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

REPLY 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
1230 Main Street, St. 700
Columbia, SC 29201
(803) 253-8279

Counsel for Appellant
WEC Carolina Energy Solutions, LLC

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

ARGUMENT

I. THE DISTRICT COURT ERRED IN DISMISSING THE COMPLAINT AS TO MILLER AND KELLEY.

A. The CFAA applies to an employee who "exceeds authorized access" by obtaining information for a purpose that violates the employer's use restrictions.

WEC authorized Miller and Kelley to access its computer systems in furtherance of WEC's business. WEC prohibited the use of confidential information or trade secrets unless authorized by WEC, and Miller and Kelley knew that their access to WEC's information was so limited. J.A. 7. Miller and Kelley's authority to access WEC's computers thus was defined by the restrictions WEC placed on the use of its information. Miller and Kelley exceeded authorized access, and thereby violated the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(a)(2), (a)(4), by obtaining WEC's information and using it for purposes not authorized by WEC. Every Circuit Court of Appeals to review this issue agrees with this reasoning.

Most recently, in *United States v. Nosal*, 642 F.3d 781 (9th Cir. 2011), the Ninth Circuit revisited and substantially clarified its prior decision in *LVRC Holdings, LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009). In granting Appellees' motions to dismiss, the district court below interpreted *Brekka* as barring CFAA claims that allege the prohibited use of information obtained by an employee who was authorized to access the information. Appellees echo the district court's reasoning on appeal. As *Nosal* makes clear, their continued reliance on *Brekka* is misplaced.

In *Brekka*, the Ninth Circuit held that "an individual who is authorized to use a computer *for certain purposes but goes beyond those limitations* is considered by the CFAA as someone who has 'exceed[ed] authorized access.'" *Brekka*, 581 F.3d at 1133 (emphasis added; alteration in original). Applying this language, *Nosal* held that under *Brekka* "an employee exceeds authorized access when he or she obtains information from the computer and uses it for a purpose that violates the restrictions on the use of the information." *Nosal*, 642 F.3d at 782. Brekka could not be liable under the CFAA because his employer—unlike WEC and unlike Korn/Ferry in *Nosal*—had imposed no use restrictions. "Therefore, Brekka did not exceed his authorized access any more than he acted without authorization: he was entitled to obtain the information because he had not acted in a way that violated any access restrictions." *Id.* at 787.

Appellees claim to be puzzled by WEC's reading of *Nosal*, which they maintain has nothing to do with "post-access restrictions on the use of confidential information." Appellees' Br. at 13 (emphasis omitted). Of course it doesn't, and that is why *Nosal* supports WEC's position. In *Nosal*, the employer "restricted the use and disclosure" of its confidential information "except for legitimate Korn/Ferry business." *Nosal*, 642 F.3d at 783 (emphasis omitted); *cf.* J.A. 7 (alleging that WEC had a "clear policy prohibiting the use of any confidential information or trade secrets unless authorized by WEC"). Nosal recruited Korn/Ferry employees to use their Korn/Ferry usernames and passwords to download and transfer Korn/Ferry's confidential information to Nosal so he could start a competing business. *Nosal*, 642 F.3d at 783; *cf.* J.A. 7

(alleging that Miller and Kelley downloaded confidential information and transferred it to Arc in order to enable Arc to compete unfairly with WEC). The Ninth Circuit held that "an employer's use restrictions define whether an employee 'exceeds authorized access.'" *Nosal*, 642 F.3d at 787. Appellees thus are correct that *Nosal* did not involve "post-access" use restrictions. Rather, *Nosal* held that use restrictions *define authorized access*: A restriction on an employee's *use* of information is, by definition, a restriction on the employee's *authority to access* that information. Just like Miller and Kelley, the employees in *Nosal* "exceed[ed] authorized access" by accessing information for purposes not permitted by Korn/Ferry.[1]

The court in *Nosal* rested its decision on the plain meaning of the statutory definition of "exceeds authorized access": "to access a computer with authorization and to use such access to obtain or alter information … that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). Appellees criticize the *Nosal* court for spending "a lot of intellectual effort" interpreting the meaning of the adverb "so." Appellees' Br. at 11. But this effort was required by

[1] *See also, e.g.*, *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010) (affirming criminal conviction because Rodriguez "exceeded authorized access" when he accessed information for personal reasons, thus violating Administration policy authorizing access to information only for business purposes), *cert. denied*, 131 S. Ct. 2166 (2011); *United States v. John*, 597 F.3d 263, 271-72 (5th Cir. 2010) (holding that "'authorized access' or 'authorization' may encompass limits placed on *the use* of information obtained by permitted access to a computer system and data available on that system" and affirming John's conviction because, although she was authorized to view and print all of the information that she accessed, her "use of Citigroup's computer system to perpetrate fraud was not an intended use of that system." (emphasis added)).

