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

AIRWATCH LLC, Plaintiff, v. MOBILE IRON, INC., Defendant.	CIVIL ACTION NO. 1:12-cv-3571-JEC

ORDER & OPINION

This case is before the Court on defendant's Motion to Dismiss [6]. Plaintiff filed a Response [8], and defendant filed a Reply [10]. The Court has considered these submissions and for the below reasons, holds that defendant's Motion [6] should be **DENIED**.

BACKGROUND

Plaintiff AirWatch, LLC ("AirWatch") sells software that permits users to securely send electronic messages and documents from mobile devices. (Compl. [1] at ¶ 2.) Airwatch is based in Georgia. (*Id.* at ¶ 1.) Defendant Mobile Iron, Inc. ("Mobile Iron") is a competitor with AirWatch in the field of mobile device software and is based in California. (*Id.* at ¶¶ 3-4.)

On or around July 12, 2012, an individual representing himself as "Jeff Woodhousen" submitted a request on AirWatch's website for a

free thirty-day trial of AirWatch's software. (*Id.* at ¶ 18.) Woodhousen's request was purportedly on behalf of his company, a real estate firm called "Havenswright." (*Id.*) AirWatch salesperson Steven Rhee responded to Woodhousen's email (which came from an "@Havenswright.com" address) and suggested that Woodhousen participate in an online demonstration of the software, which Rhee performed on July 16. (Compl. [1] at ¶¶ 19-22.) Woodhousen agreed to view the demonstration, and he provided Rhee with two physical addresses for Havensright, both in San Jose, California. (*Id.* at ¶ 23.)

On July 17, following the demonstration, Rhee sent a proposal to Woodhousen that Havenswright may receive a thirty-day free trial of AirWatch's software on the condition that Woodhousen agree to the terms of an End User License Agreement ("EULA"), which was incorporated by reference into the proposal. (*Id.* at ¶ 24 (proposal sent to Woodhousen "for his review and signature.").) The EULA provided in part that "the Software is provided to User for evaluation purposes," and that it is a "license to use the software solely for the purposes of testing and evaluating the software." (*Id.* at ¶ 26.) The EULA further stated that the user "shall not engage in competitive analysis." (*Id.* at ¶ 27.) On or about July 18, Woodhousen agreed to the terms of AirWatch's proposal, and AirWatch established a "trial environment for Havenswright," subject

to the terms of the EULA, by which Havenswright had "access to the AirWatch Resource Portal, which include[d] proprietary and confidential videos and documentation concerning the AirWatch Software." (Compl. [1] at ¶¶ 25, 28.)

Over the next several weeks, Woodhousen and his colleague (who called himself "Mr. Thompson") accessed the AirWatch trial environment at least 43 times. (*Id.* at ¶ 47.) During that period Woodhousen and his colleague asked Rhee several questions about AirWatch's software, and Rhee was generally responsive. (*Id.* at ¶¶ 29-36.)

Woodhousen's free trial was set to expire on August 17, and on August 15, Woodhousen emailed Rhee, requesting a two-week extension. (*Id.* at ¶ 40.) Rhee proposed a phone meeting via email invitation for August 16, and Woodhousen accepted. (*Id.* at ¶¶ 41-42.) Rhee postponed the meeting to August 20, at which time Woodhousen called Rhee. (Compl. [1] at ¶¶ 43, 48.) During this phone call, Rhee noticed on the visual display of his work telephone that the number Woodhousen was calling from was different than the number Woodhousen used in the past. (*Id.* at ¶¶ 48-49.) Upon discovering that Woodhousen was in fact calling from a Mobile Iron number, Rhee ended the call, and he disabled "Havenswright"'s access to the free trial. (*Id.* at ¶¶ 48, 50.) Rhee also reviewed his August 16 meeting invitation and discovered that "Woodhousen" had forwarded Rhee's

invitation to the Mobile Iron email address of Jake Woodhams.[1] (*Id.* at ¶ 52.)

On August 23, 2012, AirWatch sent a letter to the CEO of Mobile Iron demanding that it cease and desist using any and all information that its employees obtained from AirWatch or that Mobile Iron learned through its free trial. (*Id.* at ¶ 57.) Mobile Iron's CEO met with the Chairman of AirWatch on September 17, after which AirWatch requested that Mobile Iron respond in writing to the concerns AirWatch raised in its August 23 letter. (Compl. [1] at ¶¶ 58-62.) According to AirWatch, Mobile Iron has yet to provide a sufficient response, and on October 12, 2012 AirWatch brought the current action. (*Id.* at ¶ 62.)

