IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

CARNEGIE STRATEGIC DESIGN ENGINEERS, LLC, Plaintiff,	)	
vs.	)	
SCOTT M. CLOHERTY, JAMES W. BURGER, III, ROY D. POINTEK, SHAWN W. SHANER, and CHRISTINE A. BELOTTI MOYER, Defendants.	)	Civil Action No. 13-1112

MEMORANDUM OPINION

CYNTHIA REED EDDY, United States Magistrate Judge.

I. INTRODUCTION

Presently before the Court for disposition is defendants' motion to dismiss [ECF No. 7] plaintiff's complaint. For the following reasons, defendants' motion to dismiss is granted.[1]

II. BACKGROUND

Plaintiff, Carnegie Strategic Design Engineers, LLC, ("plaintiff") is a "full-service, professional engineering firm having expertise in several major engineering disciplines" and employed the defendants at its Pittsburgh, Pennsylvania office for a time up to approximately fall of 2012. *See* Compl. [ECF No. 1] at ¶¶ 1-7, 9. Defendants Burger and Piontek were employed

[1] Under the Federal Magistrate Judges Act ["Act"], a Magistrate Judge's jurisdiction may arise through the consent of the parties. 28 U.S.C. § 636(c). Under the Act, "[u]pon consent of the parties, a full-time United States magistrate judge . . . may conduct any or all proceedings in a jury or nonjury civil matter and order the entry of judgment in the case, when specially designated to exercise such jurisdiction by the district court." 28 U.S.C. § 636(c)(1). Such a referral gives the magistrate judge full "authority over dispositive motions, conduct of trial, and entry of final judgment, all without district court review." *Roell v. Withrow*, 538 U.S. 580, 585 (2003); *In re Search of Scranton Hous. Auth.*, 487 F.Supp.2d 530, 535 (M.D.Pa. 2007). "[S]o long as consent [to Magistrate Judge jurisdiction] is clear and unambiguous, it is effective." *In re Search of Scranton Hous. Auth.*, 487 F.Supp.2d at 535; *Roell*, 538 U.S. at 591 (consent may be inferred from parties' actions). Both parties have consented to Magistrate Judge jurisdiction. *See* Pl.'s Consent to Magistrate Judge Jurisdiction [ECF No. 14]; Defs.'s Consent to Magistrate Judge Jurisdiction [ECF No. 13]. Therefore, it is appropriate for this Court to decide dispositive motions and to enter final judgment.

by plaintiff as Senior Process Control Systems Engineers until they voluntarily terminated their employment on or about August 13, 2012. *Id*. at ¶¶3-4. Defendant Shaner was employed by plaintiff as a Process Control/Electrical Technical Specialist until he voluntarily quit on approximately September 12, 2012. *Id*. at ¶ 5. Defendant Moyer was employed by plaintiff as an Electrical Engineer until she voluntarily quit on or about August 13, 2012. *Id*. at ¶ 6. Defendant Moyer is also a licensed Professional Engineer. Id. Each defendant unilaterally left plaintiff's employment to work for plaintiff's competitor. *Id*. at ¶ 13.

Plaintiff owns and maintains a password-protected computer system with a file and email server for use in operating its business, storing confidential company and client information and performing work on client projects. *Id*. at ¶ 11. Each defendant had access to this system and plaintiff limited their access for purposes related to client work on plaintiff's behalf. *Id*. at ¶ 15. Upon leaving plaintiff's employ, each defendant copied and stole "valuable data from [p]laintiff's password protected computer system and took that data for use unrelated to his or her subsequent employment [with] [p]laintiff's competitor. Pl.s' Op. Br. [ECF No. 12] at 3. Plaintiff claims that defendants had "no authority to access [p]laintiff's password-protected computer system or the data therein for any other purpose, and any such access for purposes other than serving [p]laintiff was . . . without authorization. Compl. [ECF No. 1] at ¶ 15. All told, defendants took more than 285 Gigabytes of data from plaintiff's system, including confidential company and customer data. *Id*. at ¶¶ 22-26; *See* Pl.'s Op. Br. [ECF No. 12] at 1. Specifically, the data taken by defendants included "detailed company and client information including client project data, engineering drawings, cost estimating data, customer contact information, vendor contact information and other non-public proprietary, business and trade secret information." Compl. [ECF No. 1] at ¶ 31. In some instances, defendants took data

unrelated to any client work or other matters in which that particular defendant was involved, and plaintiff claims that defendant could not have any possible legitimate business purpose or use for. *Id*. at ¶ 33. Plaintiff claims that the commercial value of the non-public business information taken is worth approximately $10,000,000. *Id*. at ¶ 27. Plaintiff has suffered losses of out-of-pocket expenses in excess of $5,000 related to computer forensic investigation, analysis, review and mitigation of the data breach and theft and also loss of productivity incurred as plaintiff's senior-level management and in-house staff investigated the data breach and theft. *Id*. at ¶ 34.

