

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

VURV TECHNOLOGY LLC,

Plaintiff,

v.

1:08-cv-3442-WSD

**KENEXA CORPORATION;
KENEXA TECHNOLOGY, INC.;;
DAWN CLEMENTS; and
MICHELE SWEARINGEN,**

Defendants.

OPINION AND ORDER

This matter is before the Court on Defendants Kenexa Corporation, Kenexa Technology, Inc. (together “Kenexa”), Dawn Clements, and Michele Swearingen’s (collectively “Defendants”) Motion to Dismiss Counts 2-5 and 7-10 [16].

I. BACKGROUND

Plaintiff Vurv Technology LLC (“Plaintiff” or “Vurv”) provides human resources software and support to human resources organizations. Complaint at ¶ 14. Defendants Dawn Clements and Michele Swearingen began working for Vurv in February 2002. *Id.* at ¶ 15. On January 31, 2003, Clements and Swearingen signed confidentiality agreements (“Confidentiality Agreement”) as a

condition of their employment. Id. Under the agreements, Clements and Swearingen promised to hold Vurv's confidential and proprietary information in strictest confidence and not to disclose the information to any person, firm, or corporation without prior written authorization. Id. They also agreed that they could be held strictly liable for any abuses of Vurv's computer systems, including (i) accessing Vurv's computer system, network, or data to wrongfully obtain or otherwise use Vurv's data, and, (ii) taking, copying, or making use of any data or supporting documentation from Vurv's computer systems without permission. Id. at ¶ 16. The confidentiality agreements required Clements and Swearingen, when they left Vurv, to deliver to Vurv – and not keep or deliver to anyone else – “any and all materials, data, notes, reports, lists, documents or other property, including, but not limited to, Confidential information, or reproductions of any aforementioned items, belonging to the Company [Vurv], its successors or assigns, employees, clients, consultants, vendors, licensees, or other's with interest in the Company.” Id. (quoting Confidentiality Agreement at ¶ 5).

In May 2008, Taleo Corporation (“Taleo”) announced that it was acquiring Vurv. Declaration of Christopher Lee at ¶ 5. On or about June 16, 2008, Vurv offered Clements and Swearingen to continue their employment after Vurv was acquired by Taleo, giving them until June 23, 2008, to accept or decline the offer.

Id. Clements and Swearingen did not accept the offer of employment. Id. They were offered, and at some point accepted, jobs at Kenexa. Compl. at ¶ 17. Kenexa competes with Vurv in the development and sale of human resources software.

Clements' and Swearingen's last day of employment with Vurv was July 1, 2008. Declaration of Michelle Stark at ¶ 3. The same day, Vurv mailed to Clements and Swearingen shipping boxes for their use to return the computers that had been issued to them by Vurv. Id. Vurv received the computer issued to Swearingen on July 8, 2008. On July 20, 2008, Vurv received the computer it had issued to Clements. Id. On August 11, 2008, Vurv sent these computers to be examined forensically. Id. at ¶ 4. The results of the examination provides, at least in part, the basis on which Plaintiff asserts its claims in this litigation.

Plaintiff claims that while Clements and Swearingen were still employed at Vurv, Kenexa made employment offers to Clements and Swearingen and conspired with them to improperly access, copy, and provide to Kenexa a copy Vurv's confidential and proprietary information, using the company computers Vurv had issued to them. Compl. at ¶ 25. Plaintiff specifically claims that Clements and Swearingen, after they accepted employment offers from Kenexa, but before they left Vurv, as well as after their employment with Vurv terminated, attached external hard drives to their Vurv-issued computers and accessed, copied, and stole

large groups of documents, folders, and .zip files, which included Vurv's business strategy documents, confidential drafts of Vurv's consolidated financial statements, return-on-investment analyses, pricing proposals, and customer-specific information. Id. at ¶¶ 34-37. Plaintiff alleges that when Clements and Swearingen returned their Vurv computers, they did not provide Vurv with external hard drives or other backup media onto which Vurv claims its information was copied. Id. at ¶¶ 35, 37.

