

---

For more insights, news and analysis visit our Knowledge Center.

## Fourth Circuit Widens Split Over CFAA and Employees Violating Computer Use Restrictions

10 September 2012

### Professionals

Audra A. Dial; John M. Moye

### Services

Trade Secret; Labor & Employment

---

On July 26, 2012, the Fourth Circuit Court of Appeals weighed in on the debate about the meaning of the phrases "exceeds authorized access" and "without authorization" as used in the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030. See *WEC Carolina Energy Solutions, LLC v. Miller*, No. 0:10-CV-02775, CMC (4th Cir. July 26, 2012). Joining the Ninth and Second Circuits in narrowly construing the statute, the Fourth Circuit held that the CFAA cannot be used to impose liability on an employee who is given lawful access to company information but later misuses that information (in violation of the employer's computer use policies). Judge Floyd delivered the opinion of the Court, which ruled that the CFAA may be used to impose civil liability on employees either who are not permitted to access certain information but do so anyway, or who go "beyond the bounds" of their authorized access; however, the Court expressly found that the CFAA's prohibitions do not impose liability on an employee who has permission to access electronic information but then "improper[ly] use[s]" that information (for example, to develop a competing business).<sup>[1]</sup>

The Fourth Circuit's decision broadens a split on whether the CFAA extends to employees who misuse information gained from company computers to which they have been provided access. The decision raises significant implications for employers in Virginia, North Carolina and South Carolina and how they draft computer use policies. Moreover, at least in the Fourth Circuit, it will be increasingly difficult to bring a CFAA claim as a way to obtain federal question jurisdiction over a trade secret misappropriation case involving electronic information. Although CFAA claims are often used in conjunction with trade secret claims to obtain federal jurisdiction, the *WEC* ruling will likely decrease the opportunity to use the CFAA in this way, at least in the Fourth Circuit.

### CFAA Background

The CFAA prohibits a person from "intentionally access[ing] a computer without authorization" or "exceed[ing] authorized access," thereby obtaining "information" from a computer that is "used in or affecting interstate or foreign commerce."<sup>[2]</sup> Although the CFAA is a criminal statute, it also permits private parties who suffer "damage or loss by reason of a violation" to bring a civil action for compensatory damages and injunctive relief.<sup>[3]</sup>

The *WEC* case involved a familiar trade secret misappropriation allegation against a former employee. WEC, a company that provides welding services to the power industry sued its ex-employee, Willie Miller; his assistant, Emily Kelley; and their new employer, Arc Energy Services. During his employment, WEC provided Mr. Miller with a company laptop and granted him access to the company's servers and intranet, which contained a large amount of sensitive company data. The company had policies in place prohibiting the misuse of company information (including restrictions on the ability to download that information to personal computers); however, WEC imposed no restrictions on Mr. Miller's ability to access the information.<sup>[4]</sup>

Mr. Miller resigned from WEC and joined WEC's competitor, Arc. WEC alleged that, prior to resigning, and while still employed by WEC, Mr. Miller downloaded a number of confidential documents from the company's servers and emailed them to his personal e-mail account. Twenty days after leaving WEC, Mr.

Miller made a presentation to a potential customer on behalf of Arc in which he allegedly used the confidential information he had downloaded from the WEC servers.<sup>[5]</sup> The customer ultimately awarded projects to Arc based upon the presentation.

WEC brought suit in federal court in South Carolina, asserting nine causes of action, including misappropriation of trade secrets, tortious interference with contract, conversion, and a CFAA claim.<sup>[6]</sup> The district court dismissed the CFAA claim under Rule 12(b)(6) because WEC's policies did not limit Miller's "access" to such electronic information.<sup>[7]</sup> The district court determined that the CFAA requires that an employee either access a computer "without authorization" or "exceed authorized access," whereas Miller had been permitted to access the information; thus, no liability under the CFAA was warranted.<sup>[8]</sup> The remaining state law claims were dismissed for lack of subject matter jurisdiction.

### The Fourth Circuit's Opinion

On appeal, a unanimous three-judge panel of the Fourth Circuit affirmed the district court's interpretation of the CFAA. In its opinion, the court examined the scope of the CFAA and whether its provisions "extend to violations of policies regarding the use of a computer or information on a computer to which a defendant otherwise has access."<sup>[9]</sup> The court ultimately concluded that the phrases "without authorization" and "exceeds authorized access" as used in the statute mean that an employee cannot either "gain admission to a computer without approval" or gain information that is located "outside the bounds of his approved access."<sup>[10]</sup> The court declined to extend the CFAA to impose liability on employees for "the improper use of information validly accessed" by the employee.<sup>[11]</sup> Because Mr. Miller had been given access to the information he allegedly downloaded by his employer, WEC, the Fourth Circuit concluded there was no basis for a CFAA violation (regardless of whether he misused the information to which he was provided access).