In its complaint, AirWatch claims that Woodhams and another Mobile Iron employee masqueraded as Woodhousen and Thompson and invented a fictitious real estate company "to gain access to the AirWatch Software and to AirWatch confidential, proprietary, and trade secret information for the benefit of Mobile Iron." (*Id.* at ¶ 54.) AirWatch alleges that Woodhams' charade enabled the Mobile Iron employees to "learn[] technical details about the AirWatch Software and its functionality, and acquire[] information about AirWatch's

[1] It is unclear if Mr. Woodhams created his *nom de plume*, "Woodhousen," from a derivation of his own last name, or if he was an admirer of the Jane Austen novel, "Emma," prominently featuring the fictional Woodhouse family.

confidential and proprietary marketing strategies and pricing information, which information constitutes AirWatch's confidential, proprietary, and trade secret information." (*Id.* at ¶ 55.) "On information and belief," AirWatch alleges that "Mobile Iron has used and is currently using the AirWatch trade secrets and confidential information that the Mobile Iron Employees gained improperly for the purpose of gaining an unfair competitive advantage over AirWatch by, among other things, relying on AirWatch confidential and trade secret information to develop marketing materials and other derivative works." (*Id.* at ¶ 56.)

AirWatch brings five counts against Mobile Iron: (1) a claim under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.*, that the Mobile Iron employees improperly accessed AirWatch's computer systems; (2) a claim for misappropriation of trade secrets under the Georgia Trade Secrets Act, O.C.G.A. § 10-1-760[2] *et seq.*; (3) a claim that Mobile Iron violated the California Unfair Competition Law, CAL. BUS. & PROF. CODE § 17200 *et seq.*, by engaging in unlawful, unfair, or fraudulent business practices; (4) a tort claim for fraudulent misrepresentation; and (5) in the alternative, a breach of contract claim with respect to the EULA. (Compl. [1] at 17-24.) Defendant moves to dismiss plaintiff's state law claims, (2)-(5).

[2] The Complaint references § 10-1-76. The Court will assume that plaintiff meant § 10-1-760.

(Def.'s Mot. to Dismiss [6] at 2.)

DISCUSSION

I. MOTION TO DISMISS STANDARD

Under Federal Rule 12(b)(6), a court may dismiss a claim for failure to state a claim upon which relief may be granted. When deciding whether to dismiss a claim under Rule 12(b)(6), a court must construe the complaint in the light most favorable to the plaintiff and accept the plaintiff's allegations of material fact as true. *Beck v. Deloitte & Touche*, 144 F.3d 732, 735 (11th Cir. 1998). A court may grant a motion to dismiss if it finds that the plaintiff cannot prove any set of facts consistent with the complaint which would entitle him or her to relief. *Hishon v. King & Spalding*, 467 U.S. 69, 73 (1984). Defendant bears "the 'very high burden' of showing that the plaintiff cannot conceivably prove any set of facts that would entitle him to relief." *Beck*, 144 F.3d at 735-36.

II. MISAPPROPRIATION OF TRADE SECRETS CLAIM

The Georgia Trade Secrets Act ("GTSA") provides a civil remedy for the misappropriation of trade secrets. O.C.G.A. § 10-1-760 *et seq*. To state such a claim, a plaintiff must allege that: (1) it possessed a trade secret, and (2) the defendant misappropriated the trade secret. *Penalty Kick Mgmt. Ltd. v. Coca Cola Co.*, 318 F.3d

1284, 1290-91 (11th Cir. 2003).[3] Here, defendant disputes that AirWatch has alleged facts that would meet either prong. (*Compare* Mem. of Law in Supp. of Def.'s Mot. to Dismiss ("Def.'s Br.") [6-1] at 3-7, *with* Pl.'s Resp. in Opp. to Def.'s Mot. to Dismiss ("Pl.'s Opp'n Br.") [8] at 8-14.)

