IN THE UNITED STATES DISTRICT COURT FOR THE
MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

WACHTER, INC.,	)	
	)	
Plaintiff,	)	
	)	
v.	)	NO. 3:18-cv-00488
	)	
CABLING INNOVATIONS, LLC, *et al.*,	)	JUDGE RICHARDSON
	)	
Defendants.	)	
	)	

MEMORANDUM OPINION

Plaintiff Wachter, Inc. filed this action against Defendants Brian Pitts, Megan Pitts, Josh Estes, and Cabling Innovations, LLC, asserting nine causes of action. Before the Court is Defendants' Motion to Dismiss (Doc. No. 21), supported by an accompanying brief (Doc. No. 18). Plaintiff filed a response (Doc. No. 23), and Defendants replied (Doc. No. 28). For the below-stated reasons, Defendants' motion will be granted in part and denied in part.

ALLEGED FACTS[1]

Wachter, Inc. (hereinafter "Plaintiff"), a Kansas corporation registered to do business in the state of Tennessee, is a national provider of infrastructure services, communications equipment, and technical support. (Doc. No. 1 at ¶¶ 1, 14). Plaintiff's services include on-site wired and wireless network infrastructure, telephone and structured cabling, design, installation, and electrical services. (*Id*. at ¶ 15).

On September 13, 2010, Plaintiff hired Brian Pitts as an Account Project Manager to manage multi-client complex projects in Nashville, Tennessee. (*Id*. at ¶¶ 16-17). On December 5,

[1] The cited facts are alleged in the Complaint and accepted as true for purposes of the instant motion to dismiss.

2011, Plaintiff promoted Mr. Pitts to Local Business Unit Manager. (*Id*. at ¶ 18). As Local Business Unit Manager, Mr. Pitts' responsibilities included leading, coaching, and managing Plaintiff's Nashville office; managing projects; and monitoring profits and losses for the business unit. (*Id*. at ¶ 19). On September 20, 2017, Plaintiff promoted Mr. Pitts to Local Business Account Manager and he was responsible for seeking and maintaining new customer opportunities. (*Id*. at ¶¶ 20-21). On July 22, 2013, Plaintiff hired Josh Estes as a foreman to manage projects for customers. (*Id*. at ¶¶ 23-24).

As part of their employment, Plaintiff provided Mr. Pitts and Mr. Estes with an email account and access to Plaintiff's computer system which contained certain confidential and trade secret information including, but not limited to, pricing and other financial data; customer lists; customer requirements; customer contacts; and other nonpublic business information about Plaintiff, its customers, and suppliers. (*Id*. at ¶ 26). As a condition of their employment, Mr. Pitts and Mr. Estes signed [Plaintiff's] Employee Handbook, which contains a Conflict of Interest policy that provides, in part, as follows:

> Employees have an obligation to conduct business within guidelines that prohibit actual or potential conflicts of interest. . . .
>
> An actual or potential conflict of interest occurs when an employee is in a position to influence a decision that may result in a personal gain for that employee or for a relative as a result of Wachter's business dealings. . . .
>
> Personal gain may result not only in cases where an employee or relative has a significant ownership in a firm with which [Plaintiff] does business, but also when an employee or relative receives any kickback, bribe, substantial gift, or special consideration as a result of any transaction or business dealings involving [Plaintiff].

(*Id*. at ¶ 27). The Employee Handbook also contains a confidentiality policy that provides, in part:

> No one is permitted to remove or make copies of any [of Plaintiff's] records, reports or documents without prior management approval. Disclosure of confidential information could lead to termination, as well as other possible legal action.

(*Id*. at ¶ 28).

During the course of their employment with Plaintiff, Mr. Estes and Mr. Pitts accessed their email accounts provided by Plaintiff and Plaintiff's computer system to review and obtain data for their own personal benefit and/or for the benefit of Cabling Innovations.[2] (*Id*. at ¶ 29). Mr. Pitts forwarded emails from his Plaintiff-provided email account to his personal and/or Cabling Innovations email account, Mr. Estes, and Megan Pitts (Mr. Pitts' spouse) without Plaintiff's authorization. (*Id*. at ¶¶ 9, 30-31). The following are examples of how Mr. Pitts used the information he obtained through his employment with Plaintiff to bid for/obtain work on behalf of Cabling Innovations:

- In February 2017, Mr. Pitts utilized Plaintiff's resources and confidential information to recommend contracting work with Cabling Innovations to Plaintiff's customer.

- In November 2017, Mr. and Ms. Pitts utilized Plaintiff's resources and confidential information to submit a bid to Plaintiff's customer on behalf of Cabling Innovations for work at the eMIIDS project.

- In February 2018, Mr. Pitts utilized Plaintiff's resources and confidential information to submit a bid to Plaintiff's customer on behalf of Cabling Innovations for work at the Medhost project.

- In March 2018, Mr. Pitts and Mr. Estes utilized Plaintiff's resources and confidential information to obtain and perform work for Plaintiff's customer on behalf of Cabling Innovations at the E|Spaces Chattanooga project.

- In April 2018, Mr. Pitts utilized Plaintiff's confidential information to submit a bid to Plaintiff's customer on behalf of Cabling Innovations for work at the MDF project.

[2] Cabling Innovations, LLC, is a limited liability company organized under the laws of the State of Tennessee with a principal place of business in Brentwood, Tennessee. (*Id*. at ¶ 5). Mr. Pitts is a part owner and employee of Cabling Innovations. Mr. Estes and Ms. Pitts are also employees of Cabling Innovations. (*Id*. at ¶¶ 6-9).

(*Id*. at ¶ 32). The work obtained from Plaintiff's customers would have not been obtained by Cabling Innovations but for Mr. Pitts' sharing of Plaintiff's confidential information. (*Id*. at ¶ 33). Also during Mr. Pitts' employment, he expensed to Plaintiff entertainment expenses he claimed were for the benefit of Plaintiff's customer, when the expenses were actually for the benefit of Mr. Pitts and/or Cabling Innovations. (*Id*. at ¶ 34). Plaintiff terminated Mr. Pitts on April 27, 2018. (Id. at ¶ 22). Mr. Estes resigned on February 2, 2018. (*Id*. at ¶ 25).

LEGAL STANDARD

For purposes of a motion to dismiss, the Court must take all of the factual allegations in the complaint as true as the Court has done above. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face. *Id*. 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*. Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice. *Id*. When there are well-pleaded factual allegations, a court should assume their veracity and then determine whether they plausibly give rise to an entitlement to relief. *Id*. at 679. A legal conclusion, including one couched as a factual allegation, need not be accepted as true on a motion to dismiss, nor are mere recitations of the elements of a cause of action sufficient. *Id*. at 678; *Fritz v. Charter Twp. of Comstock*, 592 F.3d 718, 722 (6th Cir. 2010); *Abriq v. Hall*, 295 F. Supp. 3d 874, 877 (M.D. Tenn. 2018). Moreover, factual allegations that are merely *consistent* with the defendant's liability do not satisfy the claimant's burden, as mere consistency does not establish *plausibility* of entitlement to relief even if it supports the *possibility* of relief. *Iqbal*, 556 U.S. at 678.

