UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK
- -

PENROSE COMPUTER MARKETGROUP, INC., d/b/a CYBERCITY,

Plaintiff,

v. 09-CV-00911

DOUGLAS J. CAMIN,

Defendant.

- -

THOMAS J. McAVOY
Senior United States District Judge

DECISION and ORDER

Plaintiff, Cybercity, ("Plaintiff"), former employer of Defendant, Douglas Camin, ("Defendant"), brought the instant action alleging: (1) violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030; (2) violation of the Stored Communication Act ("SCA"), 18 U.S.C. § 2701; (3) breach of contract; (4) breach of the fiduciary duties of good faith and duty to preserve good will; (5) misappropriation of trade secrets; (6) tortious interference with contractual relations; (7) tortious interference with prospective economic relations; (8) unfair competition; and (9) tortious interference with prospective business advantage, arising from Defendant's actions while employed by Plaintiff. See Docket No. 1 paragraph 1. Defendant filed this motion to dismiss pursuant to Fed. R. Civ. P. 12(b)(6) alleging that Plaintiff failed to sufficiently plead: (1) a cognizable loss under the CFAA, 18 U.S.C. § 1030; (2) a claim under the SCA, 18 U.S.C. § 2701; (3) breach of contract; (4)

misappropriation of trade secrets; (5) breach of fiduciary duty or unfair competition; and (6) tortious interference with contract or tortious interference with prospective economic advantage. See Docket No. 10.

I. FACTS

Plaintiff "is a full service provider of end-to-end computer services in the greater-Binghamton area, including information technology development, solutions, maintenance, repair, training, Web Site Design, Web Site Hosting, and hardware, software, and office supply products." See Docket No. 1 at paragraph 4. Defendant was employed by Plaintiff from October 4, 2004 until he was terminated on July 7, 2008. Id. at paragraph 6. Defendant signed a Non-Disclosure Agreement as a condition of his employment. Id. at paragraph 15.

"At the time of his termination, Defendant was employed as the Director of Technical Services." Id. at paragraph 7. Pursuant to this position, Defendant was "responsible for the management of all computer services provided by [Plaintiff] to its clients, and the design, support and maintenance of [Plaintiff's] computer network and infrastructure, including security functions and policies implemented to protect company and client resources." Id. at paragraph 13. He "served as the primary interface between Plaintiff and its customers for the sale and provision of customized computer services, solutions or designs" and was "integral in, and took the lead on, all aspects of the development, testing, roll-out and servicing of [Plaintiff's] customized and confidential computer services, solutions or designs." Id. at paragraph 21.

Alexander Penrose ("Penrose") is the founder, sole shareholder, President, and Chief Executive Officer of Plaintiff. Id. at paragraph 3. In 2007, Penrose was approached by Integrated Computer Solutions ("ICS"), a local competitor, regarding a potential purchase or merger between the two companies. Id. at paragraph 27. A meeting was scheduled for July 7, 2008 to discuss this transaction. Id. at paragraph 28. In anticipation of this meeting, Penrose prepared a confidential presentation and shared it only with Plaintiff's accountant. Id. at paragraph 29. Defendant accessed this presentation through Penrose's email account and emailed it to another of Plaintiff's employees. Id. at paragraph 32 and 33. Defendant then personally met with ICS, disclosing that he was aware of the potential transaction, and proposed that ICS make a deal with Defendant instead. Id. at paragraph 34. Following this meeting, ICS cancelled its meeting with Penrose and no transaction between the two companies has transpired. Id. at paragraph 37 and 39. Plaintiff terminated Defendant for this behavior. Id. at paragraph 41. Defendant then deleted his entire Exchange Email record archive, which destroyed his client contact history. Id. at paragraph 33 and 38.

Following his termination, Defendant helped found Avant IT Consulting, Inc. ("Avant IT") and began competing directly against Plaintiff. Id. at paragraph 43. Several of Plaintiff's key clients have "discontinued their relationship with [Plaintiff] and engaged Avant IT, including, but not limited to, Olum's, Lourdes Health Care System, Newman Development Group LLC, Clintwood Pharmacy, GHS Federal Credit Union and Susquehanna Community Schools." Id. at paragraph 46.

On August 7, 2009 Plaintiff commenced the instant action against Defendant alleging that Defendant violated both his common law and statutory obligations, and the express terms of the Non-Disclosure Agreement. Id. at paragraph 1. On October 16, 2009

Defendant filed this motion to dismiss. Plaintiff opposes the motion, arguing that it has sufficiently pled all causes of action, and withdraws its cause of action for tortious interference with existing contracts. See Docket No. 13.

