UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

LOCKHEED MARTIN CORPORATION,
a Maryland corporation,

Plaintiff,

v. Case No. 6:05-CV-1580-ORL-31-KRS

KEVIN SPEED, STEVE FLEMING, and
PATRICK ST. ROMAIN,

Defendants.
_____/

DEFENDANTS KEVIN SPEED AND STEVE FLEMING'S MOTION TO DISMISS COUNTS I, II, AND III OF PLAINTIFF'S AMENDED COMPLAINT AND INCORPORATED MEMORANDUM OF LAW

Defendants Kevin Speed ("Speed") and Steve Fleming ("Fleming"), by and through undersigned counsel and pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure, hereby move to dismiss Counts I, II, and III of Plaintiff's Amended Complaint for the reasons and upon the grounds set forth in the following memorandum of law.

I. INTRODUCTION

Defendants Speed and Fleming are former employees of Plaintiff, Lockheed Martin Corporation ("Lockheed"). Speed and Fleming, who have never been subject to any non-competition agreement, are now employees of L-3 Communications, Inc. ("L-3"), a competitor of Lockheed. In its 54-page Amended Complaint, Lockheed accuses Speed and Fleming of having misappropriated confidential information from Lockheed for the benefit of L-3. Lockheed fashions these allegations, which will be

proven false in the course of this litigation, into some 13 separate counts, including breach of fiduciary duty and violation of the Florida Uniform Trade Secrets Act. Not content with the ten state law claims, Lockheed has also purported to bring three claims under the Computer Fraud and Abuse Act ("CFAA").

The first three counts of Lockheed's Amended Complaint are predicated upon alleged violations of the CFAA. The CFAA provides stiff criminal penalties, and in appropriate instances, civil remedies, against those who access a computer without authorization, and cause damage to it. This statute is designed to provide criminal and civil recourse against "hackers," cyber-terrorists, and those who intentionally damage computers by transmission of worms and viruses.

Counts I and III of Lockheed's Amended Complaint fail to state a claim against Speed and Fleming for the simple reason that Lockheed acknowledges in the Amended Complaint that Speed and Fleming were authorized to access the information allegedly misappropriated and the computers from which it was allegedly misappropriated. Because the CFAA is directed to "outside" unauthorized accessors (such as hackers) and not persons who access computers with authorization to do so, Counts I and III fail to state a claim against Speed and Fleming. Count II purports to state a claim under the provision of the CFAA that proscribes the knowing transmission of data to a computer with the intent to cause damage to the computer. Lockheed has pled nothing which would amount to a violation of this provision of the CFAA by Speed and Fleming. This Count also should be dismissed for failure to state a claim.

II. LEGAL ARGUMENT

A. Applicable Legal Standard

A complaint should be dismissed pursuant to Rule 12(b)(6) where it is "clear that no relief could be granted under any set of facts that could be proved consistent with the allegations." *Blackston v. Alabama*, 30 F. 3d 117, 120 (11th Cir. 1994). In ruling on a motion to dismiss, "conclusory allegations, unwarranted factual deductions, or legal conclusions masquerading as facts will not prevent dismissal." *Davila v. Delta Airlines, Inc.*, 326 F.3d 1183, 1185 (11th Cir. 2003). As the Supreme Court has stated, a plaintiff may not merely "label" his or her claims to survive a motion to dismiss. *Conley v. Gibson*, 355 U.S. 41, 45, 78 S. Ct. 99, 102, 2 L. Ed. 2d 80 (1957). At a minimum, the Federal Rules of Civil Procedure require "a short and plain statement of the claim" that "will give the defendant fair notice of what the plaintiff's claim is and the grounds upon which it rests." *Id.* at 47 (quoting Fed. R. Civ. P. 8(a)(2)).

B. The CFAA

The CFAA was enacted "to impose criminal penalties and civil remedies against 'computer hackers (e.g. electronic trespassers)'." *Int'l. Ass'n. of Machinists v. Werner-Masuda*, 390 F. Supp. 2d 479, 495 (D. Md. 2005). "[D]esigned primarily to punish criminal violations," the CFAA also recognizes private civil causes of action in certain limited instances. *In re: America Online, Inc.*, 168 F. Supp. 2d 1359, 1368 (S.D. Fla. 2001). "As the legislative history indicates, a civil cause of action was added to redress damage and loss as a result of serious computer abuses, such as

transmission of viruses or destructive worms and use of fraud to access non-public information." *Davies v. Afilias Ltd.*, 293 F. Supp. 2d 1265, 1273 (M.D. Fla. 2003) (Presnell, J.), *citing* S. Rep. 101-544 (1990) ("Misuse of computers, whether it is by a spy probing military secrets or a destructive computer virus or worm released onto a computer network, threatens the work of all computer users.").

C. Because Lockheed has Conceded that Speed and Fleming were Authorized to Access the Subject Computers and the Information on Them, Counts I and III Fail to State a Claim.

