IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

TEKSYSTEMS, INC.,	)	
	)	
Plaintiff,	)	
	)	Civil Action No.: 08 C 5476
v.	)	
	)	Suzanne B. Conlon, Judge
MODIS, INC., BRIAN PELLIGRINI, JASON LUKAS, and ROBERT J. RUF,	)	
	)	
Defendants.	)	

MEMORANDUM OPINION AND ORDER

TEKsystems, Inc. ("TEKsystems") sues its former employee Jason Lukas for breach of his employment agreement (Count II), misappropriation of trade secrets (Count IV), and violation of the Computer Fraud and Abuse Act ("CFAA"),[1] 18 U.S.C. § 1030(a)(2)(C) and (a)(4) (Count VI). TEKsystems alleges Lukas downloaded its trade secret and confidential client information onto an external hard drive after accepting a position with its competitor, Modis, Inc. ("Modis"), and provided the information to Modis. Lukas moves to dismiss the complaint for failure to state a claim. For the reasons set forth below, the motion is denied.

BACKGROUND

The following allegations are derived from TEKsystems' complaint. TEKsystems and Modis compete in the field of information technology and communications consulting services and staffing. Both companies provide temporary and permanent staffing services to clients in various industries. TEKsystems developed and maintains business methods and sales strategies

[1] The statute was amended effective September 26, 2008. The amendments are not applicable to this case.

systems. It relies on confidential client databases that include information such as staffing preferences, previous staffing bids, a company's internal organizational information, and unique business practices or technical requirements.

Lukas worked for TEKsystems as a technical recruiter in its Detroit, Michigan office and then an account manager in its Downers Grove, Illinois office from February 2002 to August 2007. TEKsystems requires every person in these positions, without exception, to sign an employment agreement containing noncompete, nonsolicitation, and nondisclosure provisions. Compl. ¶¶ 20, 36, 40 and Ex. A. The agreement also requires employees to return all TEKsystems records and information when ceasing employment. Compl. ¶ 40 and Ex. A. TEKsystems alleges, upon information and belief, that Lukas signed this employment agreement when he was hired, but that it cannot locate a copy. Compl. ¶ 37.

TEKsystems alleges that on or about July 29, 2007, after accepting a position at Modis, but before notifying TEKsystems, Lukas attached a hard drive to his TEKsystems laptop computer and, on information and belief, downloaded TEKsystems' confidential and trade secret customer information. Compl. ¶ 64. On August 3, 2007, Lukas announced his resignation and future employment with Modis in its Detroit office. Compl. ¶ 65.

At some point before the middle of November 2007, after Lukas started working for Modis, Modis' regional senior vice-president Jim Sweeney telephoned Tim Cebula, the managing director of Modis' Chicago office, and told him to expect a visit from Lukas. Compl. ¶ 66. Sweeney told Cebula that Lukas would bring Teksystems' information, and instructed Cebula to review the information with Lukas. Compl. ¶ 66. Defendant Brian Pelligrini, the managing director of Modis' Minneapolis, Minnesota office (and former TEKsystems manager),

also advised Cebula that Lukas would be visiting the Modis Chicago office and bringing TEKsystems' client information. Compl. ¶ 67.

In approximately November 2007, Lukas met with Cebula, and downloaded a file called "Chicago Data" to Cebula's computer. Compl. ¶ 68. The data included confidential TEKsystems client information, client job order history, and detailed client technology spending information. Compl. ¶ 69. The information was everything a salesperson would need to start calling upon a new account. Compl. ¶ 71. Information from the Chicago Data file was later added to Modis' intranet system for tracking clients and candidates. Compl. ¶ 73.

DISCUSSION

I. Legal Standard

A motion to dismiss may challenge the complaint for failure to state a claim upon which relief may be granted. Fed. R. Civ. P. 12(b)(6). In ruling on a Rule 12(b)(6) motion, all well-pleaded allegations are accepted as true and all reasonable inferences are drawn in plaintiff's favor. *Tamayo v. Blagojevich*, 526 F.3d 1074, 1081 (7th Cir. 2008). The complaint need only provide a short and plain statement giving defendants fair notice of the nature and basis of the claim. *Bell Atlantic Corp. v. Twombly*, 127 S. Ct. 1955, 1964 (2007); *Tamayo*, 526 F.3d at 1081; Fed. R. Civ. P. 8(a)(2). This requires more than labels and conclusions, or a formulaic recitation of the elements of a cause of action. *Bell Atlantic Corp.*, 127 S. Ct. at 1964-65. Factual allegations must be sufficient to state a claim to relief that is plausible on its face, rather than merely speculative. *Id.* at 1965, 1974; *Tamayo*, 526 F.3d at 1083.

