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

BRETT SENIOR & ASSOCIATES, P.C.,	:	
Plaintiff,	:	CIVIL ACTION
v.	:	
STEPHEN C. FITZGERALD, et al.,	:	
Defendants	:	NO. 06-1412

MEMORANDUM AND ORDER

McLaughlin, J. July 13, 2007

Brett Senior & Associates ("BSA") has sued a former employee, Stephen Fitzgerald, and Fitzgerald's current employer, Fesnak & Associates ("Fesnak"), alleging that they misused confidential BSA information in violation of the Computer Fraud and Abuse Act. BSA also brings several common law claims against both defendants, who have moved for summary judgment. The Court will grant the motion on all claims except the breach of fiduciary duty claim against Fitzgerald.

I. Facts

In 1989, Stephen Fitzgerald was hired by BSA, a law firm, to perform tax, accounting and financial services. He did not sign an employment agreement, and he remained an at-will

employee throughout his tenure at BSA.

BSA began restructuring its business in 1998 to include investment advice and estate planning. In preparation for these new practice areas, BSA required its employees to sign confidentiality agreements, which were presented to BSA employees, including Fitzgerald, at a June 29, 1999 meeting. The agreements were entitled "Company Policies on Conflict of Interest, Gifts and Disclosures of Confidential Information" ("policy document"). At the meeting, Brett Senior ("Senior"), the founder of BSA, reviewed the policy document with the employees, who signed it thereafter. Since the meeting, every full-time employee of BSA has signed a policy document similar to the one signed by Fitzgerald.

BSA alleges that Fitzgerald received numerous benefits in consideration for signing the policy document, including income, the opportunity to participate in business ventures, increased managerial responsibilities, liability insurance, a cell phone, a computer for home use, an upgraded expense account, an enhanced automobile allowance, and prepayment of tuition and expenses for a master's degree in taxation. Fitzgerald denies that these benefits were provided in consideration for signing the policy document.

In January of 2005, Fitzgerald had a job interview with representatives of Fesnak, a firm which provides tax and

accounting services. While in discussion with Fesnak about potential employment, he created a list, which he showed to several Fesnak partners, of approximately 69 clients that he serviced at BSA. The list included: (1) the fees paid by 48 clients; (2) the services performed (either "review & tax returns," "compilation & tax returns," or "bookkeeping through tax returns") for 15 clients; and (3) a telephone number for 11 clients.

On November 10, 2005, Fitzgerald told BSA that he had accepted a job with Fesnak. Between November 10 and December 2, Fitzgerald's last day at BSA, both Senior and Fitzgerald contacted clients and informed them of Fitzgerald's impending departure. Fitzgerald contacted approximately twenty clients and asked them to come with him to Fesnak. Fifteen did so.[1]

Before his departure, Fitzgerald made copies of certain information in his files. He copied to a CD and an external hard drive tax information for clients with whom he signed engagement letters, clients for whom he was the contact person, and clients whom he brought into BSA. Fitzgerald also emailed to Fesnak the engagement letters and financial statements of the four clients with whom he signed engagement letters. To facilitate the transfer of information, certain files were converted to ZIP or

[1] After he left BSA, Fitzgerald contacted 19 clients that he serviced at BSA. Fourteen followed him to Fesnak.

PDF format.

There is no evidence that the information copied to the CD or hard drive or emailed to Fesnak was ever used by either defendant. After Senior warned Fitzgerald on December 2, 2005 not to use information taken from BSA, Fitzgerald obtained client information from his work papers and the clients themselves.

II. Claims

BSA raises nine claims: six against both Fitzgerald and Fesnak, two against Fitzgerald alone, and one against Fesnak alone. It claims that both defendants: (1) violated the Computer Fraud and Abuse Act ("CFAA"); (2) misappropriated BSA's trade secrets; (3) misappropriated BSA's confidential business information; (4) unfairly competed with BSA; (5) tortiously interfered with BSA's former clients; and (6) engaged in an unlawful conspiracy.

BSA alleges that Fitzgerald breached his contract (the policy document) and that Fesnak tortiously interfered with the contract. Finally, it alleges that Fitzgerald breached his fiduciary duty to BSA.