Plaintiff asserts that defendant's retrieval and copying of its data was in direct violation of its employee policies. During their employment, each defendant was given and required to comply with plaintiff's employee handbook, which set forth employee policies regarding confidentiality of client and customer matters, Internet usage, laptop security, work created by employees, protecting company information, conflicts of interest and code of ethics, outside employment and resignation. *Id*. at ¶ 14.

Plaintiff filed the instant complaint alleging defendants violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA").[2] Plaintiff therefore argues that counter to defendants' obligation and agreement to return all property owned by plaintiff, the defendants accessed, copied, removed and stole valuable data from Plaintiff's password-protected computer system and took that data for use unrelated to their employment with plaintiff and for use in connection with their employment by plaintiff's competitor. Plaintiff argues that defendants "lost all authority to access [p]laintiff's password-protected computer system the instant they undertook to do so for their own benefit or the benefit of any third person." Compl. [ECF No. 1] at ¶ 20.

[2] Plaintiff's complaint additionally alleged a claim for conversion and the misappropriation of trade secrets and proprietary business information. Those claims have been voluntarily dismissed without prejudice by plaintiff. *See* Stip. of Dismissal [ECF No. 16].

Moreover, under 18 U.S.C. § 1030(e)(6), "[t]o the extent [d]efendants might otherwise have had any authority to access the data on [p]laintiff's password-protected computer system, they exceeded their authority by accessing such data for anything other than legitimate business purposes relating to [p]laintiff's business operations. *Id.* at ¶ 21.

In response to plaintiff's claims, defendants filed a motion to dismiss setting forth two discrete arguments: (1) plaintiff has not properly asserted damage or loss under the CFAA; and (2) plaintiff has failed to plead that defendants' access to its computer system was "unauthorized" under the CFAA. *See* Br. in Supp. of Mot. to Dismiss [ECF No. 8] at 2. The Court will address each argument in turn.

III. JURISDICTION

This Court has original jurisdiction over this matter pursuant to 28 U.S.C. § 1331 as the action raises questions of federal law under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA").

IV. STANDARD OF REVIEW

Generally, a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) tests the legal sufficiency of a complaint. For a complaint to survive a Rule 12(b)(6) challenge, it must include factual allegations that "state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 697 (2009). A court in determining whether a complaint meets this standard must read the complaint in the light most favorable to the plaintiff and all well-pleaded facts must be taken as true. *Id.* at 677. "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (citing *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 556 (U.S. 2007)). That a court must accept all factual allegations in a complaint does not apply to legal

conclusions of the complaint. *Iqbal*, 556 U.S. at 678. Additionally, "[t]hreadbare recitals of the elements of a cause of action supported by mere conclusory statements, do not suffice." *Id.* (citing *Twombly*, 550 U.S. at 555.) (the court is not "bound to accept as true a legal conclusion couched as a factual allegation")). Accordingly, "a complaint must do more than allege the plaintiff's entitlement to relief. A complaint has to 'show' such an entitlement with its facts." *Fowler v. UPMC Shadyside*, 578 F.3d 203, 210-11 (3d Cir. 2009). Doing so "does not impose a probability requirement at the pleading stage, but instead simply calls for enough facts to raise a reasonable expectation that discovery will reveal evidence of the necessary element." *Phillips v. County of Allegheny*, 515 F.3d 224, 232 (3d Cir. 2008) (quoting *Twombly*, 550 U.S. at 556, n.3).