A. Existence of Trade Secret

The GTSA defines a "trade secret" as:

> information, without regard to form, including, but not limited to, technical or nontechnical data, a formula, a pattern, a compilation, a program, a device, a method, a technique, a drawing, a process, financial data, financial plans, product plans, or a list of actual or potential customers or suppliers which is not commonly known by or available to the public and which information:
>
> (A) Derives 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.

O.C.G.A. § 10-1-761(4).

Though a plaintiff need not "disclose the trade secrets in detail" at the pleading stage, the Court must still discern what information AirWatch claims Mobile Iron misappropriated. *Water & Energy Sav. Corp. v. Minor*, No. Civ. A. 1:04 CV 1785 W, 2005 WL 1168423, at *2 (N.D. Ga. May 9, 2005)(Hunt, J.). While AirWatch

[3] The GTSA permits both injunctive and monetary relief. O.C.G.A. §§ 10-1-762 & 10-1-763.

references a wide swath of its information as deserving of trade secret protection,[4] the trade secrets plaintiff accuses defendant of improperly accessing include the following:

> By participating in conference calls with AirWatch personnel, through testing the AirWatch Software, and through access to the AirWatch Resource Portal, and the AirWatch ASK Portal, the Mobile Iron Employees, for the benefit of Mobile Iron, learned ***technical details about the AirWatch Software and its functionality, and acquired information about AirWatch's confidential and proprietary marketing strategies and pricing information***, which information constitutes AirWatch's confidential, proprietary, and trade secret information.

(Compl. [1] at ¶ 55 (emphasis added).)

O.C.G.A. § 10-1-761(4) lists "programs" as information that may qualify for trade secret protection, so AirWatch's software program meets at least this requirement. However, to be a trade secret, this information must also "not be[] readily ascertainable by proper means," and it must be the "subject of efforts that are reasonable under the circumstances to maintain its secrecy." O.C.G.A. § 10-1-761(4)(A)-(B).[5] Defendant contends that because AirWatch makes its

---

[4] (*E.g.*, Compl. [1] at ¶ 11 ("AirWatch's trade secrets include, without limitation, AirWatch's marketing strategies and procedures, software design, know-how, negative know-how, customer information, including customer contact information, customer purchasing preferences and decisions, pricing policies and related information, and business operation procedures.")))

[5] Plaintiff must also derive economic value from the software and from its secrecy. AirWatch has most likely met this requirement since selling this software is its business, and as explained below, AirWatch licenses its software on the condition the user keep its

product available to consumers, the program's capabilities are by definition "readily ascertainable" and therefore cannot be trade secrets. (Def.'s Br. [6-1] at 4-5; *see also Roboserve, Ltd. v. Tom's Foods, Inc.*, 940 F.2d 1441, 1454 (11th Cir. 1991)("The sale destroyed any reasonable expectation of secrecy by placing the machines in the public domain.").) According to defendant, only AirWatch's underlying "source code" may be a trade secret, and since AirWatch has not alleged that Mobile Iron's employees accessed AirWatch's source code, their trade secret misappropriation claim must fail.[6] (*See* Reply in Supp. of Def.'s Mot. to Dismiss ("Def.'s Reply Br.") [10] at 4 & n.2 (citing *Silvaco Data Sys. v. Intel Corp.*, 184 Cal. App. 4th 210, 221-22 (2010)).) Plaintiff counters that AirWatch consistently seeks to preserve its software's confidentiality by ensuring that its customers and prospective customers are subject to confidentiality obligations embodied in EULAs, and that so long as

---

contents confidential. (Compl. [1] at ¶ 2.)

[6] A software program's source code is written by a human in a programming language, after which a compiler converts the source code into "object code." The computer will then execute the object code in a fashion that makes the program cognizable for human users, resulting in the end product–what the user perceives as the software, the program, or the "system." Thus, to one running a program, the source code is not accessible. Source code is generally considered to be a trade secret. *See generally Silvaco Data Sys. v. Intel Corp.*, 184 Cal. App. 4th 210, 217-18 & n.4 (2010)(disapproved of on other grounds by *Kwikset Corp. v. Superior Ct.*, 51 Cal. 4th 310 (2011))(explaining why source code is a trade secret).

AirWatch seeks to preserve this confidentiality, its software may be a trade secret. (Pl.'s Opp'n Br. [8] at 12.)