"one of the most basic interpretive canons, that a statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant." *Corley v. United States*, 556 U.S. 303, 129 S. Ct. 1558, 1566 (2009) (internal quotation marks & alterations omitted). This canon does not cease to apply simply because the statutory term in question is short.

Moreover, *Nosal*'s construction of the phrase "so to obtain or alter" is supported by the legislative history. In the 1986 revision of the CFAA, Congress

> substitute[d] the phrase 'exceeds authorized access' for the more cumbersome phrase in present 18 U.S.C. 1030(a)(1) and (a)(2), 'or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend.' The Committee intends this change to simplify the language in 18 U.S.C. 1030(a)(1) and (2), and the phrase 'exceeds authorized access' is defined separately in Section (2)(g) of the bill.

S. Rep. No. 99-432 at 8 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2486. Far from indicating an intent to narrow the reach of the CFAA, the Committee report shows a clear intent to maintain the prior scope of the statute while using simpler language. A "substitute" is a replacement, not a limitation. *See Webster's New College Dict.* 1100 (1995) (defining "substitute" as "[a] word or construction used *in place of* another word or construction" (emphasis added)). To simplify a cumbersome phrase is to state it more plainly, not to change its meaning.[2]

[2] The views expressed by Senators Mathias and Leahy, S. Rep. No. 99-432 at 14-17, 1986 U.S.C.C.A.N. at 2493-96, on which Appellees rely, are not to the contrary. The Senators' discussion is concerned with only with the elimination of potential criminal liability for government employees under subsection (a)(3)—not with the definition of "exceeds authorized access." *See id.* (discussing problem posed by former subsection (a)(3), which created the potential that a

In conclusion, an employer is either entitled to set the terms of employee computer access, or it is not. Appellees' construction of the CFAA would artificially and unnecessarily truncate that entitlement. Appellees concede, as they must, that a person may be held liable under the CFAA for violating employer-imposed limitations on computer access. But Appellees would have this Court hold that *certain kinds* of employer-imposed access restrictions are entitled to CFAA protection, but other kinds are not. This distinction is not justified by the statutory language or by common sense, and it has been unanimously rejected by the federal courts of appeals to which it has been argued.

B. Miller and Kelley accessed WEC's computer system "without authorization" under the CFAA.

Having decided to go to work for Arc, but at the same time employed by WEC, Miller and Kelley downloaded confidential information belonging to WEC for the purpose of benefitting Arc. By deciding to act for the benefit of Arc and to harm WEC, Miller and Kelley lost any authorization they might have had to access WEC's computer systems. *See* Restatement (Second) of Agency § 112 ("[T]he authority of an agent terminates if, without knowledge of the principal, [the agent] acquires adverse interests or … is otherwise guilty of a serious breach of loyalty to the principal."); *Int'l Airport Ctrs. L.L.C. v. Citrin*, 440

government employee could be threatened with criminal liability for complying with the Freedom of Information Act, in turn creating the danger that the CFAA "could be misused to weaken the Freedom of Information Act, or to impose unnecessary obstacles to the public's right to know about government activities").

F.3d 418, 420 (7th Cir. 2006). Appellees' challenges to this argument are unpersuasive.

Appellees first argue that it is somehow improper to employ common law principles, as articulated in the Restatement (Second) of Agency, to interpret the CFAA. But it is entirely proper to refer to the common law to understand statutory terms. *See Kolstad v. Am. Dental Ass'n*, 527 U.S. 526, 542 (1999) ("[O]ur interpretation of Title VII is informed by the general common law of agency …. The common law is as codified in the Restatement (Second) of Agency (1957) provides a useful starting point for defining this general common law."); *Faragher v. City of Boca Raton*, 524 U.S. 775, 801-02 (1998) (considering Restatement (Second) of Agency § 219 in the course of determining scope of an employer's vicarious liability under Title VII). "Indeed, whenever a federal statute uses the term employee" without providing a specific definition, courts "must presume that Congress intended to incorporate traditional principles of agency law." *Carter v. Anderson (In re Carter)*, 182 F.3d 1027, 1030 (9th Cir. 1999).