V. ANALYSIS

The CFAA is generally an anti-hacker statute that prohibits unauthorized access or the exceeding of authorized access of computers connected to interstate commerce[3] and subjects such violators to criminal and/or civil liability. *See Dresser-Rand Co. v. Jones*, --- F.Supp.2d ---, ---, 2013 WL 3810859, at *3 (E.D.Pa. July 23, 2013) ("*Dresser-Rand*"); *Shamrock Foods Co. v. Gast*, 535 F.Supp.2d 962, 965 (D.Ariz. 2008) ("[t]he general purpose of the CFAA was to create a cause of action against computer hackers (e.g., electronic trespassers)"). The scope of the CFAA has been expanded in recent years and "[e]mployers . . . are increasingly taking advantage of the CFAA's civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system." *P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d

[3] *See* 18 U.S.C. § 1030(e)(2)(B); *U.S. v. Drew*, 259 F.R.D. 449, 457 (C.D.Cal. 2009) (that a computer has been connected to interstate commerce "will always be met when an individual using a computer contacts or communicates with an Internet website"); *Mahoney v. DeNuzzio*, 2014 WL 347624, at *5 (D.Mass. Jan. 29, 2014) (same). It is not challenged that the computers in question were connected to the Internet and used in interstate commerce, therefore plaintiff's computers were "protected computers" under the CFAA.

504, 510 (3d Cir. 2005) (citations omitted).

The presently applicable CFAA provision provides:

> Whoever . . . 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, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period . . . shall be punished as provided in subsection (c) of this section.

18 U.S.C. §1030(a)(4).[4] Thus, there are four elements for a claim under section 1030(a)(4): "(1) defendant has accessed a 'protected computer'; (2) has done so without authorization or by exceeding authorization as was granted; (3) has done so 'knowingly' and with 'intent to defraud'; and (4) as a result has 'further[ed] the intended fraud and obtain[ed] anything of value.'" *P.C. Yonkers, Inc.,* 428 F.3d at 508 (quoting 18 U.S.C. § 1030(a)(4)). *See also Curran v. Mark Zinnamosca & Associates*, 2014 WL 271634, at *6 (M.D.Pa. Jan. 23, 2014).

a. Damages and Loss under the CFAA

First, defendants argue that plaintiff's complaint should be dismissed for failure to allege damage or loss under the CFAA.

Section 1030(g) of the CFAA authorizes a private cause of action for any person "who suffers damage **or** loss by reason of a violation" but "only if the conduct involves [one] of the factors set forth in" subsection 1030(c)(4)(A)(i). 18 U.S.C. § 1030(g) (emphasis added). Because Section 1030(g) is disjunctive, a plaintiff meets its burden by showing either loss or damage. Here, plaintiff alleges loss under Section 1030(c)(4)(A)(i)(I) which provides that the loss be to "one or more persons during any one year period . . . aggregating at least $5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I).

[4] Although the CFAA imposes criminal penalties, it provides for civil penalties in limited situations in which a person "suffers damage or loss by reason of a violation of" the CFAA. 18 U.S.C. § 1030(g).

The term "loss" under the CFAA is defined as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). Additionally, "district court decisions in the [Court of Appeals for the] Third Circuit have held that to fall within this definition of 'loss,' the 'alleged "loss" must be related to the impairment or damage to a computer or computer system.'" *Brooks v. AM Resorts, LLC*, 954 F.Supp.2d 331, 338 (E.D.Pa. 2013) (quoting *Sealord Holdings, Inc. v. Radler*, 2012 WL 707075, at *4 (E.D.Pa. Mar. 6, 2012) (additional citations omitted)). Therefore, loss under the CFAA is compensable if "the cost of remedial measures taken to investigate **or** repair the damage to the computer, or loss is the amount of lost revenue resulting from a plaintiff's inability to utilize the computer while it was inoperable because of a defendant's misfeasance." *Clinton Plumbing & Heating of Trenton, Inc. v. Ciaccio*, 2011 WL 6088611, at *5 (E.D.Pa. Dec. 7, 2011) (emphasis added).

Here, defendants argue that plaintiff has not properly asserted damage under the CFAA, because the only damages recoverable are (1) the cost of remedial measures taken to investigate and repair damage to the computer system and (2) lost revenue when the damage computer was inoperable. *See* Br. in Supp. of Mot. to Dismiss [ECF No. 8] at 2. Specifically, defendants argue that plaintiff

> does not allege that [d]efendants deleted any data or otherwise caused harm to the computer system, nor does it assert that their conduct rendered the system inoperable . . . . [Plaintiff] merely asserts that it retained a computer forensic expert to identify the data that [d]efendant copied for their own benefit. The costs associated with investigating an alleged trade secret misappropriation are not recoverable under the CFAA.