In determining whether a complaint is sufficient under the standards of *Iqbal* and its predecessor and complementary case, *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), it may be appropriate to "begin [the] analysis by identifying the allegations in the complaint that are not entitled to the assumption of truth." *Iqbal*, 556 U.S. at 680. Identifying and setting aside such allegations is crucial, because they simply do not count toward the plaintiff's goal of showing plausibility of entitlement to relief. As suggested above, such allegations include "bare assertions," formulaic recitation of the elements, and "conclusory" or "bald" allegations. *Id*. at 681. The question is whether the remaining allegations—factual allegations, *i.e.*, allegations of factual matter—plausibly suggest an entitlement to relief. *Id*. If not, the pleading fails to meet the standard of Fed. R. Civ. P. 8 and thus must be dismissed pursuant to Rule 12(b)(6). *Id*. at 683.

ANALYSIS

I. Count I: Violations of the Computer Fraud and Abuse Act (against Mr. Pitts, Mr. Estes, and Cabling Innovations)

In Count I, Plaintiff alleges the action of Mr. Pitts, Mr. Estes, and Cabling Innovations are violations of the Computer Fraud and Abuse Act ("CFAA"). 18 U.S.C. § 1030, *et seq*. Although the CFAA is primarily a criminal statute, it also permits "[a]ny person who suffers damage or loss by reason of a violation of this section [to] maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

Plaintiff asserts these Defendants violated 18 U.S.C. § 1030(a)(2)(C), which prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer"; and Section (a)(5)(A) and (a)(5)(B), which provides for liability on the part of any person who:

> (A) 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;

> (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage;

18 U.S.C. § 1030(a)(5). The foregoing sections of the CFAA describe two types of claims: "access" claims and "transmission" claims. Such claims require that Defendants' access or transmission, respectively, of Plaintiff's data be *without authorization*. *ReMedPar, Inc. v. AllParts Med., LLC*, 683 F. Supp. 2d 605, 609 (M.D. Tenn. 2010) ("Thus, for all civil claims under the CFAA, a plaintiff must show that the defendant's access to the protected computer was either 'without authorization' or that it 'exceed[ed] authorized access.'" (citation omitted)). Defendants contend Plaintiff's CFAA claim fails because Plaintiff has not pled that Defendants accessed a computer without authorization.

i. Without Authorization/Exceeds Authorized Access

Defendants argue that, even when the factual allegations regarding the CFAA are accepted as true, these facts do not give rise to an entitlement to relief because Plaintiff granted Mr. Pitts and Mr. Estes computer access.

In response, Plaintiff correctly argues that the CFAA does not expressly define the term "without authorization" and *some* courts have "found that an employee may access an employer's computer 'without authorization' where it utilizes the computer to access confidential or proprietary information that he has permission to access, but then uses that information in a manner that is inconsistent with the employer's interest." (Doc. No. 23 at 6 (citing *Frees, Inc. v. McMillan*, No. 3:06-cv-307, 2007 WL 708593, at *2 (E.D. Tenn. Mar. 5, 2007) and *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1126 (W.D. Wash. 2000))).

The Sixth Circuit has not addressed whether an employee's misuse or misappropriation of an employer's computer-accessible business information is "without authorization" when an

employer has given the employee permission to access such information. But other district courts in this circuit have adopted a narrow approach, holding that there is no violation of the CFAA if an employer has given an employee access to a computer and the employee subsequently misuses data or confidential information obtained on the computer. *See Royal Truck & Trailer Sales & Serv., Inc. v. Kraft*, No. 18-10986, 2019 WL 1112387, at *3 (E.D. Mich. Mar. 11, 2019); *see also ReMedPar, Inc.*, 683 F. Supp. 2d at 610 (no CFAA violation when defendant "had access . . . for the purpose of performing his job while he was still an employee, and for performing the tasks he undertook as an independent contractor[.]"); *Black & Decker (US), Inc. v. Smith*, 568 F. Supp. 2d 929, 935-36 (W.D. Tenn. 2008); *Am. Family Mut. Ins. Co. v. Rickman*, 554 F. Supp. 2d 766, 771 (N.D. Ohio 2008) ("The [CFAA] was not meant to cover the disloyal employee who walks off with confidential information. Rather, the statutory purpose is to punish trespassers and hackers[.]").

Although there is a split of authority on this issue, the weight of authority appears to be that there cannot be a CFAA violation where an employee has lawful access to his computer. *See Scheper v. Daniels*, No. 1:10-CV-385, 2011 WL 13228113, at *2 (S.D. Ohio June 1, 2011) (collecting cases). In *Scheper*, referring to courts that have adopted this narrow approach, the court explained:

> Generally speaking, these courts have reasoned that the according to its plain terms, the CFAA's reference to "without authorization" and "exceeds authorized access" means that the defendant did not have permission to access the information within the computer from the outset, *i.e.*, the defendant was a hacker, and that the statute was not meant to cover employees who have authorized access to the data but later misappropriate it.

Id.

"Additionally, the majority of district courts in the Sixth Circuit to address this issue have adopted the narrow approach." *Kraft*, 2019 WL 1112387, at *3 (collecting cases). The Court

agrees with the majority of district courts within the Sixth Circuit, and also adopts the narrow interpretation of the CFAA. In addition to the weight of persuasive authority in this circuit, the Court finds three points convincing.

First, as discussed above, the plain language of the statute supports this narrow interpretation. In *Black & Decker*, the Court explained:

> [T]he statute defines the term "exceeds authorized access" as "access[ing] a computer with authorization and [using] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." § 1030(e)(6). . . . [T]he plain meaning of "exceeds authorized access" is "to go beyond the access permitted." Likewise, while there is no definition for access "without authorization," the Court finds that its plain meaning is "no access authorization."

568 F. Supp. 2d at 934-35 (internal quotation marks and citations omitted).[3] The Court concurs with this analysis.

Second, although the Court recognizes the limitations on its probativeness and persuasiveness, the CFAA's legislative history supports a narrow interpretation of the CFAA. The general purpose of the CFAA "was to create a cause of action against computer hackers (*e.g.*, electronic trespassers)[,]" *Int'l Ass'n of Machinists and Aerospace Workers v. Werner–Masuda*, 390 F. Supp. 2d 479, 495-96 (D. Md. 2005) (citation omitted), as well as to protect computer owners against trespass. *Black & Decker*, 568 F. Supp. 2d at 935-36. In 1986, "Congress amended the CFAA to substitute the phrase 'exceeds authorized access' for the phrase 'or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend.'" *Werner-Masuda*, 390 F. Supp. 2d at 499 n. 12 (quoting S. Rep. No. 99–432, at 9 (1986)). The intent of enacting this amendment was to "eliminate coverage

[3] In *Black & Decker*, the Court went on to hold that the defendant, who did not have permission to misuse the plaintiff's data by sharing it with a competitor, did have permission to access the plaintiff's network. 568 F. Supp. 2d at 935-36. Therefore, the defendant's alleged conduct did not fall within the plain meaning of the statute, and the court dismissed the claim. *Id.*

for authorized access that aims at purposes to which such authorization does not extend, thereby remov[ing] from the sweep of the statute one of the murkier grounds of liability, under which a [person's] access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization." *Id*.