The Court acknowledges defendant's distinction between source code and the visible output of the software program. *See supra* n.6. Indeed, there is support for defendant's theory that source code may be a trade secret, whereas the appearance and functionality of the software program cannot. *E.g.*, *Agency Solutions.Com, LLC v. TriZetto Grp., Inc.*, 819 F. Supp. 2d 1001, 1028 (E.D. Cal. 2011)(if a company "market[s] [a program] to its customers, revealing in the process how the program works, looks, performs and the purpose behind it[,]" the program is not a trade secret); *IDX Sys. Corp. v. Epic Sys. Corp.*, 285 F.3d 581, 584 (7th Cir. 2002)("details that ordinary users of the software could observe" are not trade secrets); *Silvaco Data Sys.*, 184 Cal. App. 4th at 221-22 (executable program may not be a trade secret, if it is evident to "anyone running the finished program.").

That being said, information regarding AirWatch's software may still be a trade secret, if AirWatch can show that it worked to preserve the secrecy of its program's functions, specifications, and pricing--*i.e.*, what AirWatch is currently claiming Mobile Iron misappropriated. The Court cannot say at the motion to dismiss stage that the steps AirWatch took to restrict how customers used its program and who had access to its program were inadequate to maintain this information's secrecy. According to AirWatch's complaint, users

of its software were subject to EULAs containing confidentiality provisions, and AirWatch only gave away its free samples through salesmen, and for limited periods of time. (*E.g.*, Compl. [1] at ¶¶ 16-17.) While defendant is correct that plaintiff presumably wished current and prospective customers to know and enjoy the benefits of its software, such users were still licensees, subject to the terms of the EULAs, and the disclosure of the program's specifications to those users does not *per se* forfeit the program's trade secret status. *See Univ. Computing Co. v. Lykes-Youngstown Corp.*, 504 F.2d 518, 535 (5th Cir. 1974)(under the definition of a trade secret in the Restatement of Torts, computer system with "unique capabilities and features" may be a trade secret even though it was sold to customers since claimant "used great caution in attempting to preserve its confidentiality"); *TDS Healthcare Sys. Corp. v. Humana Hosp. Illinois, Inc.*, 880 F. Supp. 1572, 1575 & 1583 (N.D. Ga. 1995) (Evans, J.)(denying motion for summary judgment on trade secret misappropriation claim, where alleged trade secret was licensed "computerized hospital healthcare information system"); *CMAX/Cleveland, Inc. v. UCR, Inc.*, 804 F. Supp. 337, 357-58 (M.D. Ga. 1992)(software system found to be trade secret, where users were subject to license agreements).[7]

---

[7] *See also Trandes Corp. v. Guy F. Atkinson Co.*, 996 F.2d 655, 663-64 (4th Cir. 1993)(software system may be trade secret, even

The Court also notes that the nature of AirWatch's product--*i.e.*, security software for mobile phones--is not such that a typical user of the software would be exposed to the software's capabilities by using the program. One does not know merely by sending an email or document on a smartphone whether the transmission was "secure" or what steps the phone's software took to make it secure. While these steps might be clearer once an AirWatch sales representative explained the product to the customer, if the customer signed a EULA

---

though plaintiff advertised the capabilities of the software system and gave out trial samples, where software was licensed to end users); LAW OF COMPUTER TECHNOLOGY § 3:27 ("Courts routinely recognize a distinction between licensed software and products sold to the buyer for purposes of trade secret law confidentiality issues. A license agreement provides an adequate, frankly a common, framework on which to base confidentiality restrictions.")(internal footnote omitted).

Mobile Iron attempts to distinguish *CMAX* and *TDS*, cited above, by arguing that the steps the defendants took in those cases were more extensive than the conduct AirWatch alleges here and were more akin to copying source code–a practice Mobile Iron admits is trade secret misappropriation but which AirWatch does not allege that Mobile Iron did. (Def.'s Reply Br. [10] at 4.) The Court finds this argument unpersuasive. While the *CMAX* and *TDS* defendants may have improperly acquired the plaintiffs' source code, the trade secrets at issue in those cases still included the software systems' features and not only the underlying code. *CMAX*, 804 F. Supp. at 357-58 (trade secret was the system itself); *TDS*, 880 F. Supp. at 1582-83 (same). In addition, it is at least plausible that Mobile Iron's analysis of AirWatch's software went beyond simply assessing the program's capabilities. Mobile Iron's employees accessed AirWatch's portal 43 times, and even after the free trial had almost expired, Woodhams requested two additional weeks of access. (Compl. [1] at ¶¶ 40, 47.)

agreeing to keep the information learned in such a presentation confidential, eventual dissemination of the program to smartphone users would not in itself reveal the program's specifications and capabilities.

