No. 11-1201

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

WEC CAROLINA ENERGY SOLUTIONS, LLC,

Appellant,

v.

WILLIE "MIKE" MILLER, EMILY KELLEY and
ARC ENERGY SERVICES, INC.,

Appellees.

On Appeal from the United States District Court
for the District of South Carolina

BRIEF OF APPELLANT WEC CAROLINA ENERGY SOLUTIONS, LLC

Mark Gordon, Esquire
Anthony J. Basinski, Esquire
PIETRAGALLO GORDON ALFANO
BOSICK & RASPANTI, LLP
One Oxford Centre
The Thirty-Eighth Floor
Pittsburgh, PA 15219
(412) 263-2000

Angus H. Macaulay, Esquire
Kirsten Small, Esquire
NEXSEN PRUET, LLC
P.O. Drawer 10648
Greenville, SC 29603
(864) 370-2211

Counsel for Appellant
WEC Carolina Energy Solutions, LLC

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

Cases

Federal Statutes

Other Authorities

Rules

Treatises

STATEMENT OF JURISDICTION

The District Court had jurisdiction pursuant to 28 U.S.C. § 1331 because one claim is for violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. The Court below also had supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367(a). This Court has jurisdiction pursuant to 28 U.S.C. § 1291, as WEC appeals a final decision of the District Court dated February 3, 2011, and the Notice of Appeal was timely filed on March 4, 2011.

STATEMENT OF ISSUES FOR REVIEW

1. Did the district court err in granting Miller and Kelley's Motion to Dismiss the claim under the Computer Fraud and Abuse Act when they were not authorized to access confidential information and trade secrets on WEC's computers and servers on behalf of a third party competitor?

2. Did the district court err in granting Miller and Kelley's Motion to Dismiss when they exceeded authorized access by improperly accessing and downloading certain information from WEC's computers and servers in violation of company policy?

3. Did the district court err in dismissing the claim against Arc on the basis that Arc could not itself violate the Computer Fraud and Abuse Act, but could only be liable derivatively through Miller and Kelley's violation?

STATEMENT OF THE CASE

On October 27, 2010, Plaintiff WEC Carolina Energy Solutions, LLC ("WEC") filed its Complaint against Willie "Mike" Miller, Emily Kelley, and Arc Energy Services, Inc. The Complaint is in ten counts, including one count based upon the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, and nine state law claims. All of the Defendants moved to dismiss pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure on the ground that WEC had failed to state a claim upon which relief can be granted under the CFAA. On February 3, 2011, the district court dismissed the CFAA claim and declined to exercise supplemental jurisdiction over the state-law claims.[1] Later the same day, the district court entered an Amended Opinion and Order correcting the caption.

WEC filed a timely Notice of Appeal on March 4, 2011.

[1] WEC has filed a separate suit in state court in South Carolina with respect to the state law claims, and thus those claims are no longer part of this litigation. *See WEC Carolina Energy Solutions, LLC v. Miller, et al.*, 2011-CP-40-1518.

STATEMENT OF FACTS

Appellee Willie "Mike" Miller ("Miller") was employed as a Project Manager in Field Services at WEC, and Appellee Emily Kelley ("Kelley") was his assistant. J.A. 6.[2] WEC offers a full range of specialized welding and related services to the power generation industry. J.A. 5. Appellee Arc Energy Services, Inc. ("Arc") is a direct competitor of WEC. J.A. 5.

As a result of his employment with WEC, WEC issued Miller a company laptop computer and a company cell phone. J.A. 6. In his position, Miller had access to WEC's computers and servers, and consequently to numerous confidential and trade secret documents stored on these computers and servers. J.A. 6. This confidential and trade secret information included pricing, terms, pending projects, and information regarding WEC's technical capabilities. J.A. 6.

WEC takes substantial and reasonable measures to protect the confidential information and trade secret information contained on its computers and servers. J.A. 6. WEC has a clear policy prohibiting the use of any confidential information and trade secrets unless authorized by WEC. J.A. 7. WEC also forbids employees to download confidential and proprietary information to a personal computer. J.A. 10. Both Miller and Kelley were familiar with WEC's policies prohibiting the downloading of WEC's confidential information and trade secrets to a personal computer and the use of that information for any purpose other than for the benefit of WEC. J.A. 7.

[2] "J.A. ___" refers to the Joint Appendix.