Finally, because the CFAA is a criminal statute, the rule of lenity counsels the Court to construe the CFAA's coverage narrowly. *See Black & Decker*, 568 F. Supp. 2d at 935 (explaining that the CFAA is a criminal statute, and "even though it is being applied in a civil context, the [c]ourt must apply the rule of lenity, so that the statute is interpreted consistently"). After all, conduct supports a civil claim under the CFAA only if it falls within the statute's criminal prohibitions. And since the rule of lenity limits the conduct that falls within the criminal prohibitions, it likewise limits the conduct that will support a civil claim. Under the rule of lenity, "ambiguities are generally resolved in favor of the party accused of violating the law," *United States v. One TRW, Model M14, 7.62 Caliber Rifle*, 441 F.3d 416, 420 n. 3 (6th Cir. 2006). The narrow interpretation of the CFAA resolves any ambiguities accordingly.

Here, the well-pleaded allegations in the Complaint reveal that Mr. Pitts and Mr. Estes, "[a]s part of their employment, [were] provided [] with . . . access to [Plaintiff's] computer system which contained certain confidential and trade secret information." (Doc. No. 1 at ¶ 26). Plaintiff argues that although Mr. Pitts was authorized to access Plaintiff's computer system, Cabling Innovations was not, yet did through its owner/agent Mr. Pitts. (Doc. No. 23 at 7-8). Some courts in other circuits have held that such factual circumstances state a claim under the CFAA, against either the plaintiff's employee or the employee's subsequent employer who was in cahoots with the employee while the employee was still employed by the plaintiff. Two cases in particular are

well known for so holding: (1) *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420–21 (involving suit against employee); and (2) *Shurgard Storage Ctrs., Inc.*, 119 F. Supp. 2d at 1124 (in suit against subsequent employer, holding that employees' authority to access company computers ended when those employees surreptitiously became agents of defendant competitor and sent company's proprietary information to competitor via email). Each case relied on agency principles to hold that the plaintiff's employee lost the authorized access previously possessed when the employee ceased to be a loyal employee (agent) of the plaintiff. These holdings, however, were based on a broad view of the CFAA. Thus, as numerous courts specifically have noted, these two cases are not consistent with the narrow view. *See Lockheed Martin Corp. v. Speed*, No. 6:05–cv–1580, 2006 WL 2683058, at *6 (M.D. Fla. Aug. 1, 2006) ("In this Court's view, the plain meaning brings clarity to the picture and illuminates the straightforward intention of Congress, *i.e.*, 'without authorization' means no access authorization and 'exceeds authorized access' means to go beyond the access permitted. While *Citrin* attempts to stretch 'without authorization' to cover those with access authorization (albeit those with adverse interests), Congress did not so stipulate." (citing *Citrin*, 440 F.3d at 420-21)); *Black and Decker*, 568 F. Supp. 2d at 934-936; *Diamond Power Int'l, Inc. v. Clyde Bergemann, Inc.*, 540 F. Supp. 2d 1322, 1342-43 (N.D. Ga. 2007). Under this Court's narrow reading of the CFAA, Plaintiff's argument fails because during the relevant time period Mr. Pitts and Mr. Estes had—and did not lose—authorization to access Plaintiff's information.[4] Nor did they "exceed authorized access." Consequently, Plaintiff's CFAA claim fails as a matter of law.

[4] The Court realizes there could be an argument that a defendant like Cabling Innovations—an entity that allegedly used the plaintiff's employee as its agent while the employee was still employed with the plaintiff—can be liable under the CFAA, even if its agent personally avoids liability because he or she did not exceed his or her authorized access. However, in this case, Plaintiff does not develop this argument in the alternative. Further, the Court has searched and found no authority to support this particular argument. Therefore, the Court will dismiss this claim as to all Defendants, including Cabling Innovations.

ii. Transmission Claim

Plaintiff's CFAA transmission claim fails for the additional reason that Plaintiff did not allege Defendants knowingly transmitted information that caused damage.

In *Pulte Homes, Inc. v. Laborers' International Union of North America*, 648 F.3d 295 (6th Cir. 2011), the Sixth Circuit offered guidance on the definition of "damage" in a CFAA transmission claim. The court explained:

> Under the CFAA, any impairment to the integrity or availability of data, a program, a system, or information qualifies as damage. Because the statute includes no definition for three key terms—impairment, integrity, and availability—we look to the ordinary meanings of these words. Impairment means a deterioration or an injurious lessening or weakening. The definition of integrity includes an uncorrupted condition, an original perfect state, and soundness. And availability is the capability of being employed or made use of.

Id. at 301 (quotation marks and citations omitted).

The Complaint alleges that Mr. Pitts forwarded emails and Plaintiff's confidential information[5] from his email account with Plaintiff to his personal and/or Cabling Innovations email account, to Mr. Estes, and to Megan Pitts. This may suffice to allege transmission. But the Complaint does not adequately allege that the transmission caused any damage as defined by the CFAA. Plaintiff has not alleged, for example, that any forwarded emails or confidential information was deleted, let alone allege that any deleted information could not easily be recovered. Nor has Plaintiff alleged any other concrete facts establishing damages. Although Plaintiff's Complaint does allege "damage to the integrity of its data and system" (Doc. No. 1 at ¶ 47), this allegation is a threadbare recitation of an element of a Section (a)(5)(A) claim without

[5] The Complaint is sparse on details as to the nature and handling of the applicable emails and the confidential information. It appears, however, that Plaintiff means to allege that the forwarded emails were historical emails of some import, and that the confidential information was "forwarded" as an attachment to new emails Mr. Pitts created for the specific purpose of exporting the confidential information to himself and his alleged co-conspirators.

any factual "meat on the bones." *See Advanced Fluid Sys., Inc. v. Huber*, 28 F. Supp. 3d 306, 330-31 (M.D. Pa. 2004) ("[C]onclusory allegations, reflecting only a formulaic recitation of the [CFAA]'s [] elements, are insufficient to satisfy federal pleading requirements.").

Accordingly, Plaintiff has not adequately alleged any "damage" as defined by the CFAA. If the alleged transmissions themselves in fact were wrongful, Plaintiff's remedy (if any) must be grounded elsewhere in the law. *See SKF USA, Inc. v. Bjerkness*, 636 F. Supp. 2d 696, 721 (N.D. Ill. 2009) (holding that where the defendants transferred data to a competitor without the plaintiff's authorization, the plaintiff's losses were better addressed under state contract and trade secrets law than under the CFAA). Therefore, its transmission claim fails as a matter of law.

II. Count II: Violation of the Electronic Communications Protection Act (against all Defendants)

In Count II, Plaintiff alleges that all Defendants violated the Electronic Communications Protection Act ("ECPA"). Title I of the ECPA, which amended the Wiretap Act of 1968, imposes civil liability on any person who (1) "intentionally intercepts, endeavors to intercept, or procures any other person to intercept, any . . . electronic communication"; or who (2) either "intentionally discloses, or endeavors to disclose to any other person," or "intentionally uses, or endeavors to use the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the interception of a[n] . . . electronic communication." 18 U.S.C. §§ 2511(1) and 2520. "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

Defendants argue that this claim should be dismissed because Plaintiff failed to allege that Defendants "intercepted" any communications. According to Defendants, the mere act of forwarding, from Mr. Pitts' email account with Plaintiff, emails existing in that account—which

is all Plaintiff alleges in this context[6]—is insufficient to show Defendants "intercepted" any communications.