B. Misappropriation

O.C.G.A. § 10-1-761 defines misappropriation as, in part, "***Disclosure or use*** of a trade secret of another without express or implied consent by a person who...***[u]sed improper means*** to acquire knowledge of a trade secret." O.C.G.A. § 10-1-761(2)(B)(i)(emphasis added). Defendant argues that plaintiff has not actually alleged that Mobile Iron used the trade secret. (Def.'s Br. [6-1] at 6.) The Court disagrees.

Plaintiff alleges that Mobile Iron "used and is currently using the AirWatch trade secrets...that the Mobile Iron Employees gained improperly...to develop marketing materials and other derivative works." (Compl. [1] at ¶ 56; *see also supra* n.7 (noting that defendant's access to plaintiff's alleged trade secret was extensive).) While plaintiff does not allege how exactly defendant is using the information it acquired, AirWatch's allegation that Mobile Iron acquired the program and is using it to develop its own products is sufficient at the motion to dismiss stage. *Penalty Kick*, 318 F.3d at 1292 ("As a general matter, any exploitation of the trade secret that is likely to result in...enrichment to the defendant is

a 'use'....[E]mploying the trade secret in manufacturing or production, [and] relying on the trade secret to assist or accelerate research or development...all constitute 'use.'")(quoting RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. c (1995)).

Plaintiff also adequately alleges that defendant used "improper means" in acquiring the trade secrets. O.C.G.A. § 10-1-761(2)(B)(i). Plaintiff describes defendant's use of false identities, email addresses, phone numbers, and a fake business. (*See generally* Compl. [1] at ¶¶ 48-50 (describing Rhee's discovery of the Mobile Iron employees' fraud).) These allegations satisfy the definition of "improper means" in O.C.G.A. § 10-1-761(1), which defines "improper" to mean, *inter alia*, misrepresentation.

For these reasons, AirWatch has sufficiently alleged that Mobile Iron misappropriated its trade secret, and defendant's Motion to Dismiss [6] is **DENIED** with respect to this claim.

III. FRAUDULENT MISREPRESENTATION CLAIM

Defendant argues that plaintiff's GTSA claim supersedes its fraudulent misrepresentation claim because both counts are based on the same set of facts. (Def.'s Br. [6-1] at 13-14.) Plaintiff counters that its fraudulent misrepresentation claim, unlike its trade secret claim, is premised on "defendant's intent to deceive" and is thus a separate, distinct claim. (Pl.'s Opp'n Br. [8] at 22.)

Georgia law is clear that if plaintiff's information is a trade

secret, and plaintiff alleges that defendant improperly used that trade secret, a trade secret misappropriation claim will supersede any fraud claim based on the same set of facts. O.C.G.A. § 10-1-767(a)(GTSA "shall supersede conflicting tort, restitutionary, and other laws of this state providing civil remedies for misappropriation of a trade secret."); *Penalty Kick*, 318 F.3d at 1297-98 (GTSA supersedes tort claim to the extent the claim addresses a trade secret); *Tronitec, Inc. v. Shealy*, 249 Ga. App. 442, 447 (2001)(overruled on other grounds by *Williams Gen. Corp. v. Stone,* 279 Ga. 428 (2005))(GTSA supersedes tort claims alleging theft of trade secrets).

Here, whether AirWatch's software is a trade secret is unsettled, leaving the possibility that defendant may have taken *some* information from plaintiff via fraudulent means, just not a trade secret. Thus plaintiff argues dismissing its fraud claim at this stage is premature. Indeed, plaintiff notes that the cases cited by defendant addressed summary judgment motions, not motions to dismiss. The Court agrees. Defendant may relitigate this issue at the summary judgment stage. Thus, defendant's Motion [6] is **DENIED without prejudice** with respect to plaintiff's fraudulent misrepresentation claim.