Alternatively, Plaintiff contends that, "to the extent the Court concludes that the pleading of any claim is deficient, the Court should grant leave to re-plead." See Docket No. 10. Plaintiff cites to Fed. R. Civ. P. 15(a) which provides that "[a] party may amend the party's pleading once as a matter of course at any time before the responsive pleading is served." Plaintiff notes that "Defendant's Motion to Dismiss is not a 'responsive pleading' within the meaning of Rule 15(a)". Barbara v. New York Stock Exch., Inc., 99 F.3d 49, 56 (2d Cir. 1996).

II. STANDARD OF REVIEW

To survive a motion to dismiss, the plaintiff must provide "the grounds upon which his claim rests through factual allegations sufficient 'to raise a right to relief above the speculative level.'" Camarillo v. Carrols Corp., 518 F.3d 153, 156 (2d Cir. 2008) (citations omitted). Plaintiff's factual allegations must be sufficient to give the defendant "fair notice of what the claim is and the grounds upon which it rests." Camarillo, 518 F.3d at 156 (citing Port Dock & Stone Corp. v. Oldcastle Ne., Inc., 507 F.3d 117, 121 (2d Cir. 2007)). When ruling on a motion to dismiss, "the court must accept the material facts alleged in the complaint as true and construe all reasonable inferences in the plaintiff's favor." Burns v. Trombly, 624 F. Supp.2d 185, 196 (N.D.N.Y. 2008)(citing Hernandez v. Coughlin, 18 F.3d 133, 136 (2d Cir. 1994)). The Second Circuit has recently held, however, that "'although a court must accept as true all of the allegations contained in a complaint,' that 'tenet' 'is inapplicable to legal

conclusions,' and '[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.'" Harris v. Mills, 572 F.3d 66, 72 (2d Cir. 2009) (citing Ashcroft v. Iqbal, 129 S. Ct. 1937, 1949 (2009)).

The Second Circuit went on to hold that "whether a complaint states a plausible claim for relief will . . . be a context-specific task that requires the reviewing court to draw on its judicial experience and common sense." Harris, 572 F.3d at 72 (citing Ashcroft, 129 S. Ct. at 1950). Review is "limited to the facts asserted within the four corners of the complaint, the documents attached to the complaint as exhibits, and any documents incorporated in the complaint by reference." Medtech Prods. v. Ranir, LLC, 596 F. Supp.2d 778, 802 (S.D.N.Y. 2008) (citing McCarthy v. Dun & Bradstreet Corp., 482 F.3d 184, 190 (2d Cir. 2007); see Rothman v. Gregor, 220 F.3d 81, 88 (2d Cir. 2000)(citing Cosmas v. Hassett, 886 F.2d 8, 13 (2d Cir. 1989)) (the court may review documents integral to the Complaint upon which the plaintiff relied in drafting his pleadings, as well as any documents attached to the Complaint as exhibits and any statements or documents incorporated into the Complaint by reference.).

III. DISCUSSION

a. Computer Fraud and Abuse Act

Defendant alleges that Plaintiff failed to sufficiently plead a cognizable loss under CFAA, 18 U.S.C. § 1030, and therefore the claim should be dismissed. "The CFAA, in relevant part, provides a private federal cause of action against a person who 'intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer.'" Jet One Group, Inc. v. Halcyon Jet

Holdings, Inc., 2009 WL 2524864, at *5 (E.D.N.Y. Aug. 14, 2009) (citing 18 U.S.C. § 1030)(a)(2)). Subsection (g) of the CFAA, the civil remedy at issue in this case, states:

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV) or (V) of subsection (c)(4)(A)(i).

The only relevant subsection, (c)(4)(A)(i)(I), applies to "loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value."[1] Therefore, Plaintiff's complaint must allege "loss aggregating at least $5,000 in value" to survive Defendant's motion to dismiss. See 18 U.S.C. § 1030(c)(4)(A)(i)(I).

Defendant argues that "[t]he complaint does not plead any . . . facts from which it might be inferred that [Plaintiff] incurred losses as that term is defined in the statute. The statute defines loss as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage[2] assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11) (footnote added). This has been interpreted to mean "any remedial costs of investigating the computer for damage, remedying the damage and any costs incurred

---

[1] Subsections (II), (III), (IV) and (V) are inapplicable to the case at hand as they involve medical treatment, physical injury to any person, a threat to public health or safety, and computers used for or by the U.S. Government. 18 U.S.C. § 1030(c)(4)(A)(i)(II), (III), (IV) and (V).