The Court agrees. The alleged forwarding of emails from Mr. Pitts' account did not amount to any type of "interception" as defined by the statute. *See Conte v. Newsday, Inc.*, 703 F. Supp. 2d 126, 140 (E.D.N.Y. 2010) (holding that the plaintiff failed to state a claim under the ECPA because the defendants did not intercept the emails where they "were the intended recipients of the emails and, therefore, direct parties to the communications"). Plaintiff argues that it properly alleged interception by alleging that Mr. Pitts intercepted communications meant for Plaintiff and sent that information to his personal email account, to his email accounts associated with Cabling Innovations, and to Mr. Estes, and Megan Pitts (agents or employees of Cabling Innovations). However, this argument is at odds with the actual allegations in Plaintiff's Complaint. Plaintiff alleges numerous times that any emails forwarded by Mr. Pitts were forwarded by Mr. Pitts from Mr. Pitts' email account in Plaintiff's email system. (Doc. No. 1 at ¶¶ 26, 30-31, 51-52). It is fatal to Plaintiff's claim that as far as the Complaint alleges, Mr. Pitts was an original intended recipient of the emails or otherwise properly in custody of the emails in his email account that ultimately were forwarded.

Additionally, even assuming that Plaintiff were to amend its Complaint to allege that Mr. Pitts did in fact forward emails that were never intended to be received or possessed by him, its ECPA claim would still fail. The Sixth Circuit has held "that, in order for an 'intercept' to occur for purposes of the [ECPA], the electronic communication at issue must be acquired contemporaneously with the transmission of that communication." *Luis v. Zang*, 833 F.3d 619,

[6] Plaintiff does not allege, for example, that Mr. Pitts was not an original proper recipient of those historical emails or otherwise did not properly have them in his email account. Even if it had so alleged, however, that would not have sufficed to adequately allege interception, as discussed below.

629 (6th Cir. 2016). In other words, for liability to attach, the communication must be caught "'in flight' before the communication comes to rest and ceases to be a communication." *Luis v. Zang*, 833 F.3d 619, 627–28 (6th Cir. 2016). The court explained that "the term intercept applies solely to the transfer of electronic signals. The term does not apply to the acquisition of electronic signals that are no longer being transferred." *Id*. at 627.[7]

Here, Plaintiff's complaint alleges that Mr. Pitts "forward[ed] copies of [Plaintiff's] internal emails to his own personal email account." (Doc. No. 1 at ¶ 51). Thus, at the time of forwarding, the emails had already been delivered; they never were intercepted "in flight" as required to state an ECPA claim. *Id*. at 627-28. Accordingly, Plaintiff fails to state an ECPA claim, and this claim will be dismissed.

III. Count III: Violation of the Stored Communications Act (against Mr. Pitts and Cabling Innovations)

In Count III, Plaintiff alleges that Mr. Pitts and Cabling Innovation's actions constitute violations of the Stored Communications Act, 18 U.S.C. § 2701 ("SCA"). A defendant is liable under the SCA when he or she "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such a system." 18 U.S.C. § 2701(a). Plaintiff alleges that its email server system and the components of Plaintiff's computer network are a "facility" under the SCA, and that therefore these Defendants are liable for obtaining

[7] Prior to the decision in *Luis*, many courts in this circuit had held likewise. *Fredrick v. Oldham Cnty. Fiscal Court*, No. 3:08-CV-401-H, 2010 WL 2572815, at *3 (W.D. Ky. June 23, 2010) ("[T]o bring a Section 2511(1)(a) claim, [the plaintiff] must assert that [the defendants] intercepted the original e-mail transmission, rather than accessing it later while stored in his e-mail account or on a server."); *Cardinal Health*, 582 F. Supp. 2d at 980 (agreeing with "Third, Fifth, Ninth, and Eleventh Circuits[, which] all agree that, for a communication to be 'intercepted' under the FWA, that communication must be acquired during the "flight" of the communication."); *Bailey v. Bailey*, No. 07-11672, 2008 WL 324156, at *5 (E.D. Mich. Feb. 6, 2008) (finding that ECPA claim failed as a matter of law where the e-mails at issue were not obtained contemporaneously with transmission).

this information. (Doc. No. 1 at ¶ 57). Defendants argue Plaintiff's claim should be dismissed because (1) the "user exception" to the SCA applies; and (2) Defendants did not access a "facility" as defined by the SCA. (Doc. No. 18 at 15-16).

The SCA "does not prohibit the disclosure or use of information gained without authorization . . . Rather, section 2701(a) prohibits the intentional unauthorized access of an electronic communications service." *Cardinal Health 414, Inc. v. Adams*, 582 F. Supp. 2d 967, 976 (M.D. Tenn. 2008) (J. Trauger) (quoting *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F. Supp. 2d 817, 820 (E.D. Mich. 2000)). Therefore, disclosure of information obtained by "users" that are authorized to obtain such information does not give rise to liability under the SCA; this is known as the "user exception." *Id*. Plaintiff argues that the user exception does not apply because the emails were accessed not by Mr. Pitts as an employee of Plaintiff, but rather by Cabling Innovations (through its owner, Mr. Pitts), which was not granted access to Mr. Pitts' email account associated with Plaintiff or to Plaintiff's confidential information. (Doc. No. 18 at 12).

In support, Plaintiff cites *Cardinal Health*, where the court found the "conduct of [a] former employee tantamount to trespassing and actionable under the SCA." (Doc. No. 23 at 12 (citing *Cardinal Health*, 582 F. Supp. 2d at 976)). But the Court finds *Cardinal Health* distinguishable from the case at hand. In that case, the court found a former employee violated the SCA as a matter of law when he used the log-in information *of another person*, a former co-worker, to spy on the activities of his former company; thus, the plaintiff did not have authorization himself to access the information. That is vastly different from the situation here, where Plaintiff specifically alleges that Mr. Pitts "was authorized to access and use [Plaintiff's] email system" and there is no allegation that Mr. Pitts used anyone else's log-in information. (Doc. No. 1 at ¶ 58).

The Court finds the factual allegations here are more analogous to *Sherman*. 94 F. Supp. 2d at 817. In *Sherman,* a former employee was accused of violating the SCA, by continuing to use, after he left employment, his personal access code to log on to the same business account (which was hosted by a third party) that he had used while still employed. 94 F. Supp. 2d at 821. The former employee used the computer access code to gain the plaintiff's sales data and thereafter provide that information to a competitor. *Id*. at 819. The court found that the plaintiff failed to state an SCA claim because the Complaint lacked any allegations of the former employees' "clear[ ] and [ ] explicit restriction on access [occasioned by his departure from his employer]." *Id*. at 821. Like in *Sherman*, Plaintiff's Complaint does not contain any allegations the Mr. Pitts accessed his email account provided by Plaintiff or any of Plaintiff's information at any time without authority, and in fact, alleges the opposite. Accordingly, based on the allegations in the Complaint, Mr. Pitts' act of forwarding the emails did not exceed his authority to lawful access.