IV. CALIFORNIA UNFAIR COMPETITION CLAIM

Defendant also seeks to dismiss plaintiff's claim under California's Unfair Competition Law, CAL. BUS. & PROF. CODE § 17200 (the "UCL"). The UCL's focus and purpose is to "protect[] the general public against unscrupulous business practices." *In re Tobacco II Cases*, 46 Cal. 4th 298, 312 (2009). To accomplish this goal, the UCL proscribes "business act[s] or practice[s]" that are "[1] unlawful, [2] unfair or [3] fraudulent." CAL. BUS. & PROF. CODE § 17200; *Cal-Tech Commc'ns, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal. 4th 163, 180 (1999). "Prevailing plaintiffs are generally limited to injunctive relief and restitution," and plaintiffs may not receive damages or attorneys' fees, even if a UCL violation is shown. *Cal-Tech*, 20 Cal. 4th at 179; *see also id.* at 181 (purpose of UCL is to enable courts to enjoin "the innumerable new schemes which the fertility of man's invention would contrive.")(internal quotations omitted).

As an initial matter, defendant argues that plaintiff may not bring a claim under the UCL because Georgia law applies to the dispute, and California disfavors the extraterritorial application of its statutes. (Def.'s Br. [6-1] at 7-10.)

Under Georgia's choice of law rules, the law of the place of the harm "determines the substantive rights of the parties." *Risdon Enters., Inc. v. Colemill Enters., Inc.*, 172 Ga. App. 902, 903 (1984). Here, plaintiff's injuries, if any, occurred in Georgia, so

Georgia law would apply to tort claims arising from those injuries. However, application of Georgia law to plaintiff's tort claims does not foreclose the possibility that a non-California plaintiff such as AirWatch may also bring a claim under the UCL, provided the factual nexus of its claim is sufficiently aligned with California. *E.g.*, *State of Fla., Office of Att'y Gen., Dep't of Legal Affairs v. Tenet Healthcare Corp.*, 420 F. Supp. 2d 1288, 1311 (S.D. Fla. 2005)(where Florida law applied to tort claims, Florida plaintiff could still bring UCL claim because "[plaintiff] has alleged unfair conduct occurring in the State of California"); *TruePosition, Inc. v. Sunon, Inc.*, Civil Action No. 05-3023, 2006 WL 1451496, at *5-6 (E.D. Pa. May 25, 2006)(DuBois, J.)(where Pennsylvania law applied to tort claims, Pennsylvania plaintiffs permitted to pursue action under UCL because defendant's alleged misconduct occurred in California); *see also Foster v. United States*, 768 F.2d 1278, 1281 (11th Cir. 1985) (different states' laws may apply to different issues within the same case).

A sufficient nexus with California exists, if the relevant misconduct occurred in California. *Tidenberg v. Bidz.com, Inc.*, No. CV 08-5553 PGS (FMOx), 2009 WL 605249, at *4 (C.D. Cal. Mar. 4, 2009)(Gutierrez, J.)(UCL "'may be invoked by out-of-state parties when they are harmed by wrongful conduct occurring in California.'") (quoting *Nw. Mortg., Inc. v. Superior Ct.*, 72 Cal. App. 4th 214, 224-

25 (1999)). Here, plaintiff alleges that defendant's office is in California, and one of Mobile Iron's employees called AirWatch from a California area code, suggesting that defendant's employees orchestrated the fraud there. (Compl. [1] at ¶¶ 3, 48.) At least for a motion to dismiss, these allegations are sufficient to form the requisite nexus with California. *See Tidenberg*, 2009 WL 605249, at *4.

Defendant argues that even if plaintiff could bring a UCL claim, plaintiff has not alleged conduct that constitutes a UCL violation. (Def.'s Br. [6-1] at 7-8.) To succeed on its UCL claim plaintiff must allege that Mobile Iron's conduct was unfair, fraudulent, or unlawful. CAL. BUS. & PROF. CODE § 17200. These prongs are disjunctive, so plaintiff need only meet one for its claim to proceed. AirWatch has at least alleged that Mobile Iron's misconduct was unlawful under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 *et seq.*, and defendant has not moved to dismiss this claim. (Def.'s Br. [6-1] at 2.)[8] The CFAA may form the predicate for