Indeed, Restatement § 112 has been used to interpret a *criminal* statute. In *United States v. Hill*, 579 F.2d 480 (8th Cir. 1978), the defendant argued that he could not be convicted of mail theft, 18 U.S.C. § 1702, because he was authorized to receive his mother's social security check and only later decided to cash the check for his own use. Relying on § 112, the Eighth Circuit agreed and noted that "if Carl Hill had intended to convert the check at the time he removed the mail from the porch, his agency would have terminated and he would be subject to § 1702." *Hill*, 579 F.2d at 482; *see United States v. Galindo*, 871

F.2d 99, 101 (9th Cir. 1989). Here, Miller and Kelley were authorized to access WEC's confidential information until they decided to act on behalf of Arc, at which point their authority ceased. Their subsequent conduct in accessing and downloading WEC's information was "without authorization" and therefore violated the CFAA.[3]

Appellees next contend that applying agency principles to "without access" erodes the distinction between access that is "without authorization" and access that "exceeds authorized access." The point seems to be that an employee who violates access restrictions has necessarily acted disloyally and thus lost authorization, such that no role is left for exceeding authorization. Appellees are wrong. Appellees were "without authorization" because they acted on behalf of Arc. Separate and apart from this, Appellees "exceeded authorized access" by violating WEC's express restrictions on access. In other words, Miller and Kelley would have "exceeded authorized access" by downloading confidential information in violation of known WEC policy even if Arc had not directed them to do so.

[3] In *Brekka*, the Ninth Circuit expressed concern that under *Citrin* an employee might unknowingly violate the CFAA. *See Brekka*, 581 F.3d at 1135. This concern is unfounded. It is axiomatic that an agent cannot unknowingly decide to transfer his loyalty to a new principal. Moreover, the CFAA applies only to *intentional* conduct. *See* S. Rep. No. 99-432 at 5, 1986 U.S.C.C.A.N. at 2483 ("[I]ntentional acts of unauthorized access—rather than mistaken, inadvertent, or careless ones—are precisely what the Committee intends to proscribe.").

C. Appellees' attempts to avoid the plain meaning of the statutory language must fail.

1. *The CFAA applies to employees.*

Appellees repeatedly assert that the CFAA's only purpose is to deter and punish "computer hackers." The statutory language, however, makes clear that Congress was just as concerned with theft and damage caused by employees as it was with the activities of outside computer hackers. The CFAA provides for civil and criminal liability for persons who are "without authorization" to access a computer system and also for persons who "exceed [their] authorization." If Congress were concerned only with computer hackers—those who break into a computer system from outside—the CFAA would apply only to persons acting "without authorization." But the Act plainly sweeps more broadly, covering insiders who are authorized to use a computer system—such as employees—but who exceed the bounds of that access. The CFAA thus plainly contemplates that an employee may be held liable (criminally or civilly) for violating the Act.

2. *Because the meaning of the statutory language can be determined with ordinary rules of statutory construction, the rule of lenity does not apply.*

Appellees maintain that this Court's construction of the CFAA must be guided at all times by the "rule of lenity," and they further maintain that the rule of lenity requires this Court to adopt the narrowest possible construction of the CFAA. Appellees misunderstand the purpose of the rule of lenity and the manner of its application.

The rule of lenity is not a guiding principle of statutory construction; it is a tie-breaker of last resort. As Justice Sotomayor recently explained for a unanimous Supreme Court, "The rule … is reserved for cases where, after seizing everything from which aid can be derived, the Court is left with an ambiguous statute." *DePierre v. United States*, 131 S. Ct. 2225, 2237 (2011) (internal quotation marks omitted). If "traditional tools of statutory construction … suffice to resolve the interpretive issues," there is "no occasion for resort to the rule of lenity." *United States v. Gosselin World Wide Moving, N.V.*, 411 F.3d 502, 514 (4th Cir. 2005). Even if there were some ambiguity in the CFAA, its status as a criminal statute does not require this Court to adopt the narrowest possible construction of its terms. "The canon in favor of strict construction (of criminal statutes) is not an inexorable command to override common sense and evident statutory purpose…. Nor does it demand that a statute be given the narrowest meaning." *United States v. Moore*, 423 U.S. 122, 145 (1975) (internal quotation marks omitted).

3. The CFAA is not void for vagueness, nor does it pose a trap for the unwary.

The CFAA is not void for vagueness. "A conviction fails to comport with due process if the statute under which it is obtained fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement." *United States v. Williams*, 553 U.S. 285, 304 (2008). The court must "consider whether a statute is vague as applied to the particular facts at issue, for '[a] plaintiff who engages in some conduct that is clearly proscribed cannot complain of the vagueness of the law as applied to the conduct of others.'" *Holder v. Humanitarian Law Project*, 130

S. Ct. 2705, 2718-19 (2010) (quoting *Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 495 (1982)). The "sky is falling" hypotheticals offered by Appellees are thus irrelevant; the only question is whether Appellees had sufficient warning that their own conduct was proscribed. As explained above, the plain statutory text gave Appellees ample warning that their conduct was prohibited.