III. Analysis[2]

The Court will first consider whether Fitzgerald violated the CFAA. Although the Court concludes that he did not and therefore will dismiss the plaintiff's only federal claim, it will exercise jurisdiction over the plaintiff's state-law claims in accordance with the wishes of both parties. Tr. at 26-28.

The Court concludes that the plaintiff's state law claims are deficient as a matter of law, with one exception. The claims relating to the policy document fail because the document was not a binding contract; the misappropriation and unfair competition claims fail because the information taken by Fitzgerald was not confidential nor the property of BSA; and the claim based on tortious interference with BSA's clients fails because BSA has not produced evidence that its relationship with its clients was contractual. The breach of fiduciary duty claim, however, survives to the extent that it challenges Fitzgerald's pre-departure solicitation of BSA's clients. Because there is no evidence that Fesnak encouraged Fitzgerald to breach his fiduciary duty, the claim proceeds against Fitzgerald alone.

---

[2] On a motion for summary judgment, a court must view the evidence and draw reasonable inferences therefrom in the light most favorable to the party opposing summary judgment. See, e.g., Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 255 (1986). Summary judgment is proper if the pleadings and other evidence on the record "show that there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law." Fed. R. Civ. P. 56(c) (2006).

A. The CFAA

The Computer Fraud and Abuse Act is a criminal statute that contains a civil enforcement provision. In relevant part, the statute provides:

> Whoever...knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value...shall be punished as provided in subsection (c) of this section.

18 U.S.C. § 1030(a)(4).[3] To show a violation of section (a)(4), a plaintiff must prove that: "(1) [the] defendant has accessed a 'protected computer;' (2) has done so without authorization or by exceeding such authorization as was granted; (3) has done so 'knowingly' and with 'intent to defraud;' and (4) as a result has 'further[ed] the intended fraud and obtain[ed] anything of value.'" P.C. Yonkers, Inc. v. Celebrations: The Party and Seasonal Superstore, LLC, 428 F.3d 504, 508 (3d Cir. 2005). Section 1030(g) allows a party who has suffered loss from a violation of section (a)(4) to recover compensatory damages.

The plaintiff claims that Fitzgerald violated section (a)(4) by accessing the BSA computer system to transfer BSA files to Fesnak. Specifically, it claims that Fitzgerald violated

[3] A violation of section (a)(4) is a felony punishable by a fine or imprisonment for up to 5 years for a first offense and up to ten years for a subsequent offense. Id. § 1030(c)(3)(A), (B).

section (a)(4) when he: (1) copied BSA's client files to an external hard drive and to a CD; (2) created a list of the clients he serviced at BSA; (3) transformed BSA's files to PDF or ZIP formats for the purpose of transferring them to Fesnak; and (4) emailed information relating to four BSA clients to Fesnak.

The parties agree that the main question presented by the CFAA claim is whether Fitzgerald's actions satisfy the second element of an (a)(4) claim. In other words, did Fitzgerald access a computer "without authorization" or "exceed[]" his "authorized access"? The plaintiff argues that the latter phrase is applicable, but the text of the statute, the rule of lenity, and legislative history show otherwise.

The CFAA defines "exceeds authorized access" as accessing "a computer with authorization" and using "such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." Id. § 1030(e)(6). By its plain terms, this definition does not apply to Fitzgerald's conduct. He did not obtain any information that he was not entitled to obtain or alter any information that he was not entitled to alter. As Senior testified at his deposition, Fitzgerald was allowed full access to information contained in the BSA computer system until his departure. Defs.' Br. in Supp. Ex. B at 174-75.

The plaintiff does not argue that there was anything

per se actionable about Fitzgerald converting his files to ZIP or PDF format, making a list of his clients, or copying client information to an external hard drive or a CD. Instead, it alleges that the use of this appropriately-obtained information was improper. See Pl.'s Br. in Opp. at 20; Tr. at 21-22. The conduct targeted by section (a)(4), however, is the unauthorized procurement or alteration of information, not its misuse or misappropriation. Because there is no allegation that Fitzgerald lacked authority to view any information in the BSA computer system, the CFAA claim fails.