[8] It is questionable whether plaintiff could sustain a UCL claim based on fraudulent or unfair conduct since the parties here are competitors, and plaintiff has not alleged any harm to the general public. *Nat'l Rural Telecomms. Co-op. v. DIRECTV, Inc.*, 319 F. Supp. 2d 1059, 1075 (C.D. Cal. 2003); *Watson Labs., Inc. v. Rhone-Poulenc Rorer, Inc.*, 178 F. Supp. 2d 1099, 1121 (C.D. Cal. 2001). Nonetheless, a lack of harm to the public did not preclude the court in *Watson* from permitting the plaintiff's UCL claim under the "unlawful" prong to proceed. *Watson*, 178 F. Supp. 2d at 1120.

a UCL violation, so plaintiff's UCL claim may proceed on this basis. *E.g.*, *Oracle Am., Inc. v. Serv. Key, LLC*, No. C 12-00790 SBA, 2012 WL 6019580, at *10 (N.D. Cal. Dec. 3, 2012)(Armstrong, J.)(alleged CFAA violation may be predicate for "unlawful" conduct under the UCL).[9]

Defendant also contends that AirWatch has failed to allege it lost money or property, and as a result, its UCL claim must fail. (Def.'s Br. [6-1] at 7-8.) However, in *Kwikset Corp. v. Superior Ct. of Orange Cnty.*, 51 Cal. 4th 310 (2011) the California Supreme Court held that "lost money or property" under § 17204 is not limited to only those injuries which can be compensated via restitution and instead extends to any economic injury. *Id.* at 323-25. Here, plaintiff alleges that as a result of defendant's deception, Mobile Iron's employees accessed plaintiff's intellectual property, resulting in harm to AirWatch's business. (Compl. [1] at ¶¶ 69-70.) This loss of property is sufficient to constitute economic injury under the UCL. *See Kwikset*, 51 Cal. 4th at 323 (economic injury

[9] Defendant's alleged violation of the GTSA could not be the predicate for "unlawful" conduct since "[t]o the extent that plaintiff's UCL claim is based on [trade secret misappropriation], it is preempted." *Ikon Office Solutions, Inc. v. Rezente*, No. CIV 2:10-1704 WBS KJM, 2010 WL 5129293, at *6 (E.D. Cal. Dec. 9, 2010)(Shubb, J.). There is also disagreement in the California courts about whether common law claims could be the basis for "unlawful" conduct under the UCL. *See generally Clark v. Prudential Ins. Co. of Am.*, 736 F. Supp. 2d 902, 928-30 (D.N.J. 2010)(describing conflicting threads of authority within California). However, since the plaintiff has alleged a CFAA violation, the Court need not address that issue here.

where property interest is diminished); *Fields v. QSP, Inc.*, No. CV 10-5772 CAS (Ssx), 2011 WL 1375286, at *6 (C.D. Cal. Apr. 8, 2011)(Snyder, J.)(misappropriation of confidential information and alleged trade secrets constitute economic injury). Therefore, plaintiff's claim cannot be dismissed on this basis, and defendant's Motion to Dismiss [6] is **DENIED** with respect to this count.

V. BREACH OF CONTRACT CLAIM

Defendant argues that plaintiff's breach of contract claim should be dismissed because plaintiff fails to allege that Mobile Iron assented to the EULA, and plaintiff fails to allege that it suffered any damages as a result of Mobile Iron's alleged breach. (Def.'s Br. [6-1] at 15-16.)

A. Assent

For a contract to be enforceable, all parties to that contract must assent to its terms. *Hunt v. Thomas*, 296 Ga. App. 505, 509 (2009). Courts apply an objective theory of intent whereby a party assents if a reasonable person in the position of the other contracting party would ascribe to the first party's manifestations of assent. *Frickey v. Jones*, 280 Ga. 573, 575 (2006). "In making that determination, the circumstances surrounding the making of the contract, such as correspondence and discussions, are relevant in deciding if there was a mutual assent to an agreement, and courts are free to consider such extrinsic evidence." *Id.* (internal quotations

omitted).

> Here, AirWatch alleges the following:
>
> On or about Tuesday, July 17, 2012, Mr. Rhee forwarded Quote Number 00017584 (the "Quote") for a free trial of the AirWatch Software to Mr. "Woodhousen" for his review and signature. The Quote provided that the free trial of the AirWatch Software would expire on August 16, 2012. The Quote was conditioned upon the terms and conditions of the End User License Agreement ("EULA").
>
> On or about July 18, 2012, Mr. "Woodhousen" assented to the terms of the Quote and the incorporated EULA.

