SMITH ANDERSON
expectexcellence®

FOURTH CIRCUIT LIMITS SCOPE OF EMPLOYERS' CLAIMS UNDER COMPUTER FRAUD AND ABUSE ACT

02.06.2014
Isaac Linnartz

In July 2012, the United States Court of Appeals for the Fourth Circuit issued an important decision limiting the claims employers can bring against disloyal current and former employees under the federal Computer Fraud and Abuse Act (CFAA). Subject to certain limitations, the CFAA creates a civil cause of action against a person who "intentionally accesses a computer without authorization or exceeds authorized access" and "thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(a)(2). (For a general discussion of the CFAA, see "The Computer Fraud and Abuse Act: A Potentially Potent Weapon for Employers to Combat Misappropriation of Trade Secrets", *The Litigator, Vol.* 31, No 1, July 2010, reprinted below.) Using this and similar provisions in the CFAA, employers have asserted claims against employees who misappropriated or misused confidential information obtained from their employers' computer systems. The federal courts have issued conflicting decisions, however, over whether an employee who is otherwise authorized to access information loses that authorization when he or she accesses or uses such information for a disloyal purpose (e. g., to share that information with a competitor with whom the employee intends to accept employment). For a more detailed discussion of this issue and the CFAA generally, please see Susan Hargrove and Courtney Mischen's July 2010 article "The Computer Fraud and Abuse Act," which was originally published in *The Litigator*.

The Fourth Circuit first addressed the CFAA's prohibition on accessing a computer "without authorization" or by "exceed[ing] authorized access" in *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012). *WEC Carolina* involved an employee who allegedly downloaded his employer's proprietary information. *Id.* at 202. After leaving his employment, the employee used that proprietary information in a presentation he made on behalf of a competitor to a potential customer. *Id.* The employer sued the former employee, his assistant, and the competitor under the CFAA, claiming that they violated the CFAA by accessing the proprietary information "without authorization" or by "exceed[ing] authorized access." *Id.* The district court dismissed this claim, and the Fourth Circuit affirmed, holding that the terms "without authorization" and "exceeds authorized access" only apply "when an individual accesses a computer without permission or obtains or alters information on a computer beyond what he is authorized to access." *Id.* at 206. Under this interpretation, an employee's misappropriate or misuse of information does not violate the CFAA if the employee was permitted to access that information. The Ninth Circuit has reached the same conclusion. *United States v. Nosal*, 676 F.3d 854, 862-64 (9th Cir. 2012) (en banc). On the other hand, the Fifth, Seventh, and Eleventh Circuits have concluded that an employee who accesses information he or she is otherwise authorized to access loses that authorization and becomes subject to liability under the CFAA when the employee does so for a disloyal or prohibited purpose. *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010); *United States v. John*, 597 F.3d 263, 271-73 (5th Cir. 2010); *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006).

The Supreme Court has not yet addressed this issue. In January 2013, the Supreme Court declined to review the Fourth Circuit's decision in *WEC Carolina.* Given the current Circuit split, however, there is a good chance that the Supreme Court will eventually hear and decide this issue. In the interim, the scope of the claims available to employers under the CFAA will depend on the Circuit in which those claims are filed.

PROFESSIONALS

Isaac A. Linnartz

PRACTICE AREAS

Non-Compete & Trade Secrets