Count I of Lockheed's Amended Complaint purports to state a claim against Speed and Fleming for alleged violations of 18 U.S.C. § 1030(a)(4), which provides remedies against: "[w]hoever—knowingly and with intent to defraud, accesses a protected computer **without authorization**, or **exceeds authorized access**, and by means of such conduct furthers the intended fraud and obtains anything of value. . . ." (emphasis added). Count III of Lockheed's Amended Complaint purports to state a claim under 18 U.S.C. § 1030(a)(5)(A)(ii), which provides remedies against a person who "intentionally accesses a protected computer **without authorization** and as a result of such conduct, recklessly causes damage" (emphasis added). Both of these counts fail to state claim, because the Amended Complaint affirmatively reveals that Speed and Fleming were authorized to access the computers and the information at issue.

Lockheed alleges in the Amended Complaint that "[b]ecause of his position as program manager, Speed had **complete access** to ATARS confidential and proprietary and trade secret protected information." Amended Complaint at ¶ 24

(emphasis added). As for Fleming, Lockheed admits that "[b]y virtue of his director-level position, [Fleming] had **unrestricted access** to [Lockheed's] shared network drives, including data folders containing ATARS confidential and proprietary and trade secret protected information." *Id.* at ¶ 27 (emphasis added). Lockheed also concedes that Speed and Fleming had authorized access to the alleged misappropriated documents detailed in the Amended Complaint through Lockheed's computers during the time of their employment. *Id.* at ¶ 50. Lockheed concedes, therefore, that the conduct attributed to Speed and Fleming occurred while they were still employees of Lockheed, and while they had complete, unrestricted, and fully authorized access to the subject computers and the information on them. As is evident on the face of the Amended Complaint, therefore, Speed and Fleming had authorized access to the information they allegedly misappropriated, and accordingly, could not have committed any violation of the CFAA.

To avoid this patently obvious impediment to its claim, Lockheed alleges that Speed and Fleming were not authorized to access the allegedly misappropriated information "for their own financial benefit or for the financial benefit of L-3 or Mediatech." *Id*. at ¶ 69. Thus, conceding, as it must, that Speed and Fleming were employees of Lockheed at the time they allegedly accessed the information and conceding, as it must, that Speed and Fleming had authority to access the information, Lockheed nevertheless attempts to turn these alleged acts into violations of the CFAA, by referencing the alleged motive for accessing the information, rather than the act of accessing itself. The motive of the accessor is not

a component of a claim under the CFAA, however, and a cause of action does not exist where a computer is accessed with authority, but with an improper motive.

No court in this jurisdiction has yet addressed the question of whether an employer has a claim under the CFAA against a former employee who has accessed information on the employee's computer, with authority to do so, and subsequently misappropriated it for the benefit of a new employer. Recently, however, a court in the District of Maryland expressly ruled that the CFAA does not apply in such a situation. In *Werner-Masuda*, 390 F. Supp. 2d 479, the defendant, Werner-Masuda, while an officer of the plaintiff labor union ("IAM"), had authorized access to a secure proprietary website of IAM, from which she could access IAM's confidential membership list. IAM alleged that Werner-Masuda used her status as an IAM officer to access the confidential site, retrieve the names and addresses of IAM's members, and use them to organize a rival competing union ("UIFA") to challenge IAM's representation. The *Werner-Masuda* court dismissed the plaintiff's CFAA claims, ruling that because the defendant had authority to access the allegedly misappropriated information, no claim existed under the CFAA, regardless of any subsequent misuse of the information. In the *Werner-Masuda* case, as in Lockheed's Amended Complaint here, the plaintiff's claim was based not upon damage allegedly caused by the act of accessing the computer, but rather was based upon what the defendant allegedly did with the information once it was obtained. *Id.* at 499. In ruling that no claim existed under the CFAA for such alleged conduct, the *Werner-Masuda* court concluded, "the CFAA [does] not prohibit the

unauthorized disclosure or use of information, but rather, unauthorized access. Nor [does the CFAA] proscribe authorized access for unauthorized or illegitimate purposes." *Id*.

In reaching its holding, the *Werner-Masuda* court concluded that the CFAA was not intended to apply to a situation where an employee, with authority to access information from a computer, misappropriates that information for some alleged improper purpose. *Id.* at 494-499. In so doing, the *Werner-Masuda* court considered and specifically rejected the decision in *Shurgard Storage Centers, Inc. v. Safe Guard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000), upon which Lockheed will likely rely. In *Shurgard*, employees of the plaintiff e-mailed confidential information from their work computers to the plaintiff's competitor, and later took jobs with the competitor. The *Shurgard* court concluded that even though the employees were authorized to access the misappropriated information, they acted "without authorization" because they were acting as agents of their future employer at the time of the misappropriation. In so doing, the *Shurgard* court opened the doors of the CFAA to claims against not only outside "hackers," but also "insider" employees with full authorization to access the subject computer, provided the plaintiff contends that the information was accessed for an improper purpose. In declining to follow the lead of *Shurgard*, the *Werner-Masuda* court reasoned as follows:

> Recognizing that *Shurgard* provides plaintiff some support for a broader interpretation of these statutes, the Court, nevertheless, concludes that in light of the more persuasive statutory interpretations discussed above, the legislative history, and the fact that the SECA

> and the CFAA are primarily criminal statutes, and, thus, should be construed narrowly, it is beyond doubt that plaintiff can prove no set of facts that would entitle it to relief under either the SECA or the CFAA. Plaintiff simply cannot overcome the fact, supported by its own allegations, that Werner-Masuda was authorized to access the information contained in VLodge, and that at the time she was allegedly accessing it on behalf of UIFA her access had not been revoked. Accordingly the Motion to Dismiss Counts I and II for failure to state a claim will be granted.

Werner-Masuda, 390 F. Supp. 2d at 499.

Likewise, in *In re: American Online, Inc.*, Judge Gold of the Southern District of Florida dismissed a civil action brought pursuant to 18 U.S.C. § 1030(a)(5)(A)(ii),[1] finding that this subsection of the CFAA "clearly contemplates a situation where an outsider, or someone without authorization, accesses a computer." 168 F. Supp. 2d at 1370 (citing and quoting the Senate Report on the CFAA which references "outside hackers").

The CFAA exists to provide stiff criminal penalties and civil remedies against hackers and those who damage computers by transmitting viruses and worms. The CFAA should not be interpreted to federalize garden-variety employee misappropriation of trade secret claims. Adequate and sufficient state law remedies exist where such conduct can be proven. Indeed, Lockheed has managed to recast its allegations into ten separate state-law causes of action. In light of the plain language of the CFAA, and its legislative history, this Court should adopt the reasoning of the *Werner-Masuda* court and limit the CFAA to those situations for

[1] At that time, this subsection of the statute was numbered § 1030(a)(5)(B).

which it was designed. Accordingly, Counts I and III of Lockheed's Amended Complaint should be dismissed for failure to state a claim.

D. Because Lockheed has Failed to Allege any Facts that Would Support It, Count II Also Fails to State a Claim and Should be Dismissed.

Count II of the Amended Complaint also fails to state a claim. Count II attempts to assert a claim under 18 U.S.C. § 1030(a)(5)(A)(i), which provides criminal penalties against a person who "knowingly causes the transmission of a program, information, code or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer." This subsection of the CFAA would obviously apply, for example, to a person who transmits e-mails embedded with a computer virus, for the purpose of intentionally damaging the computers to which the virus is sent. Such a person would be subject to prosecution under the CFAA, provided the transmission actually caused damage to a computer. How this statute could possibly create a remedy against an employee who is alleged merely to have copied information from his computer for the benefit of his future employer, however, is incomprehensible. In purporting to state this claim, Lockheed has done nothing more than parrot the language of the statute. Lockheed has not, and cannot, allege facts that would constitute any "transmission of a program, information, code or command," and has not, and cannot, allege any facts to support the bald conclusion that as a result of such "transmission," Speed and Fleming "intentionally cause[d] damage" to a Lockheed computer. This provision of the CFAA is simply, on its face, inapplicable to the

claims asserted by Lockheed, and Count II of the Amended Complaint should be dismissed for failure to state a claim.

III. CONCLUSION

For the foregoing reasons, Counts I through III of Lockheed's Amended Complaint fail to state a claim upon which relief can be granted against Defendants Speed and Fleming, and should be dismissed.

Respectfully submitted,

s/William C. Guerrant, Jr.
Benjamin H. Hill, III
Florida Bar No. 094585
William C. Guerrant, Jr.
Florida Bar No. 516058
Lara J. Tibbals
Florida Bar No. 0129054
HILL, WARD & HENDERSON, P.A.
Suite 3700 – Bank of America Building
101 East Kennedy Boulevard
Post Office Box 2231
Tampa, Florida 33601
Telephone: (813) 221-3900
Facsimile: (813) 221-2900
E-mail: wguerrant@hwhlaw.com
Attorneys for Defendants Speed & Fleming

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on April 24, 2006, I electronically filed the foregoing with the Clerk of the Court by using the CM/ECF system which will send a notice of electronic filing to Kay L. Wolf, Ford & Harrison, LLP, 300 South Orange Avenue, Suite 1300, Orlando, Florida 32801; Nathaniel H. Akerman and Creighton R. Magid, Dorsey & Whitney, LLP, 250 Park Avenue, New York, New York 10177; David B.

King, King, Blackwell, et al., Post Office Box 1631, Orlando, Florida 32802-1631; and to Ned H. Bassen, Hughes Hubbard & Reed, LLP, One Battery Park Plaza, New York, New York 10004.

s/William C. Guerrant, Jr.
Attorney