The Fourth Circuit raised concerns about reading the CFAA too broadly in light of the "rule of leniency" applicable in criminal law, concerns which were similar to those recently raised by the Ninth Circuit in its *en banc* decision in *United States v. Nosal*.<sup>[12]</sup> The Court noted that reading the CFAA this broadly could result in potential liability for any employee who "checked the latest Facebook posting or sporting event scores in contravention of his employer's use policy."<sup>[13]</sup> Such an interpretation would "transform a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy."<sup>[14]</sup> The Fourth Circuit thus aligned with the Ninth Circuit in finding the CFAA prevents only hacking and does not prohibit broader misuse. In contrast, the Fifth, Seventh and Eleventh Circuits have taken a broader view of the CFAA and have held that liability may be imposed when an employee acts against his employer's interest and violates a company's corporate computer use restriction.<sup>[15]</sup>

### A Widening Circuit Split

The Fourth Circuit's decision to follow the Ninth Circuit's narrow approach to the CFAA—and its rejection of other circuits' view that the CFAA extends to violations of "computer use" policies—creates a widening circuit split on the scope and meaning of the CFAA. Any hopes that the U.S. Supreme Court would resolve the circuit split soon were dashed in August 2012, when the U.S. government announced that it would not seek Supreme Court review of the Ninth Circuit's decision in *Nosal*.<sup>[16]</sup> Thus, at least for now, the scope of the CFAA will depend largely on the location of the company seeking to protect its information; depending on the particular jurisdiction, the CFAA may no longer be an effective tool to prevent an employees' misuse of electronic information and trade secrets.

### Practical Implications

The *WEC* decision adds to a growing number of courts who view the CFAA as a statute simply designed to target "hacking" rather than other kinds of misuse of electronic information. This ruling will impact a trade secret plaintiff's ability to obtain federal court jurisdiction over its trade secret claims that involve the theft of electronic trade secrets (unless the plaintiff can establish diversity jurisdiction). As the Fourth Circuit held, at least in certain jurisdictions, the CFAA can no longer be used as a proxy for trade secret misappropriation claims and other tort and contract-based claims against former employees.<sup>[17]</sup> Thus, although CFAA claims have been routinely added to trade secret cases, the *WEC* ruling will likely make the use of such claims more rare, at least in the Fourth Circuit.

Additionally, the Fourth Circuit's *WEC* ruling makes clear that computer use restrictions are necessary, but not sufficient, to protect confidential, electronic information. In addition to use restrictions, employers should limit its employees' access to sensitive information—granting access only to those employees with a specific need-to-know—instead of merely policing the use by all employees of that information. Limiting access to confidential information at the outset will not only decrease the possibility of a misappropriation, but could also preserve use of the CFAA as a litigation tool even under the narrow view of the CFAA—e.g., in the case of an employee who misuses electronic information that he was not authorized to access in the first place. Implementing stricter guidelines governing which employees may access certain information and for what purpose will provide stronger support for a CFAA claim, even in the Second, Fourth and Ninth Circuits.

[1] See *WEC Carolina Energy Solutions, LLC v. Miller*, No. 0:10-CV-02775, CMC (4th Cir. July 26, 2012), Slip Op. at 9, 14.

[2] See 18 U.S.C. § 1030(a)(2)(C).

[3] 18 U.S.C. § 1030(g).

[4] *WEC*, Slip Op. at 4.

[5] *Id.* at 4.

[6] *Id.* at 4; *id.* at 13, n.4.

[7] See *WEC Carolina Energy Solutions, LLC v. Miller*, No. 0:10-CV-2775-CMC, 2011 WL 379458, at \*5 (D.S.C. Feb. 3, 2011).

[8] *Id.*

[9] *WEC*, Slip Op. at 6.

[10] *Id.* at 9.

[11] *Id.* (emphasis in original).

[12] *Id.* at 7-8, 12.

[13] *Id.* at 12.

[14] *Id.* at 12.

[15] See *Int'l Airport Centers v. Citrin*, 440 F.3d 418 (7th Cir. 2006) (employee no longer has authorized access when he exceeds the scope of the authority given to him by his employer—at that point liability can be imposed); see also *U.S. v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010) (misuse of personal information in violation of employee policy prohibiting employees from accessing information for "nonbusiness purposes" is sufficient to impose liability); *U.S. v. John*, 597 F.3d 263 (5th Cir. 2010) (same).

[16] See REUTERS, "U.S. Will Not Challenge Computer Fraud Case to High Court," August 9, 2012, available at <http://in.reuters.com/article/2012/08/08/net-us-computerfraud-law-idINBRE8771BK20120808>.

[17] *WEC*, Slip Op. at 13 (noting that providing recourse under the CFAA is "unnecessary" because "other legal remedies exist for these grievances," including trade secret misappropriation).

For more information about these issues, please contact the author(s) of this Legal Alert or your existing firm contact.

Name	Telephone	Email
Audra A. Dial	+1 404.815.6307	<a href="mailto:Adial@kilpatricktownsend.com">Adial@kilpatricktownsend.com</a>
John M. Moye	+1 919.420.1821	<a href="mailto:Jmoye@kilpatricktownsend.com">Jmoye@kilpatricktownsend.com</a>

The information contained in this Legal Alert is not intended as legal advice or as an opinion on specific facts. For more information about these issues, please contact the author(s) of this Legal Alert or your existing firm contact. The invitation to contact the author is not to be construed as a solicitation for legal work. Any new attorney/client relationship will be confirmed in writing. You can also contact us through our web site at [www.KilpatrickTownsend.com](http://www.KilpatrickTownsend.com).

Copyright ©2010-2012 Kilpatrick Townsend & Stockton LLP. This Legal Alert is protected by copyright laws and treaties. You may make a single copy for personal use. You may make copies for others, but not for commercial purposes. If you give a copy to anyone else, it must be in its original, unmodified form, and must include all attributions of authorship, copyright notices and republication notices. Except as described above, it is unlawful to copy, republish, redistribute and/or alter this newsletter without prior written consent of the copyright holder. For reprint and redistribution requests, please email [KTSLegal@KilpatrickTownsend.com](mailto:KTSLegal@KilpatrickTownsend.com).