II. Sufficiency of Complaint

Lukas argues TEKsystems' complaint against him should be dismissed because it improperly pleads the factual predicate for all counts – that Lukas downloaded its client information and provided it to Modis – on information and belief. Compl. ¶ 64. Lukas argues allegations based exclusively on information and belief are improper unless the facts are inaccessible to the pleader, and there is a reasonable basis to suspect the facts are true. *See Bankers Trust Co. v. Old Republic Ins. Co.*, 959 F.2d 677, 684 (7th Cir. 1992). According to Lukas, TEKsystems has the relevant information within its control, *i.e.*, the alleged download was from its own computer, and TEKsystems fails to plead the grounds for its suspicions.

Lukas mischaracterizes TEKsystems' complaint. TEKsystems alleges Lukas attached an external hard drive to his TEKsystems computer after accepting a job with Modis and downloaded TEKsystems' confidential customer information. Compl. ¶ 64. A few months later, Modis management apprised its Chicago office that Lukas would be arriving with TEKsystems' customer information. Compl. ¶¶ 66-67. Lukas visited the Modis Chicago office and downloaded a TEKsystems' customer information file to Modis' managing director's computer, which made its way to Modis' internal client and candidate tracking system. Compl. ¶¶68-69, 73.

The only allegation pled on information and belief was that Lukas downloaded the customer information. Compl. ¶ 64. TEKsystems argues it pleads this on information and belief because Lukas surreptitiously downloaded the information; there were no eyewitnesses. A reasonable inference may be drawn that Lukas, as an account manager, had opportunity to access and remove confidential information, particularly from his own laptop computer, without others

being aware of his activities. *See Assurance Alliance, Inc. v. Gardner*, No. 93 C 2263, 1993 WL 243355, at *2 (N.D. Ill. June 30, 1993) (Kocoras, J.) (an information and belief allegation that company president removed confidential files stated a claim). TEKsystems sufficiently pleads a reasonable basis for its breach of employment agreement (Count II), misappropriation of trade secrets (Count IV), and violation of CFAA (Count VI) counts against Lukas.

III. Breach of Employment Agreement

Lukas argues TEKsystems fails to state a breach of employment agreement claim (Count II) because it alleges the existence of Lukas' employment agreement on information and belief. Lukas argues this is improper because the existence of his purported employment agreement is information within TEKsystems' own knowledge, citing *Oil Express Nat'l, Inc. v. Burgstone*, No. 96 C 4816, 1996 WL 666698 (N.D. Ill. Nov. 14, 1996) (Kocoras, J.), and *HWB, Inc. v. Braner, Inc.*, No. 92 C 5900, 1993 WL 389346 (N.D. Ill. Sept. 30, 1993) (Nordberg, J.). Both cases involved tortious interference with contractual relations claims. The heightened pleading standard for fraud was applied, requiring that a claim made upon information and belief also contain allegations of the facts upon which the information and belief rests. *Oil Express Nat'l*, 1996 WL 666698, at *6-7; *HWB*, 1993 WL 389346, at *2. In *Oil Express Nat'l*, Oil Express sued its franchisee, alleging, on information and belief that the franchisee induced other franchisees to breach their Oil Express contracts. 1996 WL 666698, at * 6-7. Pleading this allegation on information and belief was held improper because whether a franchisee breached an Oil Express contract was a matter within the personal knowledge of Oil Express. *Id.* at 8.

In *HWB*, HWB produced turret head slitters (steel coil processing equipment), and held multiple patents in the field. 1993 WL 389346, at *1. HWN entered into a exclusive licensing

agreement with Repco Metal Center Machine, Inc., subject only to similar agreements with Terico Engineering and Durmech Engineering for their use of the patents in Asia and Europe. *Id.* HWB alleged Repco marketed the turret head slitters in Japan, which induced Terico to breach its licensing agreement. HWB pled the breach of agreement upon information and belief. *Id.* This was held improper because HWB would have known better than anyone whether Terico breached its agreement. *Id.* at 2.