[2] "Damage" is defined as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. §1030(e)(8).

because the computer cannot function while or until repairs are made." Nexans Wires S.A. v. Sark-USA, Inc., 319 F. Supp.2d 468 (S.D.N.Y. 2004), aff'd Nexans Wires S.A. v. Sark-USA, Inc., 166 Fed. Appx. 559 (2d Cir. 2006); see also Tyco Int'l Inc. v. John Does, 2003 WL 21638205 (S.D.N.Y. July 11, 2003) ("CFAA allows recovery for losses beyond mere physical damage to property, the additional types of damages awarded by courts under the Act have generally been limited to those costs necessary to assess the damage caused to the plaintiff's computer system or to resecure the system in the wake of a hacking attack."); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 584-85 (1st Cir. 2001) (awarding costs of assessing damage).

Here, the Complaint alleges that Defendant "intentionally accessed the secure, protected computers of [Plaintiff] or other protected computers without authorization or exceeding his authorization, and thereby obtained information from those protected computers," and he did so "in furtherance of the intended fraud, obtained the valuable . . . proprietary trade secrets and confidential information . . . which have a value exceeding five thousand dollars" and "as a result . . . recklessly caused damage and loss to the secure, protected computers of [Plaintiff]" in excess of $5,000. See Docket No. 1 at paragraphs 48-53. Additionally the complaint states, "Cybercity has *incurred substantial damages and/or losses*, due to [Defendant's] unauthorized access of [Plaintiff's] protected computers and unauthorized removal, possession, and impairment of [Plaintiffs's] electronic files and documents, *including, without limitation, the costs of investigating [Defendant's] actions and assessing the damage they caused*." See Docket No. 1 at paragraph 40 (emphasis added). Because Plaintiff has alleged that Defendant's unauthorized activity resulted in over $5,000 in losses, which included the cost to investigate Defendant's actions and assess the resulting

damages, Plaintiff has adequately alleged loss sufficient to withstand Defendant's motion to dismiss the CFAA claim.

b. Stored Communications Act

Defendant alleges that Plaintiff failed to sufficiently plead a cognizable claim pursuant to the SCA, because Defendant was authorized to have full access to Plaintiff's computer system. "[Section 2701], aims to prevent hackers from obtaining, altering, or destroying certain stored electronic communications." In re DoubleClick Inc. Privacy Litigation, 154 F. Supp.2d 497, 507 (S.D.N.Y. 2001). It states in relevant part:

> (a) Except as provided in subsection (c) of this section whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access [a facility through which an electronic communication service is provided] and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished . . .[3]

Subsection (c) provides, in relevant part, that "subsection (a) of this section does not apply with respect to conduct authorized --(1) by the person or entity providing a wire or electronic communication service; or (2) by a user of that service with respect to a communication of or intended for that user."

"The purpose of the SCA was, in part to protect privacy interests in personal and proprietary information and to address 'the growing problem of unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire

---

[3]"An 'electronic communications service' is 'any service which provides to users thereof the ability to send or receive wire or electronic communications." General Bd. of Global Ministries of the United Methodist Church v. Cablevision Lightpath, Inc., 2006 WL 3479332, at *3 (E.D.N.Y. Nov. 30, 2006) (citing 18 U.S.C. 2510(15); In re Doubleclock, Inc. Privacy Litigation, 154 F. Supp.2d 497, 508 (S.D.N.Y. 2001). "Communications in 'electronic storage' are those temporarily stored by electronic communication services incident to their transmission - 'for example, when an e-mail service stores a message until the addressee downloads it." General Bd. of Global Ministries of the United Methodist Church, 2006 WL 3479332, at *3 (citing In re Doubleclock, Inc. Privacy Litigation, 154 F. Supp.2d at 512).

communications that are not intended to be available to the public.'" General Bd. of Global Ministries of the United Methodist Church v. Cablevision Lightpath, Inc., 2006 WL 3479332, at *3 (E.D.N.Y. Nov. 30, 2006) (citing Kaufman v. Nest Seekers, LLC, 2006 WL 2807177, at *4 (S.D.N.Y. Sept. 26, 2006)).

It is undisputed that Plaintiff provides its employees with a computer system and e-mail accounts for work purposes. Plaintiff alleges that Defendant "twice exceeded his authorized access to the computer system and obtained, disclosed, and/or deleted confidential or trade secret information contained therein." See Docket No. 13. Plaintiff alleges that this unauthorized access occurred when Defendant: (1) "accessed Mr. Penrose's email account in order to obtain confidential business proposals regarding the potential sale of CyberCity, only to disclose this information to a fellow employee and the potential buyer - thereby undermining the transaction;" and (2) "deleted his [own] email record . . . leaving Plaintiff bereft of any of his client contact or interaction." Docket No. 13; see Docket No. 1 at paragraph 27-40.