In response, Plaintiff's concede that "if all that occurred here was that [Mr.] Pitts accessed his email [from his account with Plaintiff] to forward those emails to his personal email account, there would be no liability." (Doc. No. 23 at 12). Plaintiff argues, however, that it was not Mr. Pitts accessing his emails; instead, it was Cabling Innovations, through its owner (Mr. Pitts), who was accessing emails. (*Id*.). The court in *Cardinal Health* rejected a somewhat similar argument. There, the plaintiff argued that even though the former employee was authorized to access his email account with his former employer, the corporation to which the plaintiff sent the information was not granted access. Thus, according to the plaintiff, the corporation (working through the plaintiff's former employee), in an unauthorized manner, intentionally made use of and "accessed" the computer.

The court rejected this "strained reading" of the term "access" and reasoned that "[c]onduct such as receiving unauthorized materials and discussing those materials implicates 'disclosure' and 'use' of those materials, and it is settled that the SCA does not punish 'disclosing' and 'using' the unauthorized materials." *Id*. at 978. The court explained that its reading of the term "access" was not "unreasonably narrow," as the plaintiff argued, "but [was] the logical interpretation of a large body of case law that all points in the same direction." *Id*. The Court finds the reasoning in *Cardinal Health* convincing. The fact that Mr. Pitts partly owned Cabling Innovations does not change the fact that he had valid access to Plaintiff's information even if he would have lost that access had Plaintiff known that he allegedly sought to use it to benefit Cabling Innovations. Accordingly, Plaintiff's SCA claim falls into the "user" exception to the SCA, and thus Plaintiff fails to state an SCA claim. *See Sun West Mortgage Co. v. Matos Flores*, No. 15-1082, 2016 WL 1030074, at *5 (D.P.R. Mar. 10, 2016) ("The mere assertion that [a former employee] sent [his previous employer's] confidential information and trade secrets to his personal e-mail account, without more, does not satisfy the Plaintiff's pleading requirements under *Twombly* and *Iqbal* [for purposes of stating a claim under the SCA]."). Accordingly, Count III will be dismissed.

IV. Jurisdiction Over State Law Claims

In the event the Court dismisses all of Plaintiff's federal claims (which it will, as indicated above), Defendants ask the court to dismiss the remaining (state law) claims pursuant to this Court's discretion under 28 U.S.C. § 1367.

The Court's jurisdiction over the state law claims is premised on supplemental jurisdiction. *See* 28 U.S.C. § 1367(a). "A district court may decline to exercise supplemental jurisdiction over state law claims if it has dismissed all claims over which it had original jurisdiction." *Novak v. MetroHealth Med. Ctr.*, 503 F.3d 572, 583 (6th Cir. 2007) (citing 28 U.S.C. § 1367(c)(3)). When

deciding to exercise supplemental jurisdiction, a court should consider the "values of judicial economy, convenience, fairness, and comity." *Gamel v. City of Cincinnati*, 625 F.3d 949, 951–52 (6th Cir. 2010) (quoting *Carnegie–Mellon Univ. v. Cohill*, 484 U.S. 343, 350 (1988)). The Court is generally inclined to refuse to exercise supplemental jurisdiction over the Plaintiff's state law claims under these circumstances. *See Musson Theatrical, Inc. v. Fed. Express Corp.*, 89 F.3d 1244, 1254–55 (6th Cir. 1996) ("When all federal claims are dismissed before trial, the balance of considerations usually will point to dismissing the state law claims[.]").

Nevertheless, in response to Defendants' Motion to Dismiss, Plaintiff asserts *for the first time* that the Court has diversity jurisdiction over the state law claims (under 28 U.S.C. § 1332) because "Plaintiff is a citizen of Kansas and each of the Defendants is a citizen of Tennessee. Given that [Plaintiff] seeks actual and punitive damages, as well as its costs and reasonable attorneys' fees, the amount in controversy clearly exceeds $75,000." (Doc. No. 23 at 13 (citing 28 U.S.C. § 1332)). But Plaintiff's Complaint asserts only that "[t]his Court has subject matter jurisdiction of this action pursuant to 28 U.S.C. § 1331 and 28 U.S.C. § 1376." (Doc. No. 1 at ¶ 10). Further, although the Complaint alleges that Plaintiff is a Kansas corporation, the Complaint does not allege the location of Plaintiff's principal place of business (and for that matter, Plaintiff's response)[8] or that the amount in controversy exceeds $75,000. Thus, the Court has no basis to conclude that diversity jurisdiction is present. *See Horton v. Liberty Mut. Ins. Co.*, 367 U.S. 348, 353 (1961) ("The general federal rule has long been to decide what the amount in controversy is from the complaint itself, unless it appears or is in some way shown that the amount in the complaint is not claimed 'in good faith.'" (citations omitted) (alterations in the original)); *Anthony*

[8] A requirement of diversity jurisdiction is that no party share citizenship with any opposing party; there must be "complete diversity." *See Peters v. Fair*, 427 F.3d 1035, 1038 (6th Cir. 2005). A corporation is a citizen of the state of its incorporation *and* a citizen of the state in which it has its principal place of business. 28 U.S.C. § 1332(c).

v. Madden, No. 3:06-cv-0739, 2007 WL 307576, at *5 (M.D. Tenn. Jan. 29, 2007) ("Allegations of citizenship, of both corporate and individual parties, must be apparent from the face of the pleadings.").

If the Court were to decline supplemental jurisdiction, Plaintiff would have an incentive to move to amend its complaint to assert diversity jurisdiction. Briefing and determination of any such motion would further delay this case—which (through no fault of the parties) has been pending for over a year and stalled while the instant motion was pending for over nine months. Thus, the Court finds it is in the interests of judicial economy, justice (especially the promptness thereof), and convenience to exercise supplemental jurisdiction over the state law claims to get this case moving. Accordingly, pursuant to 28 U.S.C. § 1367, the Court in its discretion will exercise jurisdiction over the state law claims.

V. Count IV: Breach of Fiduciary Duty (against Mr. Pitts and Mr. Estes)

Defendants argue that Plaintiff's breach of fiduciary duty claim fails as a matter of law because the Complaint does not allege that Mr. Pitts or Mr. Estes were officers or directors of Plaintiff, which, according to Defendants, is a necessary prerequisite of owing a fiduciary duty under Tennessee law.

Courts in this district have previously held that under Tennessee law, a breach of fiduciary duty claim can be brought only against a business entities' officers and directors, as opposed to mere employees. *ProductiveMD, LLC v. 4UMD, LLC*, 821 F. Supp. 2d 955, 964 (M.D. Tenn. 2011) (J. Sharp); *Weiss v. Lab. Corp. of Am. Holdings*, Nos. 3:06-cv-950, 3:06-cv-1010, 2007 WL 4365764 at *13 (M.D. Tenn. Dec. 11, 2007) (J. Echols) (citing *Efird v. Clinic of Plastic & Reconstructive Surgery, P.A.*, 147 S.W.3d 208, 220 (Tenn. Ct. App. 2003)).