Plaintiff asserts against Defendants thirteen separate counts, based on Defendants alleged wrongful conduct involving Plaintiffs claimed confidential and proprietary information. The counts are: 1) breach of contract (against Clements and Swearingen); 2) computer theft (against all Defendants); 3) conspiracy to commit computer theft (against all Defendants); 4) computer trespass (against all Defendants); 5) conspiracy to commit computer trespass (against all Defendants); 6) misappropriation of trade secrets (against all Defendants); 7) conspiracy to misappropriate trade secrets (against all Defendants); 8) violation of the Computer Fraud and Abuse Act (against all Defendants); 9) conspiracy to violate the Computer Fraud and Abuse Act (against all Defendants); 10) tortious interference with contract (against Kenexa); 11) injunctive relief (against all Defendants); 12)

punitive damages (against all Defendants); and 13) attorneys' fees and expenses of litigation (against all Defendants).

On December 12, 2008, Defendants filed their Motion to Dismiss Counts 2-5 and 7-10 of the Complaint.

II. DISCUSSION

A. The Standard on a Motion to Dismiss

The law governing motions to dismiss made pursuant to Rule 12(b)(6) is well-settled. Dismissal of a complaint is appropriate “when, on the basis of a dispositive issue of law, no construction of the factual allegations will support the cause of action.” Marshall County Bd. of Educ. v. Marshall County Gas Dist., 992 F.2d 1171, 1174 (11th Cir. 1993). The court accepts the plaintiff's allegations as true, Hishon v. King & Spalding, 467 U.S. 69, 73 (1984), and considers the allegations in the complaint in the light most favorable to the plaintiff. Watts v. Fla. Int'l Univ., 495 F.3d 1289, 1295 (11th Cir. 2007). Ultimately, the complaint is required to contain “enough facts to state a claim to relief that is plausible on its face.” Bell Atl. Corp. v. Twombly, 550 U.S. 544, 127 S. Ct. 1955, 1974 (2007). “To survive a motion to dismiss, plaintiffs must do more than merely state legal conclusions; they are required to allege some specific factual bases for those conclusions or face dismissal of their claims.” Jackson v. BellSouth Telecomms.,

372 F.3d 1250, 1263 (11th Cir. 2004) (“[C]onclusory allegations, unwarranted deductions of facts or legal conclusions masquerading as facts will not prevent dismissal.”) (citations omitted).

B. Analysis

1. *Georgia Computer Systems Protection Act (Counts 2-5)*

Defendants move to dismiss the claims asserted under the Georgia Computer Systems Protection Act, O.C.G.A. § 16-9-90 et seq. (“GCSPA”). Defendants argue that the allegations of computer theft (Count 2), conspiracy to commit computer theft (Count 3), computer trespass (Count 4), and conspiracy to commit computer trespass (Count 5) fail to state a claim because they do not allege any computer “use” that violates the Act.

The GCSPA is a criminal statute that provides for civil liability and a civil remedy. O.C.G.A. § 16-9-93(g). The GCSPA imposes liability for computer theft where a:

person [] uses a computer or computer network with knowledge that such use is without authority and with intention of:

- (1) Taking or appropriating any property of another, whether or not with the intention of depriving the owner of possession;
- (2) Obtaining property by any deceitful means or artful practice; or

- (3) Converting property to such person's use in violation of an agreement or other known legal obligation to make a specified application or disposition of such property[.]

O.C.G.A. § 16-9-93(a). The GCSPA also imposes liability for computer trespass

where a:

person [] uses a computer or computer network with knowledge that such use is without authority and with the intention of:

- (1) Deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer network;
- (2) Obstructing, interrupting, or in any way interfering with the use of a computer program or data; or
- (3) Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of how long the alteration, damage, or malfunction persists[.]

O.C.G.A. § 16-9-93(b).

O.C.G.A. § 16-9-92 lists the definitions of certain terms found in the statute.

The entry for "use" provides:

"Use" *includes* causing or attempting to cause:

- (A) A computer or computer network to perform or to stop performing computer operations;
- (B) The obstruction, interruption, malfunction, or denial of the use of a computer, computer network, computer program, or data; or
- (C) A person to put false information into a computer.

O.C.G.A. § 16-9-92(16) (emphasis added).

a. Computer “use”

Defendants argue that Defendant did not “use” a computer or computer network in violation of § 16-9-93(a) or (b). Defendants misinterpret the statute by claiming that “use” is *defined as* “causing or attempting to cause” the listed disruptions to a computer or computer network, rather than only *including* this conduct. Defendants claim the definition of “use” restricts liability to the uses listed in the definition, and that Defendants did not engage in uses described in § 16-9-92(16). The Court disagrees. Defendants’ constricted definition defies the plain meaning of the statute.