Appellees are also wrong when they assert that applying the CFAA to their conduct "makes most breaches of contract involving a computer a [sic] criminal offense." Appellees' Br. at 18. Liability under the CFAA is available only for intentional theft of data, 18 U.S.C. § 1030(a)(2), or for knowing conduct accompanied by an intent to defraud, 18 U.S.C. § 1030(a)(4). It is also clear that the CFAA does not apply to employees who access Facebook during work hours. *See* S. Rep. No. 99-432, at 9-10 (explaining that the CFAA does not apply when "the thing obtained consists only of the use of the computer" except when, under subsection (a)(5), an outsider deprives the computer owner of use of the system (internal quotation marks omitted)).

II. UNDER THE RULE OF CORPORATE CRIMINAL LIABILITY, ARC MAY BE HELD DIRECTLY LIABLE FOR VIOLATING THE CFAA.

Arc maintains that it cannot be held liable for a violation of the CFAA because it did not *itself* access WEC's computers and because the CFAA does not explicitly provide for aider-and-abettor liability.[4] Arc's argument overlooks

[4] Arc also contends that "[t]here is no federal tort common law involved in this case—only a statutorily imposed liability." Appellees' Br. at 21. But in construing

the established principle that "a [corporation] is liable for the criminal acts of its employees and agents acting within the scope of their employment for the benefit of the corporation." *United States v. Singh*, 518 F.3d 236, 250 (4th Cir. 2008) (internal quotation marks & alteration omitted). "Since a corporation acts by its officers and agents, their purposes, motives, and intent are just as much those of the corporation as are the things done…. There is no more difficulty in imputing to a corporation a specific intent in criminal proceedings than in civil." *N.Y. Cent. & Hudson River R.R. Co. v. United States*, 212 U.S. 481, 492-93 (1909) (internal quotation marks omitted). In *Singh*, for example, this Court affirmed the conviction of a corporation for violating the Mann Act. *See Singh*, 518 F.3d at 249-51.

The rule of corporate criminal liability "prevents corporations from avoiding liability by simply contracting-out the more risky elements of their business." *Id.* at 251 n.20 (internal quotation marks & alteration omitted). Miller and Kelley acted as Arc's agents when they downloaded WEC's confidential information, and they were motivated by a desire to benefit Arc. On the facts alleged, therefore, Arc may be held liable for violating the CFAA.

CONCLUSION

The Circuit Courts of Appeal have overwhelmingly concluded that by its plain terms the CFAA applies to employees who act adversely to their

a federal statutory liability, the court must "start from the premise that when Congress creates a federal tort it adopts the background of general tort law." *Staub v. Proctor Hosp.*, 131 S. Ct. 1186, 1191 (2011).

employers' interests or who violate employer-imposed restrictions on the use of confidential information. WEC has pleaded facts that support both claims in this case. Accordingly, WEC respectfully requests this Court to reverse the judgment of the district court and remand for further proceedings.

Respectfully submitted,

s/ Kirsten E. Small
Angus H. Macaulay, Esq.
Kirsten Small, Esq.
Nexsen Pruet, LLC
1230 Main Street, Suite 700
Columbia, SC 29201
Ksmall@nexsenpruet.com
Tel: 803-253-8279
Fax: 803-727-1465

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

July 22, 2011

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. _______ Caption: ____

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

Certificate of Compliance With Type-Volume Limitation,
Typeface Requirements, and Type Style Requirements

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

[Appellant's Opening Brief, Appellee's Response Brief, and Appellant's Response/Reply Brief may not exceed 14,000 words or 1,300 lines; Appellee's Opening/Response Brief may not exceed 16,500 words or 1,500 lines; any Reply or Amicus Brief may not exceed 7,000 words or 650 lines; line count may be used only with monospaced type]

[ ] this brief contains ________________ [*state the number of*] words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii), *or*

[ ] this brief uses a monospaced typeface and contains ________________ [*state the number of*] lines of text, 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:

[14-point font must be used with proportional typeface, such as Times New Roman or CG Times; 12-point font must be used with monospaced typeface, such as Courier or Courier New]

[ ] this brief has been prepared in a proportionally spaced typeface using
_____________________ [*state name and version of word processing program*] in
______________________________ [*state font size and name of the type style*]; *or*

[ ] this brief has been prepared in a monospaced typeface using
_____________________ [*state name and version of word processing program*]
with _______________________ [*state number of characters per inch and name of type style*].

(s)____

Attorney for_________________________________

Dated:___________________

CERTIFICATE OF SERVICE

I certify that on _________________ 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:

______________________________ ______________________________

Signature Date