Miller abruptly resigned his employment on April 30, 2010. J.A. 6. A review of records for Miller's WEC-issued cell phone showed that he had communicated with employees, principals and representatives of Arc for the purpose of competing with WEC and preparing to become employed with Arc. J.A. 7. Immediately before his resignation from WEC, Miller, either by himself or with Kelley's help, downloaded a substantial number of WEC's confidential documents and e-mailed the documents, unencrypted, to his personal e-mail address. J.A. 7. Miller and Kelley took these actions at Arc's direction. J.A. 9. Furthermore, ARC, through its principals, approved of, encouraged and benefitted from Miller's and Kelley's illicit actions. J.A. 8. The confidential information taken by Miller and Kelley included past and pending proposals by WEC to its customers, pricing information, and quotation worksheets. J.A. 7.

A mere 20 days after his resignation from WEC, Miller made a presentation to Dominion on behalf of Arc (his new employer) for welding work and other services at two power stations. J.A. 7-8. Miller used information and documents taken from WEC, including a proposal prepared by WEC for the Dominion projects, to prepare Arc's proposal to Dominion. J.A. 7-8. Arc was subsequently awarded both projects. J.A. 8.

SUMMARY OF ARGUMENT

This appeal presents a question of first impression in this circuit: What did Congress mean by the terms "without authorization" and "exceeds authorized access" in the CFAA? Relying on a Ninth Circuit decision, the district court held that if an employee has any authority to access information, no breach of duty nor improper use of the information can ever create liability under the CFAA. With respect, WEC suggests that this overly restrictive view of the CFAA all but eliminates the protections—civil and criminal—that the CFAA provides for employers against the actions of former employees who use confidential information to gain an unfair competitive advantage. The better view is expressed in the holdings of every other circuit court that has thus far confronted the issue, all of which have held that a violation of the CFAA may be premised upon an employee's breach of the common law duty of loyalty or violation of an employer's use policies. Moreover, the Ninth Circuit has itself recently clarified that CFAA liability is available for an employee's violation of policies governing the purposes for which information may be accessed. The majority rule is consistent with the plain language of the CFAA and with well-recognized principles of agency law, and it is the rule that this Court should adopt. Accordingly, the decision of the district court should be reversed and this case remanded for further proceedings on WEC's claim under the CFAA.

ARGUMENT

"The standard of review for dismissal pursuant to Rule 12(b)(6) is *de novo*." *Kendall v. Balcerzak*, ___ F.3d ___, 2011 WL 1108257, at *5 (4th Cir. March 28, 2011). The Court must consider the facts and all reasonable inferences in the light most favorable to WEC, the nonmovant, and it must review *de novo* all questions of law. *Id.*

This appeal turns on a question of statutory construction, "a quintessential question of law" subject to *de novo* review. *Broughman v. Carver*, 624 F.3d 670, 674 (4th Cir. 2010), *petition for cert. filed*, 79 U.S.L.W. 3594 (U.S. Apr. 11, 2011) (No. 10-12). Interpretation of a statute begins with the statutory text, the words of which must be given their plain and ordinary meaning "[a]bsent explicit legislative intent to the contrary." *Id.* at 674-75.

I. THE DISTRICT COURT ERRED IN DISMISSING THE CLAIM AGAINST MILLER AND KELLEY.

The CFAA provides in relevant part that a person is liable for a violation of the CFAA if he:

> (2) intentionally accesses a computer *without authorization* or *exceeds authorized access*, and thereby obtains–
>
> * * *
>
> (C) information from any protected computer;[3]
>
> * * *
>
> (4) knowingly and with intent to defraud, accesses a protected computer *without authorization*, or *exceeds authorized access*, and

[3] A "protected computer" is one "used in or affecting interstate or foreign commerce." 18 U.S.C. § 1030(e)(2)(B). There is no dispute that the materials accessed by Miller and Kelley were stored on a protected computer.

> by means of such conduct furthers the intended fraud and obtains anything of value ...;
>
> * * *
>
> (5) (B) intentionally accesses a protected computer *without authorization*, and as a result of such conduct, recklessly causes damage; or
>
> (C) intentionally accesses a protected computer *without authorization*, and as a result of such conduct, causes damage and loss.