The legislative history of the CFAA confirms this reading of the unlawful access requirement. The provisions of section 1030 differ, but liability under each requires at a minimum that a defendant "access without authorization" or "exceed[] authorized access." Orin S. Kerr, Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N.Y.U. L. Rev. 1596, 1615-16 (2003). The Senate Committee on the Judiciary, which authored section (a)(4), viewed the requirement as tantamount to trespass in a computer. Thus, it saw section (a)(3), which requires only unlawful access, as a "simple trespass offense." S. Rep. 99-432, at 7 (1986). In contrast, section (a)(4), requiring both computer trespass and an intent to defraud, was seen as outlawing "computer theft." Id.

at 9-10.[4] Fitzgerald therefore cannot be liable under the statute unless he, at a minimum, trespassed into BSA's computer system. The lawfulness of his entry defeats the CFAA claim.

Even if the statute allowed for the plaintiff's interpretation, the Court would find that Fitzgerald had not violated section (a)(4) because of the rule of lenity, which requires a court to construe ambiguous criminal statutes in favor of the defendant. U.S. v. Edmonds, 80 F.3d 810, 820 (3d Cir. 1996). The rule of lenity applies to the construction of a statute in a civil setting if, as here, the statute has criminal applications. U.S. v. Thompson/Center Arms Co., 504 U.S. 505, 517-18 (1992). In this case, application of the rule of lenity would require the Court to favor the narrower interpretation offered by the defendants.

The plaintiff relies heavily on caselaw to support its interpretation of section (a)(4), but courts are divided on whether an employee in Fitzgerald's position, who obtains information for an allegedly improper purpose, exceeded his authorized access. Compare Lockheed Martin Corp. v. Speed, 2006 WL 2683058 (M.D. Fla. 2006); Int'l Ass. of Machinists and Aerospace Workers v. Werner-Masuda, 390 F.Supp.2d 479 (D. Md.

---

[4] As originally enacted, section (a)(4) forbade unlawful access of a "Federal interest computer." Congress substituted "protected computer" for this phrase in 1996. See Economic Espionage Act of 1996, Pub. L. No. 104-294 § 201(1)(D)(i).

2005); SecureInfo Corp. v. Telos Corp., 387 F.Supp.2d 593 (E.D. Va. 2005)(finding that access was fully authorized and therefore no CFAA claim was stated) with EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001); Nilfisk-Advance, Inc. v. Mitchell, 2006 WL 827073 (W.D. Ark. 2006); George S. May Int'l Co. v. Hostetler, 2004 WL 1197395 (N.D. Ill. 2004); HUB Group, Inc. v. Clancy, 2006 WL 208684 (E.D. Pa. 2006); Int'l Sec. Mgmt. Group, Inc. v. Sawyer, 2006 WL 1638537 (M.D. Tenn. 2006)(finding that, under facts presented, the employee exceeded his authorized access).[5]

The Court agrees with the former cases. The common thread running through the latter cases is a focus on the employee's motive for accessing a computer and his or her intended use of the information obtained.[6] As stated above,

---

[5] Several courts have held that an employee in Fitzgerald's position violated the CFAA because he or she acted "without authorization." See, e.g., Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir 2006); Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F.Supp.2d 1121 (W.D. Wash. 2000). The plaintiff does not argue that the phrase is applicable here.

P.C. Yonkers is also inapplicable, as the plaintiffs in that case argued only that the access was "without authorization." The Court did not reach the issue because it held that the plaintiffs had failed to show intent to defraud. 428 F.3d at 506-07, 510.

[6] Explorica, 274 F.3d at 583 (defendant's use of information went "beyond any authorized use" of the plaintiff's website); Nilfisk-Advance, Inc., 2006 WL 827073 at *2 (the defendant "exceeded any authorization he had when he e-mailed the files to his personal computer with the alleged purpose of

however, this interpretation reads section (a)(4) as if it said "exceeds authorized use" instead of "exceeds authorized access."

The cases relied on by the plaintiff raise additional problems. First, in looking to the use to which an employee is permitted to put information, the cases often make the existence of a confidentiality or non-compete agreement dispositive of liability under the CFAA. It is unlikely that Congress, given its concern "about the appropriate scope of Federal jurisdiction" in the area of computer crime, intended essentially to criminalize state-law breaches of contract. S. Rep. 99-432, at 3 (1986).