The first step of statutory construction is to start “with the words of the statutory provision.” CBS Inc. v. PrimeTime 24 Joint Venture, 245 F.3d 1217, 1222 (11th Cir. 2001). With respect to computer theft, the statute specifically prohibits taking, appropriating, or converting the property of another. Computer trespass includes temporarily or permanently deleting or removing computer data from a computer or computer network.

Although the statute defines “use”, the definition is stated only to *include* certain conduct. Other statutory definitions in § 16-9-92 specifically limit the meaning of a term. For example, the definition of “remote computing service” states “‘remote computing service’ *means* the provision to the public of computer

storage or processing services by means of an electronic communications system.” O.C.G.A. § 16-9-92(14) (emphasis added). The definition for “use” is only stated to *include* the listed conduct, and does not limit the definition to the conduct listed. It is well-established that the term “include” is intended to provide a nonexclusive list of which the listed events are representative. See Estate of Wallace v. C.I.R., 965 F.2d 1038, 1046 (11th Cir. 1992) (“We agree that the word ‘including’ makes the list of activities [in the statute] nonexclusive.”). Limiting the definition of “use” to exclude its plain and ordinary meaning would undercut the core provision of the statute which broadly proscribes the taking, obtaining, deleting, converting, removing, obstructing, interrupting or interfering with the property or computer data of another. O.C.G.A. § 16-9-93(a) and (b). See Burlison v. McDonald’s Corp., 455 F.3d 1242, 1247 (11th Cir. 2006) (citing “longstanding canons of statutory construction, including the general principle that courts must not interpret one provision of a statute to render another provision meaningless.”).

The Georgia Court of Appeal’s decision in DuCom v. State, 288 Ga. App. 555 (2007), applies here. In DuCom, the defendant was charged with computer theft for using a company’s computer without authority to appropriate the computer data for Defendant’s personal use. Id. at 562. Defendant claimed her job duties gave her authority to copy the data she was charged with taking illegally.

Id. The Court of Appeals rejected her authority defense, finding that she admitted she did not have authority to take the data she acquired from her employer's computer system for use at the competing company she was forming. Id. at 562-63. The Court of Appeals noted that the data Defendant took was downloaded on the day defendant left her former employer, and she took it after she had formed her intent to start her own company with her former employer's clients. Id. The court found that there was sufficient evidence to show that the defendant *used* a computer, owned by her employer, knowing that her use was without authority and with the intention of removing programs or data from her employer's computer system, appropriating them for her own use. This use, the court found, violated O.C.G.A. § 16-9-93(a)(1). See also Automated Drawing Systems, Inc. v. Integrated Network Services, Inc., 214 Ga. App. 122 (1994) (rejecting defendant's contention that violation of GCSPA required an actual physical invasion of a computer).

In DuCom, the defendant downloaded company data and appropriated the data for personal use to form a competing company. This use was prohibited by the plain language of the statute. Plaintiff here has alleged Defendants engaged in the same use of Plaintiff's computer system—use of the Vurv-issued computer to

obtain data for use in Defendants' competing business. The Complaint alleges a use under O.C.G.A. § 16-9-93(a) and (b).¹

b. Use "without authority"

Defendants next argue that Plaintiff's claims for computer theft or trespass fail to state a claim because Plaintiff failed to allege that Defendants' actions were "without authority" as required by the GCSPA. The GCSPA defines "without authority" to include "the use of a computer or computer network in a manner that exceeds any right or permission granted by the owner of the computer or computer network." O.C.G.A. § 16-9-92(18). Defendants contend that Clements and Swearingen were, in their capacity as Vurv employees, authorized to access the information Plaintiff alleges was taken, and that Plaintiff has not alleged that Clements or Swearingen exceeded their authorized access or copied company data at a time when they were not authorized to access Plaintiff's computers or computer system.