18 U.S.C. § 1030(a) (emphasis added). Although enacted as a criminal statute, in 1994 Congress created a private cause of action for "[a]ny person who suffers damage or loss by reason of a violation of this section" when damages or losses meet or exceed $5,000 in one year. 18 U.S.C. § 1030(g).

WEC alleges that Miller and Kelley violated the CFAA when, at Arc's direction, they intentionally accessed WEC's computers and servers to download confidential and proprietary information, which Miller, Kelley, and Arc then used for Arc's benefit in competing with WEC. WEC maintains that because Miller and Kelley breached their duty of loyalty by acting on behalf of Arc, they were "without authorization" to download the information. Alternatively, WEC maintains that Miller and Kelley "exceeded authorized access" because they violated WEC's policies in downloading information to Miller's personal computer and in using that information to benefit Arc. Such actions fall squarely within the ambit of the CFAA.

The district court rejected both theories on the basis that "liability under the CFAA is based on access not use." J.A. 41. What the district court did not recognize—but the federal appellate courts have—is that an employee's right

of "access" to information is properly defined in terms of the purposes for which the employer allows access—in other words, the use of the information. Under these well-reasoned decisions, an employee acts "without authorization" or "exceeds authorized access" under the CFAA by acting disloyally or by violating the employer's policies governing computer usage, allegations which WEC has made in this case. J.A. 7-8. *See, e.g.*, *United States v. Nosal*, ___ F.3d ___, 2011 WL 1585600, at *6 (9th Cir. Apr. 28, 2011) ("[T]he *only* logical interpretation of 'exceeds authorized *access' is that the employer has placed* limitations on the employee's 'permission to use' the computer and the employee has violated—or 'exceeded'—those limitations." (emphasis in original)); *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010) (holding that employee exceeded authorized access when he violated employer policy by obtaining information for non-business purpose), *cert. denied*, ___ S. Ct. ___, 2011 WL 1100516 (Apr. 25, 2011); *United States v. John*, 597 F.3d 263, 272 (5th Cir. 2010) (holding that because "an employment agreement can establish the parameters of 'authorized' access," "the concept of 'exceeds authorized access' may include exceeding the purposes for which access is 'authorized'"); *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006) (Posner, J.) (holding that employee acted "without authorization" because his authorization "terminated when, having already engaged in misconduct and decided to quit … he resolved to destroy files … in violation of the duty of loyalty that agency law imposes on an employee"); *P.C. Yonkers, Inc. v. Celebrations The Party & Seasonal Superstore, LLC*, 428 F.3d 504, 510 (3d Cir. 2005)

(recognizing that the CFAA's reach extends to actions against "former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system"); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583 (1st Cir. 2001) (holding that former employees exceeded authorized access by violating a confidentiality agreement that prohibited the use of information "contrary to the best interests" of the plaintiff).

Rather than follow these well-supported precedents, the district court instead followed the one circuit court that interpreted the phrase "without authorization" as precluding consideration of the employee's intended purpose in accessing the information as a basis for liability. *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1131 (9th Cir. 2009). However, the Ninth Circuit has now significantly narrowed its holding in *Brekka*. *See United States v. Nosal*, ___ F.3d ___, 2011 WL 1585600 (9th Cir. Apr. 28, 2011). WEC respectfully suggests that the district court's interpretation of the CFAA is too narrow and that its decision should be reversed.

A. An employee acts "without authorization" under the CFAA by accessing information in violation of a duty of loyalty.

Employees are a type of agent and are thus subject to the general agency rules regarding the nature and extent of their authority. In that regard, the *Restatement (Second) of Agency* states that "[a]n agent is authorized to do, *and to do only*, what is reasonable for him to infer that the principal desires him to do." *Restatement (Second) of Agency* § 33. The *Restatement* also makes clear that

"authority to act as agent includes only authority to act *for the benefit of the principal*." *Restatement (Second) of Agency* § 39 (emphasis added).

> In business enterprises, an agent normally has no authority *to seek personal advantage* otherwise than through the faithful performance of these duties, *nor to conduct his principal's business with a mind to the benefit of others*.

Id. cmt. a. (emphasis added). Of course, that is exactly what Miller and Kelley did here: In downloading WEC's confidential information, they sought to advantage themselves and to benefit Arc. This case, therefore, is not simply about "use" of the information. It is about whether Miller and Kelley lost their authorization to access WEC's information by violating their duties as agents of WEC.