Id. Plaintiff responds that it has adequately pled the loss requirement of the CFAA. This Court agrees that plaintiff has adequately pled loss for the following reasons.

Under the CFAA and persuasive authority authored by our sister courts, plaintiff need not show that their system was rendered inoperable, or that tangible damage was done to their computer system. Plaintiff may show loss by alleging that it expended an amount to investigate whether such damage occurred. *See Brooks*, 954 F.Supp.2d at 338 ("fees paid to an expert for investigating and remedying damage to a computer may be a cognizable 'loss' under the CFAA"); *Dudick, ex rel. Susquehanna Precision, Inc. v. Vaccarro*, 2077 WL 1847435, at *5 (W.D.Pa. June 25, 2007) (same). *See also A.V. ex rel. Vanderhye v. iParadigms*, LLC, 562 F.3d 630, 646 (4th Cir. 2009) ("the costs of responding to the offense are recoverable including costs to investigate and take remedial steps"). Here, plaintiff relies on the "loss" factor under Section 1030(g) rather than the "damage" factor to state a claim under the CFAA. It claims it expended an amount in excess of $5,000 to conduct a computer forensic investigation, analysis and review and to mitigate the data breach, and incurred a loss of productivity due to the in-house investigation of the data breach. Taken these statements as true, as the Court must at this phase, plaintiff has met the required loss element because these are reasonable costs plaintiff expended in responding to the data breach caused by defendants and conducting a damage assessment. Therefore, plaintiff's complaint will not be dismissed for failure to show loss.

b. "Exceeding Authorized Access" under the CFAA

Although plaintiff has adequately plead that it incurred a loss under the CFAA due to defendants' actions, it must still show that defendants either obtained access to the computer without authorization or exceeded their authorized access when they obtained access to copy the data from plaintiff's computers. For the following reasons, this Court finds that defendants

neither obtained access to the data without authorization nor exceeded their authorized access in copying the files and plaintiff's complaint is dismissed for failure to state a claim under the CFAA.

To be subject to civil liability under the CFAA, the violator must access a protected computer without authorization, or exceed his authorized access. *See* 18 U.S.C. § 1030(a)(4). The term "exceeds authorized access" is defined 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). The term "authorization" is not defined under the CFAA, which thus entrusts the courts to interpret the term's reach. As one court has indicated, courts must "wrestle with the breadth of its meaning as increasingly, employers have used a statute originally designed to punish hackers against disloyal employees. Determining an employee's authorization to company computer systems is further complicated by the proliferation of employer computer and internet use policies." *Dresser-Rand*, 2013 WL 3810859 at *5.

Also complicating this issue is the circuit-split that has arisen as a result of divergent interpretations from deciphering the breadth of the term "authorization." As our sister court has detailed:

> Under the narrow view, an employee given access to a work computer is authorized to access that computer regardless of his or her intent to misuse information and any policies that regulate the use of information. *See WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012); *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (*en banc*); *LVRC Holdings, LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009). Under the broad view, if an employee has access to information on a work computer to perform his or her job, the employee may exceed his or her access misusing the information on the computer, either by severing the agency relationship through disloyal activity, or by violating employer policies and/or confidentiality agreements. *See U.S. v. John*, 597

> F.3d 263 (5th Cir. 2010); *U.S. v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010); *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *EF Cultural Travel BV v. Explorica, Inc*., 274 F.3d 577 (1st Cir. 2001).

Id. at *5.[5]

Generally, defendants argue that this Court should follow the reasoning set forth in the Court of Appeals for the Fourth and Ninth Circuits, and district courts in this circuit[6] and apply the narrow interpretation of the statutory language, while plaintiff argues that the Court of Appeals for the Third Circuit has already adopted the majority view in *United States v. Tolliver*, 451 Fed. App'x 97 (3d Cir. 2011); *cert. denied* 133 S.Ct. 105 (2012) ("*Tolliver*") and this Court should follow suit by applying the broader interpretation of the statute.

Defendants argue that plaintiff has failed to plead that their access to its computer system was unauthorized under the CFAA because other district courts in the Court of Appeals for the Third Circuit when faced with this same issue have held that employees who are authorized to access the data at issue do not "exceed their authority if they copy that data for their own benefit." Br. in Supp. of Mot. to Dismiss [ECF No. 8] at 2. Defendants argue "it is the access to the information, rather than the use of the information, that must be unauthorized in order to constitute a civil violation under the CFAA." *Id*. Therefore, because plaintiff concedes the fact that defendants "were authorized to access the information and data that they copied," defendants

---

[5] Academics have labeled these views into three categories as "agency-based authorization, code-based authorization and contract based authorization." *Dresser-Rand*, 2013 WL 3810859 at *5 (citations omitted).