Plaintiff argues that Defendants acted without authority because: 1) the Confidentiality Agreements Clements and Swearingen signed restricted their authority to access Vurv's computer systems and information; 2) Clements' and Swearingen's authority terminated when they decided to join Kenexa and thus

¹ While a use is alleged sufficiently, the Court does not predetermine whether the facts will support a use that may be prohibited by the statute.

acquired interests adverse to Plaintiff; 3) Clements and Swearingen did not have authority to continue accessing Vurv's computers or information after their last day of employment; and 4) Kenexa was not authorized to copy or remove Vurv's confidential and proprietary information which had been acquired by Clements and Swearingen without authority.

DuCom also applies on this issue. As the Court already has noted, in DuCom the defendant downloaded company data on the day she left the company and after she had formed an intent to start her own company with her former employer's clients. DuCom, 288 Ga. App. at 563. The Court of Appeals held that this was sufficient evidence to support a finding that the defendant's use of their former employer's computer and computer system was without authority. Id. Plaintiff also alleges Defendants' access here was in violation of their confidentiality agreement after they formed their intent to leave Vurv to join Kenexa.² Plaintiff thus sufficiently has alleged a use without authority.³

² Defendants' claim that Clements and Swearingen were Vurv employees authorized to access Vurv information after they left Vurv's employment is specious at best. Confronted with the illogic of their argument, Defendants' retreat position is to claim that Plaintiff fails to allege that Clements and Swearingen copied any company information after they left Vurv. A review of the Complaint clearly discredits Defendants' claim. See Compl. at ¶¶ 35, 37.

³ Defendants' reliance on SCQuARE Int'l, Ltd. v. BBDO Atlanta, Inc., 455 F. Supp. 2d 1347, 1368 (N.D.Ga. 2006) is misplaced. In SCQuARE Int'l, the court

c. Computer trespass

Defendants next argue that Plaintiff has failed to allege facts to show that Defendants had the intention of “removing” a computer program or data from Vurv’s computer or computer network sufficient to allege a claim for computer trespass.⁴ The parties have not pinpointed a case interpreting the trespass provision of the statute, and the Court’s own research has not revealed any authority construing this section. In considering the plain language of § 16-9-92(b), the Court determines that the word “remove” means: “to change the location, position, station, or residence of”; “to get rid of: eliminate”.⁵ Plaintiff does not allege that Clements and Swearingen changed the location of the files or otherwise disposed of them. That is, Plaintiff does not allege that its files were missing or removed from the company computers issued to Clements and Swearingen, or any other Vurv computer. The plain language of the statute contemplates a temporary or

granted summary judgment in favor of the defendant on plaintiff’s claim for computer theft because it noted there was no allegation that the appropriation was achieved by the unauthorized use of a computer. *Id.* In this case, though, Plaintiff claims that the Confidentiality Agreements restricted Clements’ and Swearingen’s authority, and that Clements and Swearingen did not have authority to continue accessing Vurv’s computers or information after their last day of employment.

⁴ Section 16-9-92(b) sets forth various conduct that constitutes computer trespass. Plaintiff alleges that Defendants copied or moved data from Vurv’s computers. The facts alleged do not support a claim under §§ 16-9-93(b)(2) or (3).

⁵ See <http://www.merriam-webster.com/dictionary/remove>.

permanent elimination of files or a temporary or permanent change of the file locations. Plaintiff's allegations do not support that removal occurred, and thus Plaintiff has not asserted a claim for computer trespass under O.C.G.A. § 16-9-93(b).

2. *Computer Fraud and Abuse Act (Counts 8 and 9)*

Defendants move to dismiss Plaintiff's claims asserted under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA"). Defendants argue that Plaintiff's claims under the CFAA should be dismissed because Plaintiff has not sufficiently alleged that Defendants acted "without authorization" or that Defendants "exceed[ed] authorized access," as required under the CFAA.

Plaintiff claims Defendants acted without authorization or exceeded their authorized access because: 1) the Confidentiality Agreements signed by Clements and Swearingen restricted their authority to access Vurv's computers and information; 2) Clements' and Swearingen's authority to access Plaintiff's computers and information terminated when, without Vurv's knowledge, they acquired interests adverse to Vurv; 3) even if Clements and Swearingen were authorized to access Vurv's information when they acquired interests adverse to Vurv, they did not have authority to continue accessing Vurv's computers or

information after the left Vurv's employment; and 4) Kenexa was not authorized to access Vurv's computers and information.

