Nick Akerman
(212) 415-9217 ▪ akerman.nick@dorsey.com

Nick is a partner in the New York office of Dorsey & Whitney.
For more articles like this go to http://computerfraud.us

DORSEY
DORSEY & WHITNEY LLP

Employers should include access restrictions in agreements, limit access with technology and consider the jurisdiction.

BY NICK AKERMAN

In all jurisdictions the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030, the federal computer crime statute, applies to former employees who steal data from the company computer, but in two federal circuits it does not apply when the theft occurs during employment. The difference in jurisdictions is significant to employers because the CFAA provides a civil remedy for damages and injunctive relief for a company that "suffers damage or loss" by reason of a violation of the CFAA. 18 U.S.C. 1030(g).

Last year the U.S. Court of Appeals for the Ninth Circuit in *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012), disagreed with certain of its sister circuits and narrowly interpreted what it means to access the company computer "without authorization," effectively eliminating a company's ability in that jurisdiction to use the CFAA against current employees. This article will review the conflicting interpretations of the CFAA that distinguishes between current and former employees and the strategies and options companies can employ to navigate this conflict.

The traditional remedy against the employee who steals competitively sensitive data from the company computers has been the state trade secrets laws. The CFAA provides a new approach with key advantages; as a federal statute, the CFAA includes the right to sue in federal court, not just state court, and does not require proof of the elements of a trade secret: that the data is in fact secret and that reasonable efforts were performed to maintain its secrecy. In contrast to trade secrets law, the CFAA only requires an employer to prove that the employee accessed the company computer "without authorization" or that the employee exceeded authorized access. "[W]ithout authorization" is not defined by the statute, but "exceeds authorized access" is defined as accessing "a computer with authorization and [using] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. 1030(e)(6).

THE PRACTICE
Commentary and advice on developments in the law

Nosal, an en banc opinion, reversed the decision of a three-judge panel and relied on the circuit's earlier decision in *LVRC Holdings v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009), which held that it is the employer's actions in granting or denying permission to use the company computer and not the employee's intent in accessing the computer

that determines whether the employee's access was "without authorization." Because an employer permits an employee "to use the company computer," an employee cannot "act without authorization." *Id*. The only circuit that has adopted *Nosal* is the Fourth. *WEC Carolina Energy Solutions LLC v. Miller*, 687 F. 3d 199, 204 (4th Cir. 2012), *cert. denied*, 133 S. Ct. 831 (2013).

The Ninth and Fourth circuits are at odds with the Fifth, Seventh and Eleventh circuits, which interpret "without authorization" broadly to include an employee who accesses the company computer with an intent to steal data or to use the data in violation of a company policy, or who removes the data for other than a proper business purpose. *International Airport Centers LLC v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006); *U.S. v. John*, 597 F.3d 263, 269, 272 (5th Cir. 2010); *U.S. v. Rodriguez*, 628 F.3d 1258, 1262 (11th Cir. 2010). Despite this conflict among the circuit courts, the Supreme Court recently denied the petition for review in *Miller*. In those circuits that have not yet decided this issue, district courts are choosing between the two views. *See, e.g., Sebrite Agency Inc. v. Platt*, 884 F. Supp. 2d 912, 918 n.2 (D. Minn. 2012).

The recent decision in *Metabyte Inc. v. Nvidia Corp*., 2013 WL 1729808 (N.D. Calif. April 22, 2013), reflects the status of the law in the Ninth Circuit. Metabyte, a software company, sued four of its former employees for CPAA violations, alleging that, while employed, they stole Metabyte's software code and took it to their new employer, Nvidia, where it was used to develop Nvidia's competing software. The court dismissed the CFAA claims based on *Nosal*, finding that the employees "had access to the information at issue, that access was authorized (even if circumscribed) and not exceeded," and that they were employees who had been "hired to work on the very information presently at issue." *id*. at 4. Thus, the defendants could not have violated the CFAA because they had been authorized to access Metabyte's computers.