In *ProductiveMD*, the counter-plaintiff moved to dismiss the counter-defendant's breach of fiduciary duty claim on the grounds that the counter-plaintiff was not an officer or director. 821 F. Supp. 2d at 964. The Court explained that although an employee (who is not an officer or director) cannot be held liable under a theory of breach of fiduciary duty, the claim was in essence a breach of a duty of loyalty claim, which can properly be asserted against an employee. *Id*. (citing *Efird*, 147 S.W.3d at 220). Thus, the court did not dismiss the claim "merely because [the counter-plaintiff] calls the duty a "fiduciary duty," since, on at least two occasions, the Tennessee Court of Appeals in *Efird* characterized the duty as "an employee's fiduciary duty of loyalty." *Id*.

The concerns present in *ProductiveMD* are not present here because the Plaintiff has brought both a breach of loyalty claim (in Count V, which Defendants have not moved to dismiss), which can be asserted against a mere employee, and a breach of fiduciary duty claim (in Count IV). As Plaintiff has plead that Mr. Pitts and Mr. Estes were employees of Plaintiff, without alleging they were officers or directors, (Doc. No. 1 at ¶¶ 1, 16, 18, 22, 23), Plaintiff's Count IV will be dismissed, while Count V may proceed.

VI. Count VI: Tortious Interference with a Business Relationship (against All Defendants)

In Count VI, Plaintiff asserts a tortious interference with a business relationship claim based on allegations that Defendants used Plaintiff's proprietary and confidential information to solicit away from Plaintiff specific existing or prospective customers.

Defendants assert that this claim, as well as several other of Plaintiff's state law claims (Count VII, for unjust enrichment and Count VIII, for conversion) are preempted by the Tennessee Uniform Trade Secrets Act ("TUTSA"), Tenn. Code Ann. § 47–25–1701 *et seq.*, which was adopted in 2000 to establish a comprehensive statutory scheme to govern the definition of trade

secrets and to protect against their misappropriation. *Hauck Mfg. Co. v. Astec Indus., Inc.*, 375 F. Supp. 2d 649, 654 (E.D. Tenn. 2004).

TUTSA preempts common law causes of action if "proof of those causes of action, in whole or in part, would constitute misappropriation of a trade secret." *Vincit Enters., Inc. v. Zimmerman*, No. 1:06-CV-57, 2006 WL 1319515, at *7 (E.D. Tenn. May 12, 2006) (citing *Hauck*, 375 F. Supp. 2d at 658); *see* Tenn. Code Ann. § 47–25–1708(a) ("Except as provided in subsection (b), this part displaces conflicting tort, restitutionary, and other law of this state providing civil remedies for misappropriation of a trade secret."). The Tennessee Supreme Court has not yet interpreted the scope of the TUTSA's displacement, but other state and federal courts have applied the "same proof" standard, under which "a claim will be preempted when it necessarily rises or falls based on whether the defendant is found to have 'misappropriated' a 'trade secret' as those two terms are defined in the [T]UTSA." *PGT Trucking, Inc. v. Jones*, No. 15-1032, 2015 WL 4094265, at *4 (W.D. Tenn. July 7, 2015) (collecting cases). Stated differently, "if proof of a non-[T]UTSA claim would also simultaneously establish a claim for misappropriation of trade secrets, it is preempted irrespective of whatever surplus elements or proof were necessary to establish it." *Hauck*, 375 F. Supp. 2d at 658 (citing *Smithfield Ham & Prod. Co. v. Portion Pac, Inc.*, 905 F. Supp. 346, 350 (E.D. Va. 1995)).

"TUTSA lists three requirements for information to be considered a trade secret: (1) the information must derive independent economic value from not being generally known, (2) others could obtain economic value from its disclosure or use, and (3) efforts have been made to maintain its secrecy." *Hamilton–Ryker Group, LLC v. Keymon*, No. W2008-936-COA-R3-CV, 2010 WL 323057, at *14 (Tenn. Ct. App. Jan. 28, 2010) (citing Tenn. Code Ann. § 47–25–1702(4)). In

Hamilton-Ryker, the Tennessee Court of Appeals explained the evolution of the definition of "trade secret" under Tennessee law:

> Under the common law, a trade secret was defined as any formula, process, pattern, device or compilation of information that is used in one's business and which gives him an opportunity to obtain an advantage over competitors who do not use it. Tennessee cases used the terms "trade secret" and "confidential information" interchangeably, holding that confidential business information such as customer lists, knowledge of the buying habits and needs of particular clients, and pricing information, was protectable only to the extent that it satisfied the definition of a trade secret.
>
> . . .
>
> [In 2000, t]he Tennessee legislature adopted the definition of "trade secrets" under the Uniform Trade Secrets Act,[9] and also adopted additions which make Tennessee's definition even broader than the definition in the Uniform Act. . . . Thus, the definition of a 'trade secret' under the Act is *sufficiently broad* to include information which at common law would have been considered [mere] confidential information.

Id. at *13 (emphasis added) (internal citation and quotation marks omitted). As the Court in *Hauck* explained, "Despite [TUTSA's] apparently limiting language displacing only 'conflicting tort, restitutionary, and other law . . . providing civil remedies for *misappropriation of a trade secret*," the [T]UTSA's preemption provision has generally been interpreted to abolish all free-standing alternative causes of action *for theft or misuse of confidential, proprietary, or otherwise secret*

[9] The TUTSA defines a "trade secret" as:

> [I]nformation, without regard to form, including, but not limited to, technical, nontechnical or financial data, a formula, pattern, compilation, program, device, method, technique, process, or plan that:
>
> > (A) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use; and
> >
> > (B) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Tenn. Code Ann. § 47-25-1702(4).

information falling short of trade secret status (*e.g.*, idea misappropriation, information piracy, theft of commercial information, etc.)." *Hauck*, 375 F. Supp. 2d at 655 (E.D. Tenn. 2004). Therefore, the TUTSA preempts claims of theft of an entity's confidential and proprietary information even if the information is not labeled in the Complaint as a "trade secret".[10]

In Count VI, Plaintiff alleges that "*[b]y using proprietary and confidential information* of [Plaintiff], [Defendants] intentionally and improperly interfered with [Plaintiff's] business relationship with respect to specific customers and/or prospective customers by contacting them to solicit their services away from [Plaintiff]." (Doc. No. 1 at ¶ 78) (emphasis added). Elsewhere in the Complaint, Plaintiff identifies the confidential information Mr. Pitts and Mr. Estes had access to as "confidential and *trade secret* information including, but not limited to, pricing and other financial data; customer lists, customer requirements and customer contacts; and other nonpublic business information about [Plaintiff], its customers, and suppliers." (*Id*. at ¶ 26(b)) (emphasis added). Thus, the gravamen of Plaintiff's tortious interference claim rests on the appropriation of confidential information that would be considered a "trade secret" under the TUTSA.[11] *See Hauck*, 375 F. Supp. 2d at 658 ("[P]laintiffs alleging theft or misuse of their ideas,

[10] Further, if the claim did not classify as a "trade secret" under TUTSA, then the claim would not be cognizable because Plaintiff would have no legally cognizable right in the information. "If the information is a trade secret, the plaintiff's claim is preempted; if not, the plaintiff has no legal interest upon which to base his or her claim. Either way, the claim is not cognizable. *Id*. at 656; *see also BioCore, Inc. v. Khosrowshahi*, 96 F. Supp. 2d 1221, 1238 (D. Kan. 2000) ("Even if confidential information can be something less than a trade secret, it must at least be a trade secret to give its owner a property right in it." (decided under Kansas's version of the Uniform Trade Secrets Act and cited approvingly by *Hauck*)).