Like the GCSPA, the CFAA is a criminal statute that provides for a civil cause of action for "[a]ny person who suffers damage or loss by reason of a violation of this section." 18 U.S.C. § 1030(g). The CFAA does not define "without authorization". The CFAA defines "exceeds authorized access" to mean "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 parties have not cited any controlling authority on what constitutes conduct done "without authorization" or conduct which "exceeds authorized access", and the Court's independent research has not revealed any. Courts that have addressed these issues have split on whether an employee with an improper purpose may be held civilly liable for acquiring computer information he or she is otherwise permitted to access within the scope of his or her job duties. See Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1341 (N.D.Ga. 2007) (noting the split among courts regarding the meaning of acting "without authorization" as used in the CFAA). District courts in this circuit have held that a violation under the CFAA for access "without authorization" "occurs only where

initial access is not permitted.” Id. at 1343. See also Lockheed Martin Corp. v. Speed, No. 6:05-cv-1580-ORL-31, 2006 WL 2683058 (M.D.Fla. Aug. 1, 2006).

Other courts have found that an employee accesses computer information without authorization when that employee’s interests become adverse to the interests of his current employer. See Int’l Airport Centers, L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006); Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1123, 1125-28 (W.D.Wash. 2000). See also Cronin and Weikers, Data Security and Privacy Law: Combating Cyberthreats, 8:5 (current through July 2009) (noting that since Shurgard and Citrin, many courts have departed from this broad view, holding instead that access “without authorization” occurs only where the access was never authorized in the first place).

The Court agrees with those cases that interpret the phrase “without authorization” to mean where initial access was not permitted. Judge Story’s review of the other “authorization” provision of CFAA, including Section 1030(e)(6), and his view that such sections read as a coherent whole require “without authorization” to focus on initial access, not post-access information use, is sound. Judge Story notes, and this Court agrees, that his interpretation of the statute is consistent with the statute’s legislative history. Diamond Power, 540 F.

Supp. 2d at 1342-43. See also Burlison v. McDonald's Corp., 455 F.3d at 1246-47.

Plaintiff has alleged that Defendants Clements and Swearingen accessed Plaintiff's computers without authorization both during their employment with Vurv and after they left Vurv's employment. Vurv also alleges that even if Clements' and Swearingen's initial access was allowed, the access exceeded what was authorized. Essentially, Vurv claims (i) access to the computers while employed to obtain information for improper uses was unauthorized access under the statute and, (ii) any access after employment with Vurv was not authorized. Defendant claims (i) any during-employment access precludes a finding of unauthorized access because Clements and Swearingen were allowed to access their computers for their work, and (ii) that no post-employment access occurred. The Court addresses these arguments in turn.

a. During-employment access

The Court has addressed the meaning of "unauthorized access" and whether this term prohibits access to obtain information for an improper use. Plaintiff has not alleged that Clements and Swearingen were restricted from accessing the computers that were issued to them and thus, for the reasons this Court already has

discussed, Plaintiff has failed to state a claim for unauthorized initial access. See Diamond Power, 540 F. Supp. 2d at 1342.

Plaintiff also claims these two defendants accessed information and copied it for wrongful purposes and in doing so they exceeded their authorized access in violation of CFAA. In reviewing the Complaint, the Court finds Vurv does not allege that Clements and Swearingen were not authorized to “access” the information they copied, only that they did so for a wrongful purpose. That does not state a claim under the CFAA, and Plaintiff’s claim under CFAA for Defendants’ access while employed by Vurv is not viable.

b. Post-employment access

Defendants seek to dismiss Plaintiff’s CFAA claim based on post-employment conduct on the grounds that Plaintiff does not allege in its complaint that Clements and Swearingen appropriated any company information after their employment with Vurv ended. This claim is squarely discredited by the allegations in the Complaint. Plaintiff specifically alleges:

After Clements’s last day of employment with Vurv, before returning the Vurv computer that she had been issued, and, upon information and belief, after she had begun her employment with Kenexa, Clements continued to access and copy large groups of documents, folders, and .zip files in short increments of time. When Clements returned Vurv’s computer, she did not return any external hard drive or any other backup media.

