninth Circuit's July decision in *U.S. v. Nosal* interpreting what it means to access a company computer "without authorization" under the Computer Fraud and Abuse Act (CFAA), the federal computer criminal statute. 18 U.S.C. 1030. The other development is the May amendment to the Economic Espionage Act (EEA), the federal criminal trade secrets act, permitting companies to file a federal civil action against individuals who steal the company's competitively sensitive data. 18 U.S.C. 1831, et. seq.

The CFAA, which makes it a crime for someone to steal company data, has provided for civil actions since 1994 for anyone victimized by a violation of the statute. However, the Ninth Circuit in 2009 in *LVRC Holdings v. Brekka* limited an employer's ability to sue employees under the CFAA on the theory that employees by virtue of their employment are granted access to the company computer system to perform their jobs and therefore cannot access the company computers without authorization or by exceeding authorized access, the critical element of the statute.

The *Brekka* case distinguished between access restrictions and use restrictions and held that the "exceeds authorized access" prong of the CFAA "does not extend to violations of [a company's] use restrictions. *Brekka* was adopted by the Second and Fourth Circuits, thereby exacerbating a split with the First, Fifth, Seventh and Eleventh Circuits, which make no such distinction between access and use. Thus, as of the beginning of this year, whether an employer could file a suit in federal court against an employee who stole company data was solely de-pendent on where the theft occurred.

The *Nosal* case addressed the classic case of an employee who steals his employer's data to jump start a competing business. David Nosal, who worked at the executive search firm Korn/Ferry, was not promoted, and for that reason he and several other employees decided to leave and create a competing firm.

NEW INDICTMENT AFTER INITIAL LOSS

While still employed by Korn/Ferry, Nosal and his cohorts downloaded confidential information from Korn/Ferry's proprietary database for use at their competing venture. Applying *Brekka*, the first *Nosal* decision decided by the Ninth Circuit in 2012 dismissed the CFAA counts alleging theft of data from the company computers because Nosal was a Korn/Ferry employee, even though his actions violated Korn/Ferry's confidentiality and computer-use policies.

Thereafter, the government indicted Nosal for CFAA violations that occurred after Nosal had resigned from Korn/Ferry. When Nosal resigned, Korn/Ferry revoked his password to its proprietary database. His status became a contractor whose work was limited to completing specific projects. As such, he was not entitled to access the Korn/Ferry database. Instead, Nosal had a current employee, in violation of her standard company confidentiality agreement that prohibited the sharing of passwords, use her password to access the database to obtain information for Nosal's competing business.

In July, the Ninth Circuit affirmed Nosal's CFAA conviction, rejecting the argument that its decision would "criminalize password sharing." The court focused on the "without authorization" prong of the CFAA rather than the "exceeding authorized access" prong and held that " 'without authorization' is an unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission."

The court also emphasized its "simple corollary: once authorization to access a computer has been affirmatively revoked, the user cannot sidestep the statute by going through the back door and accessing the computer through a third party," recognizing that [u]nequivocal revocation of computer access closes both the front door and the back door."

This principle of affirmative permission and unequivocal revocation should apply with equal force to current employees where the scope of authorized access is just as affirmatively spelled out. For example, based on *Nosal*, an employer could limit access to a highly sensitive database by providing access credentials only to employees with a need to use the information while at the same time establishing a policy forbidding the sharing of passwords.

While this would not subject the employee authorized to access the database with CFAA liability, other strategies can be employed by prohibiting access to the company computers through portable media or web-based email accounts, which are commonly used to steal company data.

The key to formulating such policies in the circuit courts that follow the Ninth is to avoid any policy that can be interpreted as a prohibition on the use of the data.

Most significantly, no matter what jurisdiction the data theft occurs, employers now have the right to sue in federal court under the EEA for not only the theft of trade secrets data, but also their use. As the *Nosal* court recognized, the EEA is not limited to a Coca-Cola type proprietary formula, but "by its terms, includes financial and business information."

In light of the split in the circuits on the interpretation of the "exceeds authorized access" prong of the CFAA, the U.S. Supreme Court will at some point resolve the law's interpretation, likely in favor of employers. The common-sense meaning for an employee to exceed authorized access is for the employee to access the company computer for reasons other than performing legitimate company business. When that happens, employers have two powerful tools to go after employees who steal data from the company computer.

NICK AKERMAN *is a partner in the international law firm Dorsey & Whitney. He is a member of the trial group and includes among his specialties the protection of competitively sensitive information and trade secrets litigation. He can be contacted at akerman.nick@dorsey.com.*