Second, the point of the access requirement, as explained by the Senate Committee, is to ensure that the use of the computer is integral to the perpetration of a fraud, in contrast to the more expansive definitions of mail and wire fraud. Id. at 8-9. In the plaintiff's reading, however, the computer is not the locus of the wrongful conduct, but merely the

---

misappropriating the information contained in them"); George S. May Int'l Co., 2004 WL 1197395 at *3 ([the defendant's] authorization did not extend to removing copyrighted materials from the computer system for his personal benefit or that of a competitor"); HUB Group, Inc., 2006 WL 208684 at *4 ("[the defendant] admitted that he took the information to use as a TTS [his prospective employer] employee....[The defendant] exceeded the scope of his authorization into the database..."); Sawyer, 2006 WL 1638537 at *21 ("There is no dispute that [the defendant] exceeded his authority when he e-mailed [to competitors] documents that [the plaintiff] considers proprietary").

fortuitous place where the information was obtained.[7]

Finally, the cases relied on by the plaintiff conflate the elements of a section 1030(a)(4) claim, which requires both unlawful access and an intent to defraud. P.C. Yonkers 428 F.3d at 508. In looking to an offender's motivation in accessing information in determining whether the unlawful access requirement has been met, the plaintiff seeks to collapse these independent requirements into a single inquiry: whether the offender intended to use impermissibly the information obtained. The plaintiff's interpretation thus runs afoul of the general rule that if possible, courts should adopt constructions that recognize each element of a statute. See, e.g., Ki Se Lee v. Ashcroft, 368 F.3d 218, 223 (3d Cir. 2004).[8]

B. Is the Policy Document Binding?

Two of the plaintiff's claims -- breach of contract against Fitzgerald and tortious interference with contractual

---

[7] Under the plaintiff's view, turning over information to a competitor would be a violation of the CFAA if obtained from a computer but not, for example, from a wastebasket, even though the defendant was permitted to access the information in the computer.

[8] This canon of statutory construction applies with especial force in this case, where Congress has expressed its desire to make a "clear distinction" between computer trespass, requiring only unlawful entry, and computer theft offenses, requiring in addition an intent to defraud. S. Rep. 99-432, at 10 (1986).

relations against Fesnak -- presuppose that the policy document is a binding contract. When determining whether an enforceable contract has been created, a court looks to: (1) whether both parties manifested an intention to be bound by the agreement; (2) whether the terms of the agreement are sufficiently definite to be enforced; and (3) whether there was consideration. ATACS Corp. v. Transworld Communications, 155 F.3d 659, 666 (3d Cir. 1998). The Court concludes that the policy document is not binding because of the lack of evidence supporting any of these elements.

The first section of the policy document states:

> "This communication sets forth the Company's policies on conflict of interest, gifts and disclosures of confidential information...These policies have been enacted to remind each employee to avoid [conflicts or the appearance of conflicts]....The Company requires an employee annually....to confirm his/her understanding of these policies..."

The second part, titled "What Constitutes a Conflict of Interest?," contains three subparts: (1) Conflicting Financial Interests; (2) Gifts; and (3) Disclosure of Confidential Information. The third subpart states that an employee may not disclose to a competitor confidential or proprietary information, including client lists, if the information is not generally known to the public. It further states that the employee acknowledges, "by executing this statement of policy," that the company can obtain injunctive relief against the employee if the employee

threatens to disclose confidential information.

The third section states, "I have read and understand the above policies. I have observed and will continue to observe them carefully. I agree to the provisions contained in Section II.3 above..."

Finally, in the fourth section, the document states that the signor understands that he or she is an at-will employee and that the terms of the agreement, which are to be governed by Pennsylvania law, shall survive his or her termination. The document contains a place for the signature of the employee and a witness.

The first element of contract formation, intent, cannot be discerned from the face of the policy document, which reads not as a binding contract but as a self-described "reminder" of company policies. Nor can intent be inferred from the circumstances surrounding the document's signing. The agreements were presented at once to a group of employees, who read the policies together. This procedure is consistent not with an individual meeting of the minds but rather a company's announcement of its ground rules. The facts support only one conclusion: that the document is a "statement of policy," as it states in the second section. Fitzgerald's signature at the end of the document serves, then, to confirm his awareness of the policies, a conclusion supported by the fact that the document is

countersigned not by another contracting party but by a "witness."