Defendant argues that these actions were authorized because he was an "employee with full access to the system upon which the information in question was found," and that "at the time he was allegedly accessing [the stored information] for his economic benefit, his access [to the system] had not been revoked nor had information been encrypted or otherwise password protected." See Docket No. 10 . Defendant argues that his actions fall under the exception provided in § 2701 subsection (c). Thus, the issue is whether Defendant was authorized to access the presentation and to delete his email records.

1. **Accessing the Presentation**

In the Complaint, Plaintiff contends that Defendant violated the SCA when he "without authorization and in excess of his authorized access, and without [Plaintiff's] consent, intentionally, knowingly, and with intent to defraud, accessed Mr. Penrose's CyberCity email account via [Plaintiff's] protected computers and obtained proprietary information contained in the presentation." See Docket No. 1 at paragraph 32. The complaint alleges that the presentation at issue was shared only with the corporate accountant. It further alleges that Mr. Penrose sent the presentation to the accountant from his personal email account and that the accountant then sent the revised presentation back to Mr. Penrose at his CyberCity email address. Accepting, *arguendo*, that Defendant had full access to the Plaintiff's computer system, this does not support the conclusion that Defendant had authorization to access another employee's email account. "The Senate Report explaining the statute . . . [states] for example, that a subscriber to a computer mail facility would violate the statute by accessing the electronic storage of other subscribers to the facility without specific authorization to do so." Educational Testing Service v. Stanley H. Kaplan, Educational Center, Ltd., 965 F. Supp. 731, 740 (D.Md., 1997) (citing S.Rep. No. 99-541, at 9 (1986)). Therefore, Plaintiff's allegation that Defendant accessed Mr. Penrose's email account and obtained the confidential email discussing a potential sale or merger with ICS and containing the presentation at issue is sufficient to withstand a motion to dismiss.

2. **Deleting Emails**

Secondly, Plaintiff argues that Defendant violated the SCA when he deleted his email history which deleted his client contact history. Defendant alleges that accessing a computer "without authorization" occurs when no authorization was given to use the

computer system. Likewise, Defendant contends that exceeding authorization occurs when authorization was granted for general access but the specific information that was accessed was restricted. Defendant argues that because he had full access to the computer system and his personal email, his actions in deleting his email and contacts, were authorized under the statute. Plaintiff counters that Defendant's authorization to access Plaintiff's computer system was premised on an agency relationship between the parties. Therefore, Plaintiff contends that when Defendant breached his duty of loyalty, this relationship ended and Defendant's authorization to access Plaintiff's files was likewise constructively terminated. See Docket No. 13, Plaintiff's Response in Opposition ("An employee may act 'without authorization' or 'in excess of authorized access' when he accesses confidential or proprietary business information from his employer's computers that he has permission to access, but then uses that information in a matter that is inconsistent with the employer's interests or in violation of contractual obligations or fiduciary duties.").

Although the Second Circuit Court of Appeals has not addressed this issue, Plaintiff's position finds support from the Eastern District of Missouri in its decision in Lasco Foods, Inc. v. Hall and Shaw Sales, Marketing, and Consulting, LLC, 2009 WL 3523986, at *5 (E.D.Mo. October 26, 2009). There, the court found that "[w]hile [plaintiff] afforded Defendants access to its computers, networks, and Information for purposes of their employment, [plaintiff] alleged that [defendants] accessed [plaintiff's] information to benefit the interests of Defendants, not [plaintiff]. . . . [Therefore, defendants'] authorization to access this information ceased when they breached their duty of loyalty to [plaintiff] and their employment terminated." Other courts have adopted this reasoning in the context of the CFAA and its interpretation of "authorization" and "exceeds authorization." Nilfis-Advance,