As agents of WEC, both Miller and Kelley owed certain duties to WEC, including a duty of loyalty with respect to matters within the scope of their employment. By agreeing to act on behalf of a third party and competitor, ARC, they breached their duty of loyalty to WEC and lost any authorization to access information on WEC's computers or otherwise:

> Unless otherwise agreed, the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal.

Restatement (Second) of Agency § 112.[4] The termination of authority is immediate and automatic, as the illustration makes clear:

---

[4] Albeit in a different context, Justice Scalia recently discussed the implications of § 112 on the authority of an agent. In *Holland v. Florida*, 130 S. Ct. 2549 (2010), the Supreme Court held that a death row inmate was entitled

> 1. P employs A, a traveling salesman, to sell goods and receive the price. At the beginning of his trip A embezzles a portion of the amounts received and intends to continue to do so. A is not authorized to continue to sell.

Id. § 112 cmt. b, illus. 1. Here, WEC authorized Miller and Kelley to access certain information for WEC's benefit. Arc directed Miller and Kelley to download the confidential information for *Arc's* benefit. Once they agreed to do so, they were acting adverse to their principal, WEC, and lost their authorization to access WEC's information.

Applying these principles, in *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), the Seventh Circuit held that an employee's authorization to access his employer's computer terminates when the employee uses the computer contrary to the employer's interests, thereby breaching his duty of loyalty to his employer. The employee had decided to start his own competing business and erased all data from his work computer which included confidential information of his employer that showed that he had engaged in misconduct while employed. The court held that when the employee breached his duty of loyalty to his employer, his agency relationship terminated "and with it his authority to access the laptop, because the only basis of his authority

---

to equitable tolling of the limitations period for a federal habeas corpus petition because his attorney had failed to respond to his repeated inquiries regarding the status the case. Justice Scalia dissented, arguing that the circumstances did not justify a departure from the usual rule that "[b]ecause the attorney is the litigant's agent, the attorney's acts (or failures to act) within the scope of representation are treated as those of his client." *Id.* at 2571 (Scalia, J., dissenting). Citing § 112, Justice Scalia explicitly distinguished the situation of an attorney's "conduct amounting to disloyalty or renunciation of his role, which *would* terminate his authority." *Id.* at 2573 n.9 (emphasis in original).

had been that relationship." *Id.* at 420-21. Because of that breach of loyalty, the Seventh Circuit held that the employee's actions in deleting or erasing the information were "without authorization" for purposes of § 1030(a)(5).

The one circuit court case relied upon by the Court below,[5] *LVRC Holdings, LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), rejected the approach in *Citrin*, apparently because the court viewed the CFAA through the lens of a criminal statute.[6] *Id.* at 1134-35. The Ninth Circuit determined that "nothing in the CFAA suggests that a defendant's liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer." *Id.* at 1135. What *Brekka* fails to recognize, however, is that a statute must be understood in light of the existing law at the time of its adoption. *Palisades Collections LLC v. Shorts*, 552 F.3d 327, 335 (4th Cir. 2008) (holding that Congress is presumed to legislate "consistently with existing law"). The common law principles of agency discussed above were well-established when Congress enacted § 1030(g), and thus those principles must inform the Court's understanding of the term "without authorization." Otherwise, much of the protection of the CFAA—criminal and civil—is lost.

[5] The other cases relied upon by the Court below are District Court cases, including one of the Court's own prior decisions. J.A. 44 (citing *Sloan Fin. Grp., LLC v. Coe*, 2010 WL 4668341 (D.S.C. Nov. 18, 2010)).

[6] The District Court in this case uses the same rationale for its narrow reading of the statute. J.A. 45.

Accordingly, the district court erred in holding that the term "without authorization" under the CFAA does not encompass an employee's loss of authority through an act of disloyalty to his employer.

B. By violating WEC's policies regarding use of confidential information, Miller and Kelley exceeded their authorization.