TEKsystems does not allege tortious interference with contractual relations against Lukas, and the rationale of these cases does not apply here. TEKsystems identifies the basis for its belief that Lukas executed an employment agreement. TEKsystems alleges every technical recruiter and account manager like Lukas is required to sign an employment agreement – no exceptions. Compl. ¶ 36. TEKsystems describes the standard agreement's terms, including its noncompete, nonsolicitation, and nondisclosure provisions, and attaches a copy executed by defendant Pelligrini as an exhibit to the complaint. Compl. ¶¶ 26-31 and Ex. A. TEKsystems alleges, upon information and belief, that Lukas signed this employment agreement when he was hired, but that TEKsystems cannot locate a copy. Compl. ¶ 37. These allegations do not amount to a mere hunch as Lukas contends. A reasonable inference may be drawn that Lukas executed TEKsystems' employment agreement.

Moreover, a plaintiff is not required to attach the contract to a breach of contract complaint. *See Murphy v. White Hen Pantry Co.*, 691 F.2d 350, 352-53 (7th Cir. 1982) (complaint must reference agreement between the parties to allege breach of contract claim); *U.S. Data Corp. v. Realsource, Inc.*, No. 08 C 1092, 2008 WL 4369766, at *6 (N.D. Ill. Sept. 22, 2008) (Manning, J.) (allegation of existence and content of contract sufficient to state a claim).

Thus, in *Parks v. Female Health Care Ass'n, Inc.*, No. 96 C 7133, 1997 WL 285870, at *5 (N.D. Ill. May 23, 1997) (Anderson, J.) (unsigned agreement attached to a complaint was sufficient to withstand a motion to dismiss). Dismissal would be premature because the plaintiff would not have the benefit of obtaining the fully executed copy of the contract through discovery. *Id.*

TEKsystems alleges Lukas executed the employment agreement it requires every employee in Lukas' position to sign. TEKsystems describes the agreement, and attaches the standard agreement as an exhibit to its complaint. Dismissal of the breach of employment agreement claim (Count II) is unwarranted.

IV. CFAA Violation

A. Improper Access

Lukas argues TEKsystems fails to state a CFAA claim (Count VI) because it has not alleged improper access to a protected computer. Lukas states he was still working for TEKsystems, and authorized to view the customer information at the time of his alleged wrongdoing. According to Lukas, he could not have violated the CFAA, §§ 1030(a)(2)(C) and (a)(4), requiring lack of computer authorization. Specifically, § 1030(a)(2)(C) provides that a person violates the CFAA by intentionally accessing a computer *without authorization*, or exceeding his authorized access, and thereby obtaining information from a protected computer. 18 U.S.C. §1030(a)(2)(C). A violation of § 1030(a)(4) occurs when a person knowingly and with the 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 something of value. 18 U.S.C. §1030(a)(4). Lukas' theory is that he had authorization to access the information on his company computer.

Lukas relies upon district court cases from other jurisdictions. *See, e.g.*, *Black & Decker, Inc. v. Smith*, 568 F. Supp. 2d 929 (W.D. Tenn. 2008); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962 (D. Ariz. 2008); *Diamond Power Intern, Inc. v. Davidson*, 540 F. Supp. 2d 1322 (N.D. Ga. 2007). These cases stand for the proposition that the CFAA was not intended to apply to employees who misappropriate confidential information from computers for which they had authorized access at the time. These cases are not binding, and conflict with Seventh Circuit precedent. *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006).

In *Citrin*, the employer alleged its former employee permanently deleted, through an erasure software program, incriminating and company information from his company computer after he decided to quit and go into business for himself. Dismissal of the claim was reversed. *Id.* at 421. As alleged, the employee in *Citrin* violated § 1030(a)(5)(A)(ii) of the CFAA , another provision of CFAA containing the "without authorization" language. Section 1030(a)(5)(A)(ii) provides that a person violates the statute by intentionally accessing a protected computer *without authorization*, and thereby recklessly causes damage. 18 U.S.C. § 1030(a)(5)(A)(ii). When he destroyed the company files, the employee breached his duty of loyalty, and consequently terminated his agency relationship. Unless otherwise agreed, an agent's authority terminates if, without knowledge of the principal, he acquires adverse interests or seriously breaches the duty of loyalty. *Id.* at 421 (citing RESTATEMENT (SECOND) OF AGENCY § 112). The agency relationship was the basis for authority to access the company computer. *Id.* at 420-21.