Nosal, however, does not necessarily spell the end of the use of the CFAA against employees in the Ninth and Fourth circuits. Following the Ninth Circuit's decision in *Nosal* and prior to trial, the defendants in that case moved in the district court to dismiss the three remaining CFAA counts that had not been the subject of the appeal. *U.S. v. Nosal*, 2013 WL 978226 (N.D. Calif. March 12, 2013). Those three counts alleged that David Nosal, while he had been employed by the executive-search firm Korn/Ferry, had been aided and abetted by two former Korn/Ferry employees and one current Korn/Ferry employee, who provided him with confidential data from the company's proprietary database of executives and companies. Nosal, according to the indictment, had set up a rival executive-search firm while still employed by Korn/Ferry.

These three counts alleged that a former Korn/Ferry employee twice accessed the Korn/Ferry database to conduct searches using a current Korn/Ferry employee's password that was "intended for use by employees only" and had requested the current employee whose password she had used to provide other information from the

database to Nosal. On another occasion, Nosal's former assistant, who was still employed by Korn/Ferry, remotely accessed the Korn/Ferry database from Nosal's office and then turned over the computer to a former Korn/Ferry employee who downloaded search information from the database.

The district court upheld the validity of these three CFAA counts. The court found that the use of another employee's password to access the computer was "without authorization" because it was the employer's intent to limit access to those who were assigned the individual passwords. *Id.* at *2. The court observed, "If the CFAA were not to apply where an authorized employee gave or even sold his or her password to another unauthorized individual, the CFAA could be rendered toothless." *Id*. at *9.

As to the count alleging that a current employee remotely entered her password on the Korn/Ferry database and then allowed a former employee to review the database, the court held that "[t]he common definition of the word 'access' encompasses not only the moment of entry, but also the ongoing use of a computer system," and the former employee was not authorized to access the Korn/Ferry database. *Id*. at *10. On April 24, the jury convicted Nosal on, among other things, all three CFAA counts.

Given the conflict in the circuits, employers faced with employee theft of data should consider the following options and strategies:

- The Ninth Circuit's holding in *Nosal* only invalidated those CFAA counts in the indictment alleging that Nosal accessed the Korn/Ferry database "without authorization" based on Korn/Ferry's employee agreement that restricted "the use of the database and related information to legitimate company business." *Id*. at *2. There was no restriction on access. This leaves open the possibility that the Ninth Circuit would enforce agreements/company rules that restrict employee access for certain nonbusiness purposes such as removing data to be used to compete against the company. The First Circuit in *EF Cultural Travel B.V. v. Zefer Corp*., 318 F.3d 58, 63 (1st Cir. 2003), recognized that the "CFAA...is primarily a statute imposing limits on access and enhancing control by information providers." Thus, a company "can easily spell out explicitly what is forbidden." Companies in all jurisdictions should consider using such access restrictions in their agreements and policies.

- Similarly, employers should use technological means to limit an employee's access to those portions of the computer network needed to perform the scope of the employee's job. A theft of data from an off-limits portion of the network would then exceed authorized access.

- One such access restriction emphasized in the recent district court decision in *Nosal* is use of passwords for individual access. As the court pointed out, "[T]he CFAA appears to contemplate that one using the password of another may be accessing a

computer without authorization, as it elsewhere provides penalties for anyone who 'knowingly and with intent to defraud traffics in any password or similar information through which a computer may be accessed without authorization.'" *Id.* at *9. Thus, an employer should promulgate strong policies forbidding the use and dissemination of individual employee passwords.

• Finally, before filing a CFAA action, it is critical for the employer to consider the jurisdiction in which the action will be brought, tailor the complaint to the law in that jurisdiction and carefully investigate and plead all facts showing that the access to the company computer was done without the permission of the employer. As reflected in *Metabyte*, a court is unlikely to allow an employer to explore various factual theories post-complaint in discovery to validate a factually invalid CFAA pleading.