The district court also erred in holding that an employee "exceeds authorized access" under the CFAA only by "access[ing] information he was not entitled to access." J.A. 44. This was the holding of the Ninth Circuit in *Brekka*. *See Brekka*, 581 F.3d at 1133 (holding that "a person who 'exceeds authorized access' … has permission to access the computer, but accesses information on the computer that the person is not entitled to access"). Since the district court issued its order in this case, however, the Ninth Circuit has abrogated this portion of *Brekka*'s reasoning, holding that an employee "exceeds authorized access" by violating his employer's access restrictions, including restrictions placed upon the use of information. *See United States v. Nosal*, ___ F.3d ___, 2011 WL 1585600, at *6-7 (9th Cir. Apr. 28, 2011). In so holding, the Ninth Circuit joined every other circuit court of appeals that has addressed the issue. WEC respectfully urges this Court to adopt the now-unanimous rule of the circuits that an employee "exceeds authorized access" by downloading or using information in violation of his employer's policies.

The CFAA defines "exceeds authorized access" as "to access a computer with authorization and to use 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). As one court has noted, the line between "without authorization" and "exceeding authorized access" is "paper thin." *Citrin,* 440 F.3d at 420. However, there must be a difference, or Congress would have limited the CFAA only to accessing a computer without authorization. *See Barnes v. Holder*, 625 F.3d 801, 806 (4th Cir. 2010) (stating that the rules of statutory construction require the court to "give meaning to all statutory provisions").

While the CFAA defines the phrase "exceeds authorized access," it does not define the term "authorization." *See John*, 597 F.3d at 271. The word "authorization" must be given its plain and ordinary meaning. *See Broughman*, 624 F.3d at 674. Dictionary.com defines "authorization" as "permission or power granted by an authority" and "authority" as "a power or right delegated or given; authorization." Thus, both phrases connote that "authority" is a right granted by another—in this case, by WEC—who defines the extent of the right conferred. *See Restatement (Second) of Agency* § 33, cmt. a ("The implicit, basic understanding of the parties to the agency relation is that the agent is to act only in accordance with the principal's desires as manifested to him."). The purpose for which access is authorized is an inseparable component of the authorization itself, such that an employee "exceeds authorized access" by accessing information for any purpose other than those permitted by the employer. As the Ninth Circuit explained in *Nosal*, in providing that by using his access "to obtain or alter information … that the accesser is not entitled *so* to obtain or alter," the CFAA allows for liability based upon an employer's restrictions on use of information:

> "So" in this context means "in a manner or way that is indicated or suggested." *Webster's Third New Int'l Dictionary* 2159 (Philip Babcock Gove, ed. 2002). Thus, an employee exceeds authorized access … when the employee uses that authorized access "to obtain or alter information in the computer that the accesser is not entitled [in that manner] to obtain or alter."

Nosal, at *4. An employer who places restrictions on the use of information—for example, by prohibiting downloading information to a personal computer—has restricted the manner in which an employee may access information. Thus, any employee who violates those restrictions has exceeded his authorization. *Id.* at *6.

In so holding, the Ninth Circuit joined the unanimous holdings of the First, Third, Fifth, and Eleventh Circuits. Under this line of cases, company-created rules governing computer usage define the limits of an employee's permissible access, and if those rules are violated, the employee has "exceed[ed] authorized access" under the CFAA.

The Fifth Circuit adopted this precise theory *United States v. John*, 597 F.3d 263 (5th Cir. 2010). Defendant John was charged with exceeding authorized access to the computer system of her employer, Citigroup, in order to obtain confidential customer account information in violation of the CFAA. *Id.* at 269-70. In her defense, John argued that because "she was authorized to use Citigroup's computers and to view and print information regarding accounts in the course of her official duties," she did not violate the CFAA. *Id.* at 271. John further argued—as Appellees did below—that "the statute does

not prohibit unlawful *use* of material that she was authorized to access through authorized use of a computer." *Id.*

The Fifth Circuit flatly rejected these arguments, holding that "the concept of 'exceeds authorized access' may include exceeding the purposes for which access is 'authorized.'" *Id.* at 272. John "was not authorized to access that information for any and all purposes but for limited purposes."

> Citigroup's official policy, which was reiterated in training programs that John attended, prohibited misuse of the company's internal computer systems and confidential customer information. Despite being aware of these policies, John accessed account information for individuals whose accounts she did not manage, removed this highly sensitive and confidential information from Citigroup's premises, and ultimately used this information to perpetrate fraud on Citigroup and its customers.

Id.