(Compl. [1] at ¶¶ 24-25.) The "Quote" contains an electronic signature from "Jeff Woodhousen." (See Ex. A, attached to Pl.'s Opp'n Br. [8-1] at 3.)

Defendant argues that "the Complaint does not allege facts which suggest MobileIron or its employees ever knew or were on notice of what the terms of the EULA were," and "[t]here is no indication regarding whether or how [or when]...Plaintiff provided the EULA to MobileIron or its employees." (Def.'s Br. [6-1] at 15.) The Court disagrees. For present purposes, plaintiff has adequately described the manner in which AirWatch conveyed the EULA to Mobile Iron's employees. The "Quote" clearly referenced the EULA and provided that acceptance of the software trial offer was conditioned upon agreement to the EULA's terms. (See Ex. A, attached to Pl.'s Opp'n Br. [8-1] at 2.) Further, Mobile Iron's employee electronically signed the Quote, which incorporated the EULA by reference, thus signaling his

agreement to be bound by the EULA's terms. *See Harris v. Baker*, 287 Ga. App. 814, 817 (2007)(party's signature indicates assent).[10] These allegations are sufficient such that plaintiff may survive a motion to dismiss.

B. Damages

Defendant also argues that plaintiff's breach of contract claim fails because plaintiff does not allege it incurred any damages. (Def.'s Br. [6-1] at 16.) AirWatch alleges that Mobile Iron is using AirWatch's trade secrets for the purpose of gaining an unfair competitive advantage over AirWatch. (Compl. [1] at ¶ 56.) While plaintiff does not allege precisely how much defendant's alleged breach of the EULA is costing AirWatch, AirWatch still alleges that

[10] Defendant argues that the EULA submitted by plaintiff with its Opposition Brief has been redacted so extensively that it is not clear whether this was the EULA Mobile Iron allegedly signed, and because "plaintiff has failed to identify the contract or the contractual terms at issue, the claim is subject to dismissal." (Def.'s Reply Br. [10] at 13-14.) Defendant's citation to *Anderson v. Deutsche Bank Nat'l Trust Co.*, Civil Action No. 1:11-cv-4091-TWT-ECS, 2012 WL 3756512, at *5 (N.D. Ga. Aug. 12, 2012)(Scofield, M.J.) for this proposition is inapposite. The claimant in *Anderson* did not cite to a "single provision of any contract," nor did he "allege[] the existence of a specific contract." *Id.* Contrast that to the current case, where AirWatch references its proposal and the EULA throughout its pleadings and includes excerpts from the EULA in its complaint. (*E.g.*, Compl. [1] at ¶ 26.) Defendant is free to probe during discovery the extent to which the EULA was made available to Mobile Iron's employees and prospective customers, and whether Mobile Iron's employees actually received the EULA. Dismissal of plaintiff's contract claim at this stage is inappropriate.

it "invested substantial assets in developing its [software] system and [defendant], as its competitor, saved time and money by studying [plaintiff's] system." *TDS*, 880 F. Supp. at 1584, n.10. If these allegations are true, it is certainly plausible that AirWatch may have incurred damages. *Id.*; *see also Rosen v. Protective Life Ins. Co.*, 817 F. Supp. 2d 1357, 1374 (N.D. Ga. 2011)(Duffey, J.)("The rule against the recovery of vague, speculative, or uncertain damages relates more especially to the uncertainty as to cause, rather than uncertainty as to the measure or extent of the damages.")(internal quotations omitted); *CMAX*, 804 F. Supp. at 359 (defendant liable for breach of contract, where defendant breached licensing agreement with plaintiff by copying plaintiff's software system).

For these reasons, plaintiff may proceed with its contract claim, and defendant's Motion to Dismiss [6] is **DENIED** with respect to this claim.

CONCLUSION

For the foregoing reasons, defendant's Motion to Dismiss [6] is **DENIED.**

SO ORDERED, this 4th day of SEPTEMBER, 2013.

/s/ Julie E. Carnes
JULIE E. CARNES
CHIEF UNITED STATES DISTRICT JUDGE