Inc. v. Mitchell, 2006 WL 827073, at *2 (W. D. Ark., Mar. 28, 2006)(finding that Defendant "exceeded any authorization he had when he e-mailed the files to his personal computer with the alleged purpose of misappropriating the information contained in them."); Personalized Brokerage Servs., LLC v. Lucius, 2006 WL 208781, at *2 (D. Minn., Jan. 26, 2006) ("An employee who exceeds authorized access to an employer's computer may violate the CFAA."); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp.2d 1121, 1125 (W.D. Wash. 2000) ("Under this rule, the authority of the plaintiff's former employees ended when they allegedly became agents of the defendant. Therefore, for the purposes of this 12(b)(6) motion, they lost their authorization and were 'without authorization' when they allegedly obtained and sent the proprietary information to the defendant via e-mail.")(citing Restatement (Second) of Agency § 112 (1958)). Additionally, the District Court of the Southern District of New York adopted this reasoning in the context of the CFAA, stating that "[c]ourts in other circuits have interpreted [ ] 'without authorization' and 'exceeds authorized access' in different ways. . . . [T]he plain language of the statute seems to contemplate that, whatever else, 'without access' and 'exceeds authorized access' would include an employee who is accessing documents on a computer system which that employee had to know was in contravention of the wishes and interests of his employer." Calyon v. Mizuho Securities USA, Inc., 2007 WL 2618658, at *1 (S.D.N.Y. July 24, 2004) (comparing Intern. Ass'n of Machinists v. Werner-Masuda, 390 F. Supp.2d 479 (D. Md. 2000); Secureinfo Corp. v. Telos Corp., 387 F. Supp.2d 593 (E.D. Va. 2005); Lockheed Martin Cop. v. Speed, 2006 WL 2683058 (M.D. Fla. Aug. 1, 2006) with Shurgard Storage Centers v. Safeguard Self Storage, 119 F. Supp.2d 1121 (W.D. Wash. 2000); International Airport Centers, L.C.C. v. Citrin, 440

F.3d 418 (7th Cir. 2006); Pharmerica, Inc. v. Arledge, 2007 WL 865510 (M.D. Fla. March 21, 2007)).

Defendant's position is also supported by case law. In International Ass'n of Machinists and Aerospace Workers v. Werner, 390 F. Supp.2d 479,496 (D. Md., 2005), the court quoted the Eastern District of Michigan stating that "[b]ecause section 2701 prohibits only unauthorized access and not the misappropriation or disclosure of information, there is no violation of section 2701 for a person with authorized access to the database no matter how malicious or larcenous his intended use of that access. . . . [S]ection 2701 outlaws illegal entry, not larceny." See also Educational Testing Service v. Stanley H. Kaplan, Educational Center, Ltd., 965 F. Supp. 731, 740 (D. Md. 1997) ([T]he sort of trespasses to which the Stored Communications Act applies are those in which the trespasser gains access to information to which he is not entitled to see, not those in which the trespasser uses the information in an unauthorized way.). "Moreover, although Congress did not define the phrase "without authorization" in either the SECA or the CFAA, it did provide a statutory definition for the phrase "exceeds authorized access" in the CFAA . . . [which means] 'to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter.'" 18 U.S.C. § 1030(e)(6)." International Ass'n of Machinists and Aerospace Workers v. Werner-Masuda, 390 F. Supp.2d 479, 498 (D. Md. 2005).

Here it is undisputed that Defendant was authorized to access his email account, send messages, and control his inbox. This authorization therefore included the ability to delete certain messages which may have included client history. The Court is not persuaded by Plaintiff's argument and finds that although the messages deleted contained information

useful to the company, their deletion was authorized within the meaning of the SCA. Therefore, the Court finds that Defendant's deletion did not exceed authorization and, therefore, cannot support a cause of action under the SCA.

c. Breach of Contract[4]

Defendant alleges that Plaintiff failed to sufficiently plead a claim for breach of contract because the non-disclosure agreement is not a covenant against competition, and that, therefore, the claim should be dismissed. Specifically, Defendant alleges that Plaintiff's complaint "fails to plead exactly what provision of the non-disclosure agreement [Defendant] actually violated, when he violated it, and what he did to violate it." See Docket No. 10. "In a breach of contract claim, a plaintiff must 'plead the provisions of the contract upon which the claim is based.'" Phoenix Four, Inc. v. Strategic Resources Corp., 2006 WL 399396, at *10 (S.D.N.Y. Feb. 21, 2006).

Plaintiff's complaint "re-states verbatim the relevant provisions of the non-disclosure agreement." See Docket No. 13; Docket No. 1 at paragraphs 15-18. The relevant provisions, both in paragraph (a), state:

> The Employee shall keep secret and retain in strictest confidence and not use or disclose, furnish or make accessible to anyone outside the Employer . . . or use for the benefit of himself/herself or others except in connection with the business of Employer . . . any Protected Information in any Unauthorized manner or any Unauthorized purposes.
>
> The term "Protected Information" shall mean trade secrets, confidential or proprietary information and all other knowledge, know-how, information, documents or materials owned, developed or possessed by Employer or any of its subsidiaries, divisions or affiliates, whether in tangible or intangible form, pertaining to the business of Employer or any of its subsidiaries,

[4] The Parties agree that New York law governs each of the state law claims asserted in this case.