[6] The Eastern District of Pennsylvania has generally adopted the narrow interpretation of the CFAA. *See Synthes, Inc. v. Emerge Medical, Inc.*, 2012 WL 4205476 (E.D.Pa. Sept. 19, 2012); *Grant Mfg. & Alloying, Inc. v. McIlvain*, 2011WL 4467767 (E.D.Pa. Sept. 23, 2011) *aff'd* 499 Fed. App'x 157 (3d Cir. 2012); *Clinton Plumbing and Heating of Trenton, Inc. v. Ciaccio*, 2010 WL 4224473 (E.D.Pa. Oct. 22, 2010); *Integrated Waste Solutions, Inc. v. Goverdhanam*, 2010 WL 4910176 (E.D.Pa. Nov. 30, 2010); *Bro-Tech Corp. v. Thermax, Inc.*, 651 F.Supp.2d 378 (E.D.Pa. 2009); *Brett Senior & Assoc., P.C. v. Fitzgerald*, 2007 WL 2043377 (E.D.Pa. July 13, 2007); *but see HUB Grp. Inc. v. Clancy*, 2006 WL 208684 (E.D.Pa. Jan. 25, 2006) (finding employee exceeded scope of authorization when he emailed confidential information to his wife); *Feinberg v. Ecklemeyer*, 2009 WL 4906376 (E.D.Pa. Dec. 16, 2009) (the employee's authorization to access the employer's computers after a certain date was a question of fact that survived the motion to dismiss phase).

have not violated the CFAA. *Id*.

Plaintiff responds that civil liability under the CFAA extends to employees who copy data from an employer's protected computer. Pl.'s Op. Br. [ECF No. 12] at 7. Plaintiff relies heavily on the non-precedential finding in *Tolliver* for this point. In *Tolliver*, the defendant was convicted of violating, inter alia, the CFAA for running a fraudulent check cashing scheme. Tolliver was an employee of a bank and had access to the bank's computer systems that were used to manage and track its customer accounts. *Tolliver*, 451 Fed. App'x at 99. Tolliver used her own employee number and password to the bank's computer system to access customer information and used such information to gain access to customer information and allegedly provided it to a third party to be used to create and cash fraudulent checks. *Id*. The Court of Appeals noted that Tolliver had no business purpose to access the customer's information as "Tolliver was . . . not assigned to contact any of these individuals for sales purposes . . . [and bank] employees were not permitted to look at a customer's account and personal information without a business purpose." *Id*. at 100. Plaintiff argues that "the Third Circuit explicitly found that the CFAA's 'exceeds authorized access' provisions apply in circumstances . . . where employees are given access to a protected computer for business purposes but exceed their authorized access to obtain information for unauthorized purposes." Pl.'s Op. Br. [ECF No. 12] at 10.

This Court finds that the Court of Appeals for the Third Circuit has not explicitly adopted the broader and majority interpretation, and accordingly finds that the narrow interpretation of the CFAA adopted by the Court of Appeals for the Ninth and Fourth Circuits and by district courts in our circuit is the proper interpretation of the statute and the true interpretation of Congress' intent in enacting the statute.

The entirety of the Court of Appeal's analysis on the CFAA in *Tolliver* is as follows:

> As already discussed, there was sufficient evidence from which to infer that Tolliver intentionally accessed the customers' accounts and that she did not have a business purpose to do so. As such, the government established that Tolliver exceeded her authorized access, and we will affirm her conviction for this offense.

Tolliver, 451 Fed. App'x at 103.

The Court had no occasion and did not address the discrete issue at hand. The narrow holding in *Tolliver* cannot fairly be characterized as an express adoption of the broad interpretation of the CFAA language. The issue in *Tolliver* was whether the criminal conviction was supported by sufficient evidence. The Court was not asked to address the breadth of the term "authorization." Tellingly, the opinion in *Tolliver*, which was decided in the midst of circuit split described above, did not reference that fact. The Court did not cite to or discuss cases in which the broad view or the narrow view of the language in the CFAA was at issue. Thus, this Court declines to find that the Court of Appeals for the Third Circuit "expressly" adopted the broader interpretation of the CFAA or to extend the holding in *Tolliver*, especially in light of the non-precedential status of that decision. *See In re Grand Jury Investigation*, 445 F.3d 266, 276 (3d Cir. 2006); *Gilmore v. Ford Motor Co*., 2013 WL 869382, at *1 (W.D.Pa. March 7, 2013). In addition, the narrow interpretation of the CFAA, as applied by the district courts in this circuit, provides persuasive authority that the term "authorization" should be so interpreted.