[11] Plaintiff argues that "to the extent there is any recitation of facts to establish a TUTSA claim might be appropriate in that a use of confidential information is alleged, no preemption exists to the extent [Plaintiff] offers additional independent facts in support of its common-law claims that satisfy the elements of those claims." (Doc. No. 23 at 15). In support, Plaintiff cites *Alvion Properties, Inv. v. Weber*, No. 3:08-0866, 2012 WL 4903678, at *2 (M.D. Tenn. Oct. 15, 2012), where the court held that Plaintiff's various tort claims were not preempted because misappropriation of confidential information was not the "gravamen" of the claims. The court reasoned that "although the assets of Alvion [] are alleged to include certain trade secrets and proprietary information," the primary asset [alleged to be appropriated] consists of something in excess of 4,500 acres of undeveloped coal reserves[.]" *Id*. at *2. The court expressly distinguished *Cardinal Health* on this basis. *Id.* Here, the Complaint contains no such similar allegation of resources *other than* Plaintiff's confidential and proprietary information being misused or appropriated by Defendants;

data, or other commercially valuable information are confined to the single cause of action provided by the [T]UTSA."); *see also J.T. Shannon Lumber Co. v. Barrett*, No. 2:07-CV-2847-JPM-CGC, 2010 WL 3069818, at *12 (W.D. Tenn. Aug. 4, 2010) (finding the plaintiff's tortious inference with a contract claim preempted in part by TUTSA because "the alleged harm [] relate[s] exclusively to the disclosure of confidential or proprietary information."). Accordingly, the Court finds Count VI is preempted by TUTSA and it will be dismissed.[12]

VII. Count VII: Unjust Enrichment (against all Defendants)

In Count VIII, Plaintiff asserts a claim for unjust enrichment. Unfortunately for Plaintiff, such cause of action cannot be based on just any set of circumstances where the defendants were "enriched" in a way that was "unjust." The cause of action, properly understood, is much more specific than that. Unjust enrichment is a quasi-contractual theory or is a contract implied-in-law in which a court may impose a contractual obligation where one does not exist. *Whitehaven Cmty. Baptist Church v. Holloway*, 973 S.W.2d 592, 596 (Tenn. 1998) (citing *Paschall's, Inc. v. Dozier*, 407 S.W.2d 150, 154–55 (1966)). "A contractual obligation under an unjust enrichment theory will be imposed when: (1) no contract exists between the parties or, if one exist, it has become unenforceable or invalid; and (2) the defendant will be unjustly enriched absent a quasi-contractual obligation." *B & L Corp. v. Thomas and Thorngren, Inc.*, 162 S.W.3d 189, 217-18 (Tenn. Ct. App. 2004) (citation omitted).

---

beyond such misuse and misappropriation, it alleges nothing wrongful in Defendants' interference with Plaintiff. Thus, just as *Alvion* is distinguishable from *Cardinal Health*, it is distinguishable from the present case, thus dooming Plaintiff's argument. The Complaint could be construed additionally to allege Mr. Pitts and Mr. Estes' misuse of their positions as a means of interference, but Count VI is in no way grounded on misuse of position, and Plaintiff doesn't argue otherwise.

[12] Defendants also argue the tortious interference with a business relationship claim fails because: (1) the "competitor's exception" applies; thus, Plaintiff cannot demonstrate improper motive, which is required to state a claim for tortious interference with a business relationship, as a matter of law; and (2) the allegations in the Complaint fail to meet the *Twombly*/*Iqbal* pleading standard. (Doc. No. 18 at 17-18, 20). The Court finds it unnecessary to reach these arguments because the tortious interference with a business relationship claim is preempted by TUTSA.

A Tennessee court, when examining facts somewhat similar to those here, explained that it was

> unaware of any case applying an unjust enrichment theory of recovery under circumstances similar to those in the case at bar. Quasi-contractual theory of recovery involves *the willing conferring of a benefit by one party* to the other and is contraindicated when the benefit alleged is involuntarily conferred. Further, under the circumstances of this case, any losses proven to have been suffered as a result of the defendants participation in a covert scheme to establish a competing business . . . will be compensated via an award on plaintiff's breach of fiduciary duty claim.

B & L Corp., 162 S.W.3d at 217-18 (emphasis added). Plaintiff alleges that as a result of Defendants' "misconduct," they "have been unjustly enriched through the continued possession of [Plaintiff's] confidential information[.]" (Doc. No. 1 at ¶ 83). It does not allege that Plaintiff *willingly* conferred such a benefit, and the entire gist of the Complaint is that Plaintiff in no way did so. Thus, the unjust enrichment claim fails as a matter of law. Further, insofar as this claim relies on the conversion of confidential information, it is preempted by TUTSA. Count VII will be dismissed.

VIII. Count VIII: Conversion (against all Defendants)

In Count VIII, Plaintiff alleges that Defendants "intentionally exercised wrongful dominion or control over [Plaintiff's] property—to wit, the information regarding [Plaintiff's] customers to which they only had access to by virtue of [Mr. Pitts and Mr. Estes's] prior status as employees [of Plaintiff]." (Doc. No. 1 at ¶ 87). Plaintiff's conversion claims fails as a matter of law because Tennessee law does not recognize an action for the conversion of intellectual property, *Corp. Catering, Inc. v. Corp. Catering, Etc.*, No. M1997-230-COA-R3-CV, 2001 WL 266041, at *5 (Tenn. Ct. App. Mar. 20, 2001), or intangible property (such as an interest in business relationships with customers). *B & L Corp. v. Thomas & Thorngren, Inc.*, 917 S.W.2d 674, 679-80 (Tenn. Ct. App. 1995); *see also Ralph v. Pipkin*, 183 S.W.3d 362, 368 (Tenn. Ct. App. 2005).

Further, as Plaintiff's conversion claim relies solely on the conversion of "confidential information" it is preempted by TUTSA. Accordingly, Count VIII will be dismissed.

IX. Count IX: Civil Conspiracy (against all Defendants)

A civil conspiracy is defined as:

> a combination of two or more persons who, each having the intent and knowledge of the other's intent, accomplish by concert an unlawful purpose, or accomplish a lawful purpose by unlawful means, which results in damage to the plaintiff.