> divisions, affiliates, including, but not limited to, research and development operations, systems, databases (including membership databases), computer programs and software, designs, models, operating procedures, knowledge of the organization, products and services (including prices, costs, sales or content), processes, techniques, contracts, financial information or measures, business methods, future business plans, details of consultant contracts, new personnel acquisition plans, business plans, customers and suppliers (including identities of customers and prospective customers and suppliers, identities of individual contacts at business entities which are customers or prospective customers or suppliers, preferences, businesses or habits), business relationships and other information owned, developed or possessed by Employer or its subsidiaries, divisions or affiliates, except as required in the course of performing duties hereunder; provided however, that Protected Information shall not include information that shall become generally known to the public or the trade without violation of this Agreement.

See Id. at paragraphs 16-17. Furthermore, Plaintiff's complaint "alleges that [Defendant] breached the non-disclosure agreement . . . [when he] disclosed the contents of the confidential information to be presented to [ICS] . . . [and when he] utilized the highly confidential and trade secret information of [Plaintiff] and its customers in marketing Avant IT's services to [Plaintiff's] customers." See Docket No. 1 at paragraphs 33, and 45-47. Plaintiff's Complaint sufficiently states a cause of action for breach of contract.

d. Misappropriation of Trade Secrets

Defendant alleges that Plaintiff failed to sufficiently plead a claim for misappropriation of trade secrets and, therefore, the claim should be dismissed. Specifically, Defendant argues that Plaintiff's "complaint fails to state any facts that would lead to the conclusion that [Defendant] possessed trade secrets as opposed to general business knowledge gained from his experience, or that [Defendant] has used any alleged trade secrets in his business dealings since leaving [Plaintiff]." See Docket No. 10.

"To succeed on a claim for the misappropriation of trade secrets under New York law, a party must demonstrate: (1) that it possessed a trade secret, and (2) that the defendants used that trade secret in breach of an agreement, confidential relationship or duty, or as a result of discovery by improper means." Faiveley Transport Malmo AB v. Wabtec Corp., 559 F.3d 110, 117 (2d Cir. 2009) (quoting N. Atl. Instruments, Inc. v. Haber, 188 F.3d 38, 43-44 (2d Cir. 1999)). "A trade secret is any formula, pattern, device or compilation of information which is used in one's business, and which gives the owner an opportunity to obtain an advantage over competitors who do not know or use it." Id. (internal quotation marks and brackets omitted). "In determining whether information constitutes a trade secret, New York courts have considered:

> (1) the extent to which the information is known outside of the business; (2) the extent to which it is known by employees and others involved in the business; (3) the extent of measures taken by the business to guard the secrecy of the information; (4) the value of the information to the business and its competitors; (5) the amount of effort or money expended by the business in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.

Id. (quoting Ashland Mgmt., Inc. v. Janien, 82 N.Y.2d 395, 407, 604 N.Y.S.2d 912, 624 N.E.2d 1007 (1993)). Furthermore, "confidential proprietary data relating to pricing, costs, systems, and methods are protected by trade secret law." In re Dana Corp., 574 F.3d 129 (2d Cir. 2009); see generally Lehman v. Dow Jones & Co., 783 F.2d 285, 298 (2d Cir. 1986).

Plaintiff's Complaint identifies as protected trade secrets its "customized and confidential computer services, solutions or designs for its clients, as well as its cost structure, supply vendors, customer relationships, sales strategies, customer files, customer lists and identities, and other confidential and proprietary information not known to the general public." See Docket No. 1 at paragraphs 19-26. The Complaint states that Plaintiff "has taken careful

measures to treat this information as highly confidential" by "among other things, requiring all employees to sign Non-Disclosure Agreements upon hiring." Id. at 26. Plaintiff's customized computer solutions are individually developed "after gaining intimate knowledge of the specific needs and unique IT infrastructure and framework of each client" and through the expenditure of significant time and resources. Id. at 19-20. Additionally, Plaintiff's customized approach creates a competitive advantage because it allows Plaintiff to develop and provide "maintenance services and project upgrades" for its clients. Id.