In *Brett Senior & Associates*, an employee before resigning from the plaintiff-employer copied certain confidential business information from the employer's system to an external hard drive and the court held as a matter of law that he did not exceed his authorized access because "[h]e did not obtain any information that he was not entitled to obtain or alter any information that he was not entitled to alter." *Brett Senior & Assoc., P.C. v. Fitzgerald*, 2007 WL 2043377, at

*3 (E.D.Pa. July 13, 2007). In so finding the court stated that the conduct targeted by the CFAA "is the unauthorized procurement or alteration of information, not its misuse or misappropriation. Because there is no allegation that [defendant-employee] lacked authority to view any information in the [employer's] computer system, the CFAA claim fails." *Id*. at *3 (internal citations omitted).

Subsequently, in *Consulting Professional*, the court dismissed a claim under the CFAA against a former employee who was permitted to access the plaintiff-employer's computer system for use in her employment. *Consulting Professional Resources, Inc. v. Concise Technologies LLC*, 2010 WL 1337723, at *5 (W.D.Pa. March 9, 2010). Again, the employee copied her employer's confidential information from the employer's computer system to use at her new company before resigning. *Id*. The court dismissed the claim because it found that the employee's access to her employer's computer system did not exceed her authorization under the CFAA. *Id*. The court found that because the employer admitted that the employee had access to the confidential information accessed, and argued that the employee violated her employment contract to obtain confidential information only for business purposes, this was not enough to state a claim under CFAA. *Id*. It found that "[w]hile disloyal employee conduct might have a remedy in state law, the reach of the CFAA does not extend to instances where the employee was authorized to access the information he later utilized to the possible detriment of his former employer." *Id*. at *6.

Finally, in *Dresser-Rand*, the former-employees/defendants accessed their work laptops and downloaded thousands of documents to external storage devices. *Dresser-Rand*, 2013 WL 3810859 at *9. The court found that if the defendants "were authorized to access their work laptops and to download files from them, they cannot be liable under the CFAA even if they

subsequently misused those documents to compete against" the plaintiff. *Id*. As for the employer's policies limiting its computers and system to be used only for legitimate business purposes, the court found that such policies governed use and not access of the computers. *Id*.

In coming to this conclusion, the *Dresser-Rand* court conducted a thorough analysis of both the majority and minority views and found that the narrow interpretation of "without authorization" and "exceeds authorized access" applied. It stated:

> Courts that adopt the narrow view base their reasoning on the plain language of the statute, dictionary definition of "authorization," and the rule of lenity. The Fourth Circuit goes through this analysis for a factual scenario very similar to this case. A [former] employee emailed downloaded confidential [company] documents to a personal computer prior to resigning from the company to work for one of its competitors. *WEC Carolina* [*Energy Solutions LLC v. Miller*], 687 F.3d [199,] 202 [(4th Cir. 2012)]. The employee allegedly used the downloaded information to make a presentation on behalf of the competitor to a potential [company] customer, and won the projects for the competitor. *Id*. [The employer] had given the employee a laptop computer and authorized access to the company's intranet and servers. *Id*. [The employer] has policies "prohibiting the use of any confidential information and trade secrets unless authorized" and prohibiting the "download[ing] [of] confidential and proprietary information to a personal computer. *Id*. at 206-07. Yet [the employer] alleged in its complaint that defendant "had access to [the employer's] intranet and computer servers and to numerous confidential and trade secret documents stored on these computer servers." *Id*. at 207.
>
> The Court began with examining the plan language of the statue. *Id*. at 203. It recites the Oxford English Dictionary definition for "authorization": "formal warrant, or sanction." *Id*. at 204. Citing the Ninth's Circuit's analysis in *LVRC Holdings, LLC v. Brekka*, the [Fourth Circuit] concluded that "**an employee is authorized to access a computer when his employer approves or sanctions his admission to that computer," and employee is "without authorization" when "he gains admission to a computer without approval," and an employee "exceeds authorized access" "when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access**." *Id*. at 204