Evidence of the second element of contract formation, sufficiently definite terms, is also lacking. The document contains no reference to any obligation owed by BSA, and consequently the bounds of any agreement between the parties cannot be made out. The plaintiff points to the various benefits conferred on Fitzgerald, but listing his employment benefits does not establish that it had burdened itself with an enforceable obligation to provide them.

The plaintiff has therefore also failed to show the third element, that the policy document was supported by consideration. Because the policy document was signed en masse, the plaintiff must take one of two positions: either it was binding on all employees, supported by consideration in each case, or it was binding on some, depending on whether the employee received an augmented benefits package somewhere around the time he or she signed the document. Both possibilities are implausible, and neither has any support in the record. The plaintiff has therefore failed to show that a dispute of material fact exists as to whether a binding contract existed. The claims of breach of contract against Fitzgerald and tortious interference with contract against Fesnak will therefore be dismissed.

C. Misappropriation of Trade Secrets

The plaintiff claims that Fitzgerald misappropriated its trade secrets in violation of the Pennsylvania Uniform Trade Secrets Act ("PTSA"). Specifically, the plaintiff alleges that Fitzgerald's use of the information on the client list (client names and telephone numbers, services performed, and prices charged) enabled him to lure away BSA clients.[9] The Court concludes that this information is not entitled to trade secret protection because it was not proprietary and it was available from other sources.

The PTSA defines a trade secret as "information including a formula, drawing, pattern, [or] compilation including a customer list...that [d]erives independent economic value... from not being generally known to, and not being readily ascertainable by proper means by, other persons...." 12 Pa. Stat. Ann. § 5302. In considering whether information is a trade secret, a court may consider: (1) the extent to which it is known outside the owner's business; (2) the extent to which it is known by employees and others involved in the owner's business; (3) the measures taken by the owner to guard the secrecy of the information; (4) the value of the information to the owner and

[9] The plaintiff has not argued that the tax documents taken by Fitzgerald are a part of its misappropriation claim. Because these documents were never used, the plaintiff cannot show damages flowing from their misappropriation.

his competitors; (5) the amount of effort or money expended by the owner in developing the information; and (6) the ease or difficulty with which the information could be properly acquired by others. Iron Age Corp. v. Dvorak, 880 A.2d 657, 663 (Pa. Super. Ct. 2005).[10]

Although customer lists may be entitled to protection as trade secrets, they are at the "very periphery" of the law of unfair competition. Id. at 663 (citation omitted). A determination of whether a particular compilation of customer data merits protection as a trade secret must be made on a case-by-case basis, and several limitations apply: neither information that can be readily obtained from another source nor information that is not the plaintiff's intellectual property qualifies as a trade secret. Pestco, Inc., 880 A.2d at 707; Den-Tal-Ez, Inc. v. Siemens Capital Corp., 566 A.2d 1214, 1228 (Pa. Super. Ct. 1989).

---

[10] The PTSA displaced Pennsylvania's common law tort for misappropriation of trade secrets, but there is no indication that the statute effected a substantive shift in the definition of "trade secret." The common-law definition, like the statutory one, provided for protection for a formula, pattern, device, or compilation of information and required that the information be kept secret and provide a competitive value to the owner. Pestco, Inc. v. Associated Products, Inc., 880 A.2d 700, 706 (Pa. Super. Ct. 2005). The conclusion that the PTSA did not substantially alter the definition of "trade secret" is supported by post-PTSA cases that rely on common law in determining whether certain information rises to the level of a trade secret. See, e.g., Parsons v. Pa. Higher Educ. Assistance Agency, 910 A.2d 177, 185-86 (Pa. Commw. Ct. 2006); Select Med. Corp. v. Hardaway, 2006 WL 859741 at *8 (E.D. Pa. 2006); Brubaker Kitchens, Inc. v. Brown, 2006 WL 1193223 at *1-2 (E.D. Pa. 2006).