The Complaint alleges that Defendant had access to and "gained intimate knowledge of" these trade secrets through his employment with Plaintiff because Defendant was the "primary interface between [Plaintiff] and its customers for the sale and provision of customized computer services, solutions or designs" and Defendant "took the lead on, all aspects of the development, testing, roll-out and servicing of [Plaintiff's] customized and confidential computer services, solutions or designs." Id. Furthermore, Plaintiff's complaint alleges that upon founding Avant IT Defendant "immediately began soliciting [Plaintiff's] clients" and "persuaded many [of Plaintiff's] clients to undergo 'assessments,' in which [Defendant] utilized highly confidential information and trade secrets regarding the client's information technology systems - which he obtained during his employment with [Plaintiff] - in order to market additional services to these clients." Id. at 44-45. Because Plaintiff has alleged that Defendant learned Plaintiff's confidential information through his employment and then used that information to compete against Plaintiff, Plaintiff has sufficiently plead a claim for misappropriation of trade secrets.

e. Breach of Fiduciary Duty and Unfair Competition

Defendant argues that Plaintiff failed to sufficiently plead a claim for breach of fiduciary duty, duty to preserve good will, or unfair competition because Defendant owed no further fiduciary duty to Plaintiff after he was terminated. Defendant attacks the Complaint on the grounds that it involved Defendant's conduct after he left Plaintiff's employment.

1. **Unfair Competition**

Under New York law, . . . [an] unfair competition claim, 'usually concerns the taking and use of the plaintiff's property to compete against the plaintiff's use of the same property.'" American Bldg. Maintenance Co. of New York v. Acme Property Services, 515 F. Supp.2d 298, 311 (N.D.N.Y. 2007) (quoting Roy Exp. Co. Establishment v. Columbia Broadcasting Sys., Inc., 672 F.2d 1095, 1105 (2d Cir. 1982). "Courts have found that the misappropriation of detailed, internal customer information can give rise to a claim of unfair competition, but only when that customer information has several of the attributes of a trade secret and is being used in breach of an agreement, confidence, or duty." Id. (citing Integrated Cash Mgmt. Servs., Inc. v. Digital Transactions, Inc., 920 F.2d 171, 173 (2d Cir. 1990); Innoviant Pharm., Inc. v. Morganstern, 390 F. Supp.2d 179, 194 (N.D.N.Y. 2005). Here, as described *supra,* Plaintiff has adequately alleged misappropriation of trade secrets and that the misappropriation was in violation of a non-disclosure agreement.

2. Breach of Fiduciary Duty

"A fiduciary relationship exists under New York law when one [person] is under a duty to act for or to give advice for the benefit of another upon matters within the scope of the relation." Boccardi Capital Systems, Inc. v. D.E. Shaw Laminar Portfolios, L.L.C., 2009 WL 4640652, at *2 (2d Cir. Dec. 9, 2009) (citing Flickinget v. Harold C. Brown & Co., 947 F.2d 595,

599 (2d Cir. 1991)). "New York imposes a duty not to use trade secrets in competition with a former employer." North Atlantic Instruments, Inc. v. Haber, 188 F.3d 38, 47 (2d Cir. 1999); see ABKCO Music Inc. v. Harrisongs Music, Ltd., 772 F.2d 988, 994 (2d Cir. 1983) ("an agent has a duty not to use confidential knowledge acquired in his employment in competition with his principal") (citing Byrne v. Barrett, 268 N.Y. 199, 206 (1935)). This duty "exists as well after the employment is terminated as during its continuance." Id.; accord L.M. Rabinowitz & Co. v. Dasher, 82 N.Y.S.2d 431, 435 (Sup. Ct. New York County 1948) ("It is implied in every contract of employment that the employee will hold sacred any trade secrets or other confidential information which he acquires in the course of his employment. This is a duty that the employee assumed not only during his employment but after its termination.").

Here, Plaintiff alleges not only that Defendant used his knowledge and skills to compete against Plaintiff but that Defendant used confidential trade secret information in violation of the non-disclosure agreement to compete. Because, as discussed *supra*, Plaintiff has adequately alleged that Defendant used Plaintiff's trade secrets to compete against Plaintiff, Plaintiff has adequately alleged a breach of fiduciary duty.

f. Tortious Interference

Defendant alleges that Plaintiff failed to sufficiently plead a claim for tortious interference with contract or any version of tortious interference with prospective economic advantage and, therefore, the claims should be dismissed.[5]

[5] Plaintiff complaint's alleges tortious interference with prospective economic relations and tortious interference with prospective business advantage.