The Fifth Circuit in *John* relied on the First Circuit's opinion in *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001). In that case, several of the plaintiff's former employees used their knowledge of codes obtained while working for the plaintiff to develop a computer program that mined the plaintiff's public website for pricing information, which the defendants then used to undercut the plaintiff's prices. *Id.* at 579-80. While employed by the plaintiff, however, the defendants "voluntarily entered a broad confidentiality agreement prohibiting … disclosure of any information which might reasonably be construed to be contrary to the interests of [the plaintiff]." *Id.* at 583. The First Circuit held that the defendants "exceeded authorized access" by using the plaintiff's information to compete against it. *Id.* at 583-84.

The Eleventh Circuit reached the same conclusion in *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010). Rodriguez, an employee of the Social Security Administration, accessed the personal information of 17 individuals. Relying on *Brekka*, Rodriquez's defense was premised on the fact that he had authority to access that information. The Eleventh Circuit rejected Rodriguez's argument because "the policy of the Administration is that use of databases to obtain personal information is authorized only when done for business reasons." *Id.* at 1263. The court distinguished *Brekka* on the basis that Brekka's employer "had no policy prohibiting employees from emailing company documents to personal email accounts," while in contrast "the Administration told Rodriguez that he was not authorized to obtain personal information for nonbusiness reasons." *Id.* at 1263.

The Third Circuit has reached the same conclusion, holding in *P.C. Yonkers, Inc. v. Celebrations The Party & Seasonal Superstore, LLC*, 428 F.3d 504, 510 (3d Cir. 2005), that the CFAA applies to "former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system."

The reasoning of these decisions is consistent with congressional intent, as revealed in the Senate report accompanying the 1996 amendments to the CFAA, which recognized that

> The seriousness of a breach in confidentiality depends, in considerable part, on the value of the information taken, *or on what is planned for the information after it is obtained.*

S. Rep. No. 104-357, at 8 (1996) (emphasis added). From this language it is apparent that the Senate intended to give a broad interpretation to the statute which would encompass the improper use of the information obtained as well as improper access. This makes sense. Any other interpretation simply would encourage theft of an employer's secrets.[7]

Here, WEC's Complaint alleges that Miller and Kelley's action were "in direct violation of WEC's clear policy prohibiting the use of any confidential information or trade secret unless authorized by WEC, which policy was known by Miller and Kelley." J.A. 7. Thus, as the above-cited caselaw indicates, the pleading alleges "enough facts to state a claim to relief that is plausible on its face." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 547 (2007).

II. THE DISTRICT COURT ERRED IN DISMISSING THE CLAIM AGAINST ARC.

The district court dismissed the claim against Arc on the basis that it was dependent upon the claims against Miller and Kelley. J.A. 43. However, Arc may be held directly liable for its own conduct in violation of the CFAA. The

[7] While not within the employment context, at least two district courts within the Fourth Circuit have found that a "terms of use" policy can establish the boundaries of authorized access under the CFAA. *See Bus. Info. Sys. v. Prof'l Gov'tl Research & Solutions Inc.*, 2003 WL 23960534, at *7-8 (W.D. Va. Dec. 16, 2003) (finding the defendant did not violate the CFAA, but noting that "if [the plaintiff] wanted to restrict its users in their abilities to make unfettered use of the records they were accessing, then it could have done so easily through its terms and conditions of usage"); *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 450 (E.D. Va. 1998) (granting summary judgment to the plaintiff based on allegation that the defendant sent spam bulk email through the plaintiff's server in violation of the plaintiff's terms of service).

Complaint alleges that Arc directed Miller and Kelley to access WEC's computers and servers and to obtain the confidential information for its benefit. J.A. 9. The Complaint also alleges that Arc aided and abetted Miller and Kelley in the violation of their breaches of loyalty. J.A. 9-10. "One who orders an act to be done is liable for the consequences as he would be for his own personal conduct if he knew or should have known of the conditions under which it is to be done." *Restatement (Second) of Torts* § 877, cmt. a. *Accord* 18 U.S.C. § 2(a) ("Whoever … aids, abets, counsels, commands, induces or procures [the] commission [of an offense] is punishable as a principal."); *United States v. Lee*, 602 F.3d 974, 976 (9th Cir. 2010) ("[A] principal is guilty of an offense if she used [another] to cause an act to be done which, if performed by the principal, would be unlawful."). It is no different than if a bank robber directs a bank employee to embezzle money from the bank and give it to the robber. Simply put, Arc may be held liable for its own conduct.