TEKsystems alleges Lukas downloaded its confidential information after accepting a position with its competitor Modis, but before notifying TEKsystems. Compl. ¶¶ 64-65. His agency relationship with TEKsystems terminated at this point, and he no longer was authorized

to access the information under the CFAA. Under *Citrin*, Count VI sufficiently alleges Lukas accessed TEKsystems' computer without authorization.

B. Damage

Lukas argues TEKsystems fails to state a CFAA claim (Count VI) because TEKsystems alleges mere loss from Lukas' alleged conduct, not loss *and* damage as required by the statute. The CFAA defines damage as any impairment to the integrity or availability of data, a program, a system, or information. 18 U.S.C. § 1030(e)(8). Loss is defined as any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, restoring the system or information to its prior condition, and lost revenue, cost incurred, or other consequential damages incurred because of service interruption. 18 U.S.C. § 1030(e)(11).

Section 1030(g) unambiguously provides that a civil action may be maintained for damage *or* loss. 18 U.S.C. § 1030(g). *See Charles Schwab & Co., Inc. v. Carter*, No. 04 C 7071, 2005 WL 351929, at *3 (N.D. Ill. Feb. 11, 2005) (St. Eve, J.) (holding the CFAA provides a civil cause of action). Damage is expressly required in specific subsections of the CFAA. *See, e.g.*, 18 U.S.C. § 1030(a)(5)(A)(I) (prohibiting knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causing *damage* without authorization to a protected computer). The word is not included in §§ 1030(a)(2)(C) or (a)(4) – the provisions Lukas is alleged to have violated. If the language of a statute is plain and unambiguous, then the inquiry ends there, and it must be applied to the facts of the case. *See United States v. Jones*, 372 F.3d 910, 913 n.2 (7th Cir. 2004). Under the plain language of CFAA, a damage pleading is not required to state claims under §§ 1030(a)(2)(C) or (a)(4). TEKsystems pleads that Lukas' purported violation of the CFAA caused it loss exceeding $5,000

for the cost of a computer forensic investigation into Lukas' conduct. Compl. ¶ 149. TEKsystems sufficiently alleges loss, and is not required to plead damage to state its CFAA claim (Count VI).

C. Heightened Pleading Standard

Lukas asserts TEKsystems § 1030(a)(4) claim (Count VI) must be pled with particularity under Rule 9(b)'s heightened pleading standard for fraud because this statutory provision requires an intent to defraud. This argument ignores Rule 9(b)'s provision that malice, intent, knowledge, and other conditions of a person's mind may be alleged generally. Fed. R. Civ. P. 9(b). TEKsystems is not required to meet a heightened pleading standard to state a §1030(a)(4) claim. *See C.H. Robinson Worldwide, Inc. v. Command Transportation, LLC*, No. 05 C 3401, 2005 WL 3077998, at *4 (N.D. Ill. Nov. 16, 2005) (St. Eve, J.) (rejecting identical argument). Count VI stands.

CONCLUSION

Lukas' motion to dismiss the complaint is denied. TEKsystems sufficiently pleads that Lukas downloaded its client information and provided it to Modis (Counts II, IV, and VI). TEKsystems sufficiently pleads the existence of Lukas' employment agreement (Count II). TEKsystems states a CFAA claim (Count VI) because Lukas' access to TEKsystems' computer after he allegedly accepted employment with Modis and decided to download TEKsystems' confidential client information was unauthorized. TEKsystems is not required to plead damage to state its §§ 1030(a)(2)(C) and (a)(4) claim (Count VI). TEKsystems need not meet a heightened pleading standard to state a §1030(a)(4) claim (Count VI).

ENTER:

Suzanne B. Conlon

Suzanne B. Conlon
United States District Judge

December 5, 2008