Compl. at ¶ 81 (emphasis added). The Complaint contains an identical allegation against Swearingen. Id. at ¶ 83. These allegations show that Plaintiff has alleged that Clements and Swearingen accessed Vurv’s computers and copied Vurv’s confidential information after their employment with Vurv ended, and thus Plaintiff has stated a claim that is plausible on its face.^{6 7}

⁶ Although the Court has viewed the facts in a light most favorable to the Plaintiff to find that Plaintiff has alleged a viable claim, the Court does not predetermine what the facts will show regarding what post-employment access was allowed or whether, if allowed, Clements’ and Swearingen’s access exceeded any authority extended to them.

⁷ Defendants argue for the first time in their reply brief that Plaintiff’s CFAA claim must be dismissed because Plaintiff does not allege that it suffered any damage or loss recoverable under the CFAA. Defendants also argue for the first time in their reply brief that Plaintiff’s claim that Kenexa acted without authorization does not state a claim because Plaintiff has not alleged any independent basis to hold Kenexa liable, and “Kenexa cannot be vicariously liable for any wrongdoing, because there was none.” Defendants’ Reply at 8. First, these arguments were initially raised only in Defendants’ reply brief, and the Court is not required to consider them. Second, Defendants do not cite any controlling authority to support their claims. Because Defendants did not raise these arguments in their opening brief, the Court does not consider them here. See United States v. Georgia Dept. of Natural Resources, 897 F. Supp. 1464, 1471 (N.D.Ga. 1995) (citing United States v. Oakley, 744 F.2d 1553, 1556 (11th Cir. 1984) (“Arguments raised for the first time in a reply brief are not properly before the reviewing court.”)). These arguments, if warranted, may be made in a summary judgment motion. In fact, the Court believes that is the appropriate time to raise these issues.

3. *Tortious Interference with Contract (Count 10)*

Defendants move to dismiss Plaintiff's claim for tortious interference because it allegedly is based on the same facts as Plaintiff's claim for misappropriation of trade secrets and is therefore superseded by the Georgia Trade Secrets Act, O.C.G.A. § 10-1-761, et seq ("GTSA").

The GTSA supersedes conflicting tort, restitutionary, and other laws of Georgia providing civil remedies for misappropriation of a trade secret. O.C.G.A. § 10-1-767(a). The statute specifically provides that it shall not affect contractual duties or remedies, or "[o]ther civil remedies that are not based upon misappropriation of a trade secret." O.C.G.A. § 10-1-767(b). In other words, the GTSA does not supersede claims based on conversion and theft of property that does not constitute a trade secret. Tronitec, Inc. v. Shealy, 249 Ga. App. 442, 447 (2001), overruled on other grounds, Williams Gen. Corp. v. Stone, 279 Ga. 428 (2005). See also Penalty Kick Management Ltd. V. Coca Cola Company, 318 F.3d 1284 (11th Cir. 2003).

To support a claim for tortious interference with contract, "a plaintiff must establish the existence of a valid contract and that the defendant acted intentionally, without privilege or legal justification, to induce another not to enter into or continue a business relationship with the plaintiff, thereby causing the

plaintiff financial injury.” Atlanta Mkt. Ctr. Mgmt., Co. v. McLane, 269 Ga. 604, 608 (1998) (citing Lake Tightsqueeze, Inc. v. Chrysler First Fin. Servs. Corp., 210 Ga. App. 178, 181 (1993)). “Improper inducement may thus involve separate proof of conduct and injury from the conduct and injury required to prove misappropriation of a trade secret.” Diamond Power Int’l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1347 (N.D.Ga. 2007).

Here, Plaintiff alleges that Kenexa “interfered with the contractual relationship between Vurv and its employees, [by] inducing Clements and Swearingen to breach their confidentiality agreements by misappropriating Vurv’s trade secrets.” Compl. at ¶ 99. Plaintiff argues that while it alleges Defendants misappropriated trade secrets, it also claims Defendants stole thousands of other documents, folders, and files, which do not constitute trade secrets under the GTSA. In other words, Plaintiff argues that its claims relating to confidential and proprietary information, including customer information, cannot be superseded by the GTSA because they are not based upon misappropriation of only trade secret information. Plaintiff’s Response at 19; Compl. at ¶¶ 2, 19.⁸ The Court agrees.