These limitations disallow trade secret protection for the information taken by Fitzgerald. Client names and services performed were located in Fitzgerald's work papers, which under Pennsylvania law remain an accountant's property absent an agreement with the client. 63 P.S. § 9.11(a). Pricing information was also obtainable from Fitzgerald's own papers, as he issued the invoices for the work he performed. See Defs.' Br. in Supp. Ex. D at 88-89.[11]

The price charged was also available from the clients themselves. Several courts have recognized that prices charged are not protectible because they can be obtained by the customer. In SI Handling Systems, Inc. v. Heisley, 753 F.2d 1244, 1257, 1260 (3d Cir. 1985), the Court, interpreting Pennsylvania law, differentiated between pure pricing information, readily obtainable from other sources, and "a whole range of data relating to materials, labor, overhead, and profit margin," which was entitled to protection as a trade secret. See also Tyson Metal Products, Inc. v. McCann, 546 A.2d 119, 121-22 (Pa. Super. Ct. 1988)(holding that pricing information could be obtained from other sources and therefore trade secret protection was

[11] The plaintiff argues that Fitzgerald was able to poach BSA clients by using the price charged by BSA to formulate a lower bid. The plaintiff has not provided any evidence that Fitzgerald engaged in this practice even if it could establish that such actions constituted misappropriation of trade secrets.

unwarranted).

The Pennsylvania Superior Court, commenting on SI Systems, affirmed its distinction between prices -- "the numbers themselves" -- and a "whole gamut" of information that would enable a person to ascertain the plaintiff's pricing methods. Den-Tal-Ez, Inc., 566 A.2d at 1230. The price charged by Fitzgerald falls on the non-protectible side of this line. Compare A.M. Skier Agency, Inc. v. Gold, 747 A.2d 936 (Pa. Super. Ct. 2000)(trade secret protection appropriate for documents containing an analysis of each client's insurance needs and the plaintiff's methodology for determining what prices to charge).

The information on the client list is also not protectible as a trade secret because it did not contain proprietary information. Under Pennsylvania law, if client information is in the possession of the employer but then disclosed to the employee, trade secret protection may attach. Morgan's Home Equipment Corp. v. Martucci, 136 A.2d 838 (Pa. 1957)(trade secret protection for a list of clients provided to the employee by the employer). In contrast, if customer information is created by the employees themselves during the course of their employment, it is not property of the employer and thus cannot qualify as a trade secret. Fidelity Fund, Inc. v. Di Santo, 500 A.2d 431 (Pa. Super. Ct. 1985)(no trade secret protection for list of clients brought to firm by broker, or

developed by him during employment).

The plaintiff has not produced any evidence that the names of the clients serviced by Fitzgerald or the amount they were charged were its property. The plaintiff has failed to name a single client it provided to Fitzgerald. See Spring Steels, Inc. V. Molloy, 162 A.2d 370, 372 (Pa. 1960)(customer list not protected because not product of "special work" by the employer). The client information assembled by Fitzgerald was not BSA's "special work" but instead Fitzgerald's compilation of the clients he serviced while at BSA. See, e.g., United Aircraft Corp. v. Boreen, 284 F.Supp. 428, 446 (E.D. Pa. 1968) (telephone numbers on client list prepared by the defendant not property of the employer). In short, the plaintiff has failed to show that the client list was assembled through "great expense, time, and effort," and therefore it is not entitled to trade secret protection. A.M Skier Agency Inc., 747 A.2d at 940.

The plaintiff also alleges that Fitzgerald's use of the client list constituted misappropriation of confidential business information, a tort which allows a party to recover when a rival procures by improper means information about another's business. The information need not rise to the level of trade secret in order to qualify for protection, but it must be confidential. Rest. (First) of Torts § 759 cmt. b; Pestco, Inc., 880 A.2d at 709); Den-Tal-Ez, Inc., 566 A.2d at 1231.