1. **Tortious Interference with Contract**

Defendant contends that Plaintiff does not allege the existence of any contract and that "even if [Plaintiff] had such [an] agreement, it would be insufficient to support a cause of action for tortious interference unless they were not terminable at the whim of the parties." Plaintiff withdraws its cause of action for tortious interference with existing contracts. See Docket No. 13 FN1. Therefore, Plaintiff's cause of action alleging tortious interference with contract is dismissed.

2. **Tortious Interference with Prospective Economic Advantage**

Defendant next argues that Plaintiff's claims alleging tortious interference with prospective economic advantage must fail because: (1) Plaintiff failed to "plead exactly which current purchasers were dissuaded from purchasing [Plaintiff's] products;" and (2) "nothing in Plaintiff's complaint raises to the level of tortious interference." See Docket No. 10 (internal citations omitted). Defendant also contends that Plaintiff's claims alleging interference with relationships not yet in existence must fail because they are not "existing economic relationships." See Docket No. 10.

"Under New York law, in order to make out a prima facie case for tortious interference with prospective economic advantage, a plaintiff must establish '(1) that [he] had a business relationship with a third party; (2) the defendant knew of that relationship and intentionally interfered with it; (3) the defendant acted solely out of malice, or used dishonest, unfair, or improper means; and (4) the defendant's interference caused injury to the relationship.'" Friedman v. Coldwater Creek, Inc., 321 Fed. Appx. 58, 59-60 (2d Cir. 2009) (citing Kirch v. Liberty Media Corp., 449 F.3d 388, 400 (2d Cir. 2006)).

a. Current Customers

Defendant alleges that Plaintiff failed to "plead exactly which current purchasers were dissuaded from purchasing [Plaintiff's] products." This allegation ignores paragraph 46 of Plaintiff's Complaint which states that "[a]s a result of [Defendant's] unlawful actions, several key clients have discontinued their relationship with [Plaintiff] and engaged Avant IT, including, but not limited to, Olum's, Lourdes Health Care System, Newman Development Group LLC, Clintwood Pharmacy, GHS Federal Credit Union and Susquehanna Community Schools." Therefore, this argument is without merit.

b. Tortious Interference

Defendant next alleges that "nothing in Plaintiff's complaint rises to the level of tortious interference." See Docket No. 10. The New York Court of Appeals has explained that, "as a general rule, a defendant's conduct must amount to a crime or an independent tort" in order to amount to a tortious interference with a prospective economic advantage. Carvel Corp. v. Noonan, 3 N.Y.3d 182, 190, 785 N.Y.S.2d 359, 818 N.E.2d 1100 (2004)). Here, because Plaintiff has sufficiently alleged that Defendant's conduct: (1) violated the CFAA and the SCA; (2) resulted in misappropriation of trade secrets; and (3) breached fiduciary duties, Plaintiff has sufficiently alleged tortious interference.

c. Prospective Purchaser

Defendant, next, contends that because a "prospective purchaser" can not satisfy the element of an existing economic relationship, Plaintiff's allegation that Defendant interfered with the sale to ICS fails as a matter of law. "Tortious interference with prospective economic relations requires an allegation that plaintiff would have entered into an economic relationship but for the defendant's wrongful conduct." Premium Morg. Corp. v. Equifax, Inc., 583 F.3d 103,

107 (2d Cir. 2009) (citing Vigoda v. DCA Prods. Plus Inc., 293 A.D.2d. 265, 741 N.Y.S.2d 20, 23 (1st Dep't 2002)). Here, although there are no factual allegations that a merger or sale would have occurred but for Defendant's actions, a jury could conclude that Plaintiff and ICS were in a business relationship - - looking to buy or merge - - although not consummated at the time Defendant interfered.

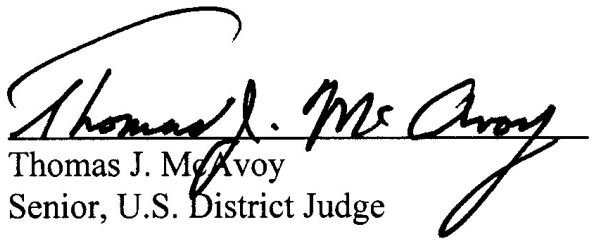
Therefore, Plaintiff's claim for tortious interference with prospective economic advantage withstands Defendant's motion to dismiss.

IV. CONCLUSION

For the foregoing reasons, Defendant's Motion to Dismiss is GRANTED as to Plaintiff's claim under the Stored Communications Act and Tortious Interference with Contact. In all other respects Defendant's motion is DENIED.

IT IS SO ORDERED.

Dated: January 22, 2010



Thomas J. McAvoy
Senior, U.S. District Judge