⁸ Defendants contend that Plaintiff’s claim for tortious interference is not based upon misappropriation of other types of property. Defendants cite paragraphs 96-101, the paragraphs relating to the tortious interference count, to support their contention. However paragraph 96 expressly incorporates paragraphs 1-25 into the

Defendants rely on Opteum Financial Services, LLC v. Spain, 406 F. Supp. 2d 1378, 1380 (N.D.Ga. 2005) to support their claim that Plaintiff cannot plead an alternative theory of recovery should the allegedly stolen information ultimately not qualify as a trade secret. Opteum Financial does not apply here because the plaintiff in that case did not allege that *both* trade secrets and non-trade secret information were stolen. Vurv has alleged that Defendants stole trade secrets, and confidential and proprietary information that does not rise to the level of a trade secret. While this claim may be weak, it survives Defendants' Motion to Dismiss.

4. *Conspiracy Counts (Counts 3, 5, 7, and 9)*

Finally, Defendants claim the conspiracy counts alleged in the complaint must be dismissed because a conspiracy count cannot survive if the substantive count is dismissed and Plaintiff's claimed conspiracies are not supported by Plaintiff's factual allegations.

"A conspiracy is a combination of two or more persons to accomplish an unlawful end or to accomplish a lawful end by unlawful means. To recover damages for a civil conspiracy claim, a plaintiff must show that two or more persons, acting in concert, engaged in conduct that constitutes a tort. Absent the underlying tort, there can be no liability for civil conspiracy." J. Kinson Cook of

claim for tortious interference, and these paragraphs refer to Vurv's information which may not be limited to trade secrets.

Georgia, Inc. v. Heery/Mitchell, 284 Ga. App. 552, 560 (2007) (quoting Mustaqeem-Graydon v. SunTrust Bank, 258 Ga. App. 200, 207 (2002)). “A corporation may be a party to a conspiracy and may be held civilly liable for resulting damages to the same extent as a natural person.” NAACP v. Overstreet, 221 Ga. 16, 22 (1965). The Court has determined that Plaintiff has sufficiently alleged a claim for computer theft, and under the CFAA, and these conspiracies cannot be dismissed, as Defendants request, on the ground there is not a supporting substantive claim. The Court has found that Plaintiff has not sufficiently alleged a claim for computer trespass, and Plaintiff’s claim for conspiracy to commit computer trespass is dismissed because the substantive claim on which it is based does not survive the dismissal motion.

The Court next turns to Defendants’ claim that Plaintiff’s allegations of conspiracy are required to be dismissed under Twombly, because the conspiracies are insufficiently alleged and consists simply of the statement of legal elements for the claim unsupported by any fact allegations. In its complaint, Plaintiff alleges that Clements, Swearingen, and Kenexa:

entered into a conspiracy to accomplish a common, unlawful design to steal Vurv’s confidential and proprietary information. They arrived at a mutual understanding that, before Clements and Swearingen returned Vurv’s computers and started working for Kenexa, Clements and Swearingen would copy or remove Vurv’s confidential and

proprietary information from Vurv's computers or computer networks, despite not having the permission or authority to do so.

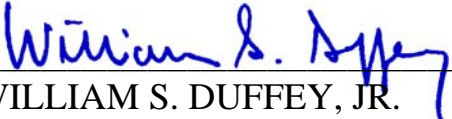
Compl. at ¶¶ 43, 91. Plaintiff's claim for conspiracy to misappropriate trade secrets contains similar allegations. See Compl. at ¶ 75. Plaintiff also alleges that Clements and Swearingen established outside channels of communication with Kenexa executives that would not involve using their Vurv e-mail accounts. Id. at ¶ 20. These allegations are sufficient, albeit barely, to state a claim for civil conspiracy to withstand a motion to dismiss. See Overstreet, 221 Ga. at 22. Plaintiff has alleged that two or more persons acted in concert to engage in conduct that constitutes a tort, and dismissal of these counts is not appropriate.

III. CONCLUSION

Accordingly,

IT IS HEREBY ORDERED that Defendants' Motion to Dismiss Counts 2-5 and 7-10 [16] is **GRANTED IN PART** and **DENIED IN PART**. Defendants' Motion to Dismiss Counts 4 and 5 is **GRANTED**. Defendants' Motion to Dismiss Counts 2, 3, 7, 8, 9, and 10 is **DENIED** provided, however, that Plaintiff's claims in Counts 8 and 9 are limited to post-employment access and copying of information.

SO ORDERED this 20th day of July, 2009.



WILLIAM S. DUFFEY, JR.
UNITED STATES DISTRICT JUDGE