> (citing *LVRC Holdings LLC, v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009)). **These definitions do not extend to the improper use of information validly accessed**. *Id*. at 204. Thus, the [Fourth Circuit] concluded that while defendants may have misappropriated information, they did not access a computer without authorization or exceed their authorized access. *Id*. at 207.
>
> As for an ambiguity surrounding the term "without authorization," the Court noted that its interpretation would apply to both the civil and criminal parts of the statute, and therefore any ambiguity would be resolved in favor of lenity. *Id*. at 204. This rule ensures that we are shielded from unexpected criminal consequences of ambiguous statutes. *Id*. As a result, the Court was "unwilling to contravene Congress's intent by transforming 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." *Id*. at 207.

Id. at *6 (internal citations and quotations omitted) (emphasis added).[7] Therefore, based on this interpretation, the court found that "[t]he statute simply does not support a broad interpretation of 'authorization' based on employer use policies." *Id*. at *8.

Here, plaintiff admits that each defendant was permitted to access its computer system and network and was permitted to access the data at issue. Compl. [ECF No. 1] at ¶ 15. Plaintiff does not allege that defendants "hacked into" a computer or the files that they were not otherwise permitted to access. Rather, the crux of plaintiff's argument is that rejected by the *Consulting Professional* court – that defendants lost the right to access such information when they did so for their own or a third parties benefit, and to the detriment of plaintiff. Such a finding is

[7] The *Dresser-Rand* court also explained the reasoning used by the Court of Appeals for the Ninth Circuit adopting a narrow interpretation of the statute in *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc). The *Nosal* court posited its analysis on the seemingly innocuous scenarios that would be criminally and civilly punishable should a court broadly interpret "authorization." *Nosal*, 676 F.3d at 860. The court opined: "[b]asing criminal liability on violations of private computer use policies can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved. Employees who call family member from their work phones will become criminals if they send an email instead. Employees can sneak in the sports section of the New York Times to read at work, but they'd better not visit ESPN.com. And Sudoku enthusiasts should stick to the printed puzzles, because visiting www.dailysudoku.com from their work computers might give them more than enough time to hone their sudoku skills behind bars." *Id.* This Court shares the sentiment of the Court of Appeals for the Ninth Circuit in that broadly applying the CFAA "would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute." *Id*. at 857.

contrary to the plain language of the statute that governs "access" and not "use."

This Court finds that plaintiff has failed to state a claim for a violation of the CFAA because defendants' conduct, as alleged, does not claim that defendants either accessed their computers without authorization or exceeded their authorized access. Plaintiff cannot state a claim under the CFAA by transforming its employee policies which prohibited the using of the computer system for anything other than business purposes into a violation of the CFAA. Plaintiff does not claim that defendants gained admission to a computer without its approval or that they used their access to obtain information that falls outside the bounds of approved access. That defendants obtained information that could not have been used for any bona fide business purpose does not fall within the scope of exceeding authorized access if the employee is permitted to otherwise access the data.

While defendants may have misappropriated plaintiff's business information, they did not access a computer without authorization, nor did they exceed their authorized access. Plaintiff's statement that "[d]efendants lost all authority to access [its] password protected computer system the instant they undertook to do so for their own benefit or the benefit of any third person" and "[t]o the extent [d]efendants might otherwise have has any authority to access the data on [p]laintiff's password-protected computer system, the exceeded their authority by accessing such data for anything other than legitimate business purposes relating to Plaintiff's business operations" are legal conclusions couched as factual assertions properly disregarded by this Court. Compl. [ECF No. 1] at ¶¶ 20-21. The scope of the CFAA does not extend to employees who were authorized to otherwise access the data in question, but did so in bad faith or to the future detriment of his former employer because the this Court interprets the term "authorization" narrowly and finds that it does not extend to the improper use of information

validly accessed.

Accordingly, defendants' motion to dismiss plaintiff's complaint for failure to state a claim under the CFAA is granted and plaintiff's claim is dismissed with prejudice.

VI. CONCLUSION

For the foregoing reasons, defendants' motion to dismiss plaintiff's complaint is granted and plaintiff's claim for a violation of the CFAA is dismissed with prejudice. An appropriate Order follows.

Dated: March 6, 2014

/s Cynthia Reed Eddy
Cynthia Reed Eddy
United States Magistrate Judge

cc: all counsel of record