CONCLUSION

The overwhelming body of case law requires the reversal of the district court's decision dismissing WEC's CFAA claim. WEC's allegations against Miller, Kelley, and Arc state a legally cognizable claim that all three acted "without authorization" or "exceeded authorized access" within the meaning of the CFAA. WEC asks this Court to reverse the decision below and to remand for further proceedings.

STATEMENT REGARDING ORAL ARGUMENT

This appeal presents questions of first impression for this Court, one of which (the meaning of "without access") has divided the circuits. WEC requests oral argument on the basis that argument is necessary for adequate consideration of the issues.

Respectfully submitted,

s/ Kirsten E. Small
Angus H. Macaulay, Esq.
Kirsten Small, Esq.
NEXSEN PRUET, LLC
P.O. Drawer 10648
Greenville, SC 29603
Ksmall@nexsenpruet.com
Tel: 864-377-2211
Fax: 864-282-1177

and

s/ Anthony J. Basinski
Mark Gordon, Esq.
Anthony J. Basinski, Esq.
PIETRAGALLO GORDON ALFANO BOSICK & RASPANTI, LLP
One Oxford Centre, 38th Floor
Pittsburgh, PA 15219
MG@Pietragallo.com
AJB@Pietragallo.com
Tel: 412-263-2000
Fax: 412-263-2001

Attorneys for Appellant WEC Carolina Energy Solutions, LLC

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 11-1201 **WEC Carolina Energy Solutions, LLC v. Willie "Mike" Miller, Emily Kelley and ARC Energy Services, Inc.**

CERTIFICATE OF COMPLIANCE WITH RULE 28.1(e) or 32(a)

1. This brief complies with the type-volume limitation of Fed. R. App. P. 28.1(e)(2) or 32(a)(7)(B) because:

   X this brief contains **4,855** words, excluding the parts of the brief exempted by Fed R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because:

   X this brief has been prepared using Microsoft Word 2003, with a proportionally spaced typeface, Garamond 14 point.

s/ Kirsten E. Small
Kirsten Small, Esq.
Nexsen Pruet, LLC
P.O. Drawer 10648
Greenville, SC 29603
Ksmall@nexsenpruet.com
Tel: 864-370-2211
Fax: 864-282-1177

Counsel for Appellant

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the within **Appellant's Brief** was electronically filed with the Court using the ECF system, which sent notification of such filing to all counsel of record, including the following:

Brian S. McCoy, Esq. HORACK TALLEY 633 East Main Street Rock Hill, SC 29730 BMcCoy@horacktalley.com Tel. 803-366-2280 Fax 803-366-0643 *Attorney for Willie "Mike" Miller and Emily Kelley*	James W. Bradford, Jr. JIM BRADFORD LAW FIRM, LLC P.O. Box 1347 York, SC 29745 Jim@BradfordLawyers.com Tel. 803-684-6965 Fax 803-684-7289 *Attorney for Arc Energy Services, Inc.*

May 2, 2011

s/ Kirsten E. Small

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Only one form needs to be completed for a party even if the party is represented by more than one attorney. Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case. Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements. Counsel has a continuing duty to update this information.

No. 11-1201 Caption: WEC Carolina Energy Solutions, LLC v. Willie Miller, et al.

Pursuant to FRAP 26.1 and Local Rule 26.1,

WEC Carolina Energy (name of party/amicus) who is Appellant (appellant/appellee/amicus), makes the following disclosure:

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☐ NO
2. Does party/amicus have any parent corporations? ☐ YES ☐ NO
   If yes, identify all parent corporations, including grandparent and great-grandparent corporations:
   Westinghouse Electric Company, LLC (parent); Toshiba Corp. (grandparent)
3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☐ NO
   If yes, identify all such owners:
4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(b))? ☐ YES ☐ NO
   If yes, identify entity and nature of interest:
5. Is party a trade association? (amici curiae do not complete this question) ☐ YES ☐ NO
   If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:
6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☐ NO
   If yes, identify any trustee and the members of any creditors' committee:

CERTIFICATE OF SERVICE

****

I certify that on March 18, 2011 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

Brian McCoy
Horack Talley
633 East Main Street
Rock Hill, SC 29730

James W. Bradford, Jr.
Jim Bradford Law Firm, LLC
P.O. Box 1347
York, SC 29745

s/ Kirsten E. Small (signature) March 18, 2011 (date)

Reset Form