Lane v. Becker, 334 S.W.3d 756, 763 (Tenn. Ct. App. 2010) (quoting *Trau-Med of America, Inc. v. Allstate Ins. Co.*, 71 S.W.3d 691, 703 (Tenn. 2002)). The elements of a civil conspiracy include "'common design, concert of action, and an overt act.'" *Knott's Wholesale Foods, Inc. v. Azbell*, No. 01A-01-9510-CH-459, 1996 WL 697943, at *5 (quoting *Kirksey v. Overton Pub, Inc.*, 739 S.W.2d 230, 236 (Tenn. Ct. App. 1987)). To be liable under a theory of civil conspiracy, one or more Defendants must be liable for an underlying tort that was committed pursuant to the conspiracy. *Lane*, 334 S.W.3d at 763 (citing *Watson's Carpet & Floor Coverings, Inc. v. McCormick*, 247 S.W.3d 169, 180 (Tenn. Ct. App. 2007)). There must be a concerted effort by the defendants to cause harm to the plaintiff, and the plaintiff must, in fact, suffer harm as a result of the defendants' efforts. *Azbell*, 1996 WL 697943, at *5 (citing *Kirksey*, 739 S.W.2d at 236).

Defendant did not move to dismiss the breach of the duty of loyalty claim against Mr. Pitts and Mr. Estes.[13] Thus, there is a surviving underlying claim to which the civil conspiracy theory can attach. *PNC Multifamily Capital Inst. Fund XXVI Ltd. P'ship v. Bluff City Cmty. Dev. Corp.*, 387 S.W.3d 525, 557 (Tenn. Ct. App. 2012) (explaining that under Tennessee law, a civil conspiracy claim "requires an underlying predicate tort allegedly committed pursuant to the conspiracy."). Plaintiff alleges that during Mr. Pitts "employment . . . [he] forwarded emails and

[13] The Court does not mean to suggest that Defendants should have done so or that any such motion would have been successful.

[Plaintiff's] confidential information from his [] email account to Mr. Estes and/or Megan Pitts without authorization from [Plaintiff]" and Megan Pitts and/or Mr. Estes "received and use confidential [Plaintiff] information from Brian Pitts for [their] and/or Cabling Innovations benefit." (Doc. No. 1 at ¶¶ 31, 35-36). These allegations demonstrate that *all* Defendants participated in a concerted effort to cause harm to Plaintiff, although Ms. Pitts and Cabling Innovations are not liable for the underlying tort. *See Azbell*, 1996 WL 697943, at *5 (citing *Kirksey*, 739 S.W.2d at 236). Accordingly, Plaintiff's claim for civil conspiracy will not be dismissed. But this does not mean that Plaintiff has a cause of action for civil conspiracy; under Tennessee law, there is no such thing. *E.g. Campbell v. BNSF Ry. Co.*, 600 F.3d 667, 677 (6th Cir. 2010); *Stanfill v. Hardney*, No. M2004-02768-COA-R3-CV, 2007 WL 2827498, at *7-8 (Tenn. Ct. App. Sept. 27, 2007); *Levy v. Franks*, 159 S.W.3d 66, 82 (Tenn. Ct. App. 2004). Rather, it means that Plaintiff may proceed under the theory that, as civil conspirators, Mr. Pitts' and Mr. Estes' two co-conspirators are liable on Count V[14] to the same extent Mr. Pitts and Mr. Estes are as the actual tortfeasors, and that each conspirator is liable for all damages occasioned by the actions of any of the conspirators. *Trau-Med of Am., Inc.*, 71 S.W.3d at 703 ("Upon a finding of conspiracy, each conspirator is liable for the damages resulting from the wrongful acts of all co-conspirators in carrying out the common scheme.").

X. Motion to Amend

Buried in Plaintiff's response to Defendants' Motion to Dismiss is a request for leave to amend its Complaint "as to remedy any deficiency" should the Court grant Defendants' Motion to Dismiss. (Doc. No. 23 at 2, 23). Plaintiff emphasizes that the Federal Rules of Civil Procedure

[14] The civil conspiracy theory is inapplicable—and thus useless to Plaintiff—as to any underlying cause of action that (unlike Count V) is invalid. *See Campbell*, 600 F.3d at 677 (noting that a civil conspiracy claim fails to the extent wrongful conduct is not actionable).

state that a court should grant leave to amend a complaint "when justice so requires." Fed. R. Civ. P. 15(a)(2).

The Sixth Circuit has held that a bare request to amend a complaint in lieu of a properly filed motion is not proper under Rule 15(a). *PR Diamonds, Inc. v. Chandler*, 364 F.3d 671, 699 (6th Cir. 2004). Further, this Court's Local Rules requires such motions to "describe the substance of the amendments sought" and "include as an exhibit the signed proposed amended pleading[.]" LR 15.01(a)(1); *see also PR Diamonds*, 364 F.3d at 699 ("Failure to file a motion to amend [that complies with] the local rules governing practice before the district court," is sufficient grounds for not allowing a complaint to be amended.). "Plaintiffs [are] not entitled to an advisory opinion from the Court informing them of the deficiencies of the complaint and then an opportunity to cure those deficiencies." *PR Diamonds*, 364 F.3d at 699 (quoting *Begala v. PNC Bank, Ohio, N.A.*, 214 F.3d 776, 784 (6th Cir. 2000)); *see also Beydoun v. Sessions*, No. 16-2168/2406, 2017 WL 4001336, at *7 (6th Cir. Sept. 12, 2017). If Plaintiff had filed a proper motion to amend the Complaint prior to the Court's consideration of Defendants' Motion to Dismiss, "the Court would have considered the motion to dismiss in light of the proposed amendments to the complaint." *Begala*, 214 F.3d at 784. Since Plaintiff did not do so, Defendants are "entitled to a review of the complaint as filed pursuant to Rule 12(b)(6)." *Id*. Thus, Plaintiff will not be granted leave to amend based on its alternative request in its brief for such leave.

CONCLUSION

Plaintiff asserts a large and somewhat complex array of claims based on an alleged fact pattern that actually is quite straightforward: two of Plaintiff's employees used their access to Plaintiff's proprietary and confidential information to misappropriate Plaintiff's information and provide it to a competitor of Plaintiff, who was conspiring with those employees (and one or

person) to commit this misconduct in order to "steal" customers from Plaintiff. Allegations like these can and often do support certain claims against the employees, as well as the extension of liability on such claims to Plaintiff's competitor (and in this case another alleged co-conspirator) under a conspiracy theory. What they do not do is support anywhere near the nine separate causes of action asserted by Plaintiff. As this Memorandum Opinion reflects, the full array of claims asserted by Plaintiff is neither appropriate nor, truth be told, necessary for Plaintiff to seek substantial relief based on the alleged misconduct.

For the foregoing reasons, Defendants' Motion to Dismiss (Doc. No. 21) will be **GRANTED** in part and **DENIED** in part. Count V (breach of the duty of loyalty) against Brian Pitts and Josh Estes will proceed. In addition, although it is not an independent cause of action, Plaintiff may proceed under Count IX (civil conspiracy) as a basis to: (1) assert the liability of Defendants Megan Pitts and Cabling Innovations, LLC based on the alleged underlying torts of Defendants Brian Pitts and Josh Estes asserted in Count V; and (2) seek against each of the four Defendants all damages occasioned by any acts of any of them in furtherance of the alleged civil conspiracy. All of Plaintiff's remaining claims (Count I, II, III, IV, VI, VII, and VIII) will be **DISMISSED**.

An appropriate Order will be entered.

Eli Richardson

ELI RICHARDSON
UNITED STATES DISTRICT JUDGE