This claim fails for the same reasons as the misappropriation of trade secrets claim. Because the information in the client list was not proprietary, it was not the plaintiff's "business information." Further, it was not "confidential" because it was available from other sources.[12]

D. Tortious Interference with BSA's Contractual Relationship with its Clients

The plaintiff alleges that Fesnak tortiously interfered with its contractual relationships with its clients. In order for this claim to succeed, the plaintiff must first show the existence of a contractual relationship. Hillis Adjustment Agency, Inc. v. Graham Co., 911 A.2d 1008, 1012 (Pa. Super. Ct. 2006). Because the plaintiff has failed to produce any evidence that its relationship with its clients was contractual, this claim fails. At his deposition, Senior testified that a firm could have an oral contract with a client, but did not name any BSA client with whom it had such an agreement. Pl.'s Br. in Opp. Ex. A at 266-67. The phonecalls made by Fitzgerald and Senior during Fitzgerald's final days at BSA-- Fitzgerald soliciting

[12] The failure of the misappropriation claims also defeats the plaintiff's unfair competition claim. A claim for unfair competition may be based on conduct that is otherwise actionable at common law. Restatement (Third) of Unfair Competition § 1(b). In this case, the plaintiff's unfair competition claim is dependant upon its misappropriation claims, and therefore they fall together. See Pl.'s Br. in Opp. at 52.

clients, Senior urging them to stay -- suggest that the clients were free to leave BSA at will, and BSA has not produced evidence to indicate otherwise.

E. Breach of Fiduciary Duty

Finally, the plaintiff claims that Fitzgerald breached his fiduciary duty by interfering with BSA's goodwill with its clients and diverting business opportunities to a competitor. Prior to the termination of an employment relationship, an agent may make arrangements to compete with a principal and may freely compete once the employment relationship is terminated. Before the employment relationship ends, however, an employee cannot solicit customers for a rival business. See Restatement (First) of Agency § 393 cmt. e; Oestreich v. Environmental Inks and Coatings Corp., 1990 WL 210599 at *6 (E.D. Pa. 1990); Colonell v. Goodman, 78 F.Supp. 845, 847 (E.D. Pa. 1948); Roman Sentry Sec. Sys., Inc. v. Mannino, 25 Phila. Co. Rptr. 178, 189-90 (Pa. Ct. Comm. Pls. 1993).

Under this rule, Fitzgerald did not breach his fiduciary duty in contacting clients after he left BSA. As stated above, however, Fitzgerald contacted twenty clients while he was still employed at BSA, fifteen of whom followed him to Fesnak. Fitzgerald conceded that at least some of these contacts were solicitations. The plaintiff has therefore produced

sufficient evidence for a jury to conclude that Fitzgerald breached his fiduciary duty in making these phonecalls.

The final issue is the plaintiff's conspiracy claim. A cause of action for civil conspiracy requires a separate underlying tort as a predicate for liability. In re Orthopedic Bone Screw Products Liability Litigation, 193 F.3d 781, 789-90 & n.7 (3d Cir. 1999). Consequently, the conspiracy claim survives only as it relates to the breach of fiduciary duty claim.

To prevail on a civil conspiracy claim, a plaintiff must adduce evidence that two or more parties agreed to undertake either an unlawful act or a lawful act by unlawful means. Scully v. US Wats, Inc., 238 F.3d 497, 516 (3d Cir. 2001). In this case, there is no evidence that Fesnak induced or encouraged Fitzgerald to breach his fiduciary duty to BSA. Although Fesnak might have desired Fitzgerald to bring his clients with him to the firm, a contention Fesnak denies, there is no evidence that Fesnak desired to accomplish this through unlawful means. Fesnak therefore cannot be held liable for any breach of fiduciary duty by Fitzgerald.

An appropriate order follows.

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

BRETT SENIOR & ASSOCIATES, P.C.,	:	
Plaintiff,	:	CIVIL ACTION
v.	:	
STEPHEN C. FITZGERALD, et al.,	:	
Defendants	:	NO. 06-1412

ORDER

AND NOW, this 13th day of July, 2007, upon consideration of the defendants' motion for summary judgment, the plaintiff's opposition, and the defendants' reply, and after oral argument on the motion held on April 12, 2007, IT IS HEREBY ORDERED that the motion is granted as to all claims except the breach of fiduciary duty claim against Fitzgerald as stated in the accompanying memorandum.

BY THE COURT:

/s/ Mary A. McLaughlin
MARY A. McLAUGHLIN, J.