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

HUB GROUP, INC.,	**:**	**CIVIL ACTION**
Plaintiff	**:**	
	:	
v.	**:**	**NO. 05-2046**
	:	
JEFFREY M. CLANCY,	**:**	
Defendant	**:**	

M E M O R A N D U M

STENGEL, J. **January 25th, 2006**

Plaintiff, HUB Group, Inc. ("HUB") seeks a preliminary injunction temporarily barring defendant, Jeffrey Clancy, from contacting, soliciting, or servicing any of the 29 customers he serviced during his final year of employment with HUB. HUB contends that Clancy stole secret information regarding those current and former HUB clients, and that he should not be allowed the opportunity to use that information to unfairly compete against HUB. HUB's complaint alleges violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, et. seq., Misappropriation of Trade Secrets, Breach of Contract, Breach of Fiduciary Duty, Conversion, Tortious Interference with an Economic Advantage, and Unfair Competition. This court entered a temporary restraining order on May 4, 2005 directing the defendant to cease using or disclosing any confidential or proprietary information that Mr. Clancy obtained from HUB. On August 23, 2005, a hearing was held so the court could consider evidence as to whether its temporary restraining order should remain in place. Based upon my findings of fact after careful consideration of the

evidence from the hearing, and based upon the legal conclusions and discussion which follow, I will dissolve the temporary injunction entered on May 4, 2005.

I. FINDINGS of FACT

1) HUB is a Delaware corporation with its principal place of business in Downers Grove, Illinois. HUB is a transportation management service company that provides intermodal, truckload, LTL International and logistics services to its customers. Specifically, HUB arranges for the transportation of goods in trailers and/or containers on behalf of third parties from their point of origin to their final destination.

2) Defendant, Jeffrey Clancy ("Clancy") is a Pennsylvania resident. Clancy worked for HUB between June of 1999 and March 15, 2005. He worked out of his home as a Regional Sales and Account Manager using a HUB-issued computer.

3) Clancy worked for HUB as an at-will employee. There was no employment contract between Clancy and HUB.

4) While working for HUB, Clancy had access to HUB's electronic database containing detailed customer information. The database contained information including the prices HUB charges and HUB's profit margins.

5) HUB compiled the electronic database and considers it a trade secret.

6) The database is password protected.

7) Some of the information contained within the database was compiled and entered by Clancy.

8) With the information contained in HUB's database, one may make a detailed pricing proposal to a prospective client without ever having met the client.

9) During his employment with HUB, Clancy was presented with a "confidentiality agreement" as part of a Code of Business Conduct and Ethics Guide. He was also presented with a "confidentiality agreement" prepared by HUB as part of an Employment Guide. He signed each "agreement." The "agreements" related to the confidentiality of HUB's database. These confidentiality agreements did not constitute an employment agreement. By signing these "agreements," Clancy indicated his understanding of the policy statements contained in each and confirmed that he received the statements. These statements were drafted by HUB, and HUB made the unilateral decision to require Mr. Clancy to sign them. The policy statements, or "agreements," were not bargained-for conditions of Clancy's employment with HUB.

10) Clancy did not sign a covenant or agreement not to compete with HUB.

11) Following Clancy's resignation from HUB on March 15, 2005, he began working for one of HUB's direct competitors, Trailer Transport Systems, Inc. ("TTS").

12) TTS issued Clancy a computer.

13) Immediately after Clancy's resignation, HUB revoked his password and prohibited his access to their electronic database.

14) Clancy returned the HUB-issued computer on April 1, 2005.

15) After Clancy's resignation, HUB investigated Clancy's recently sent emails to see if he had informed a client about HUB's rate increases. While searching those emails, HUB discovered that Clancy sent emails with attachments to his wife's Hotmail account.[1]

16) The attachments sent by Clancy to his wife's Hotmail account contained detailed pricing and customer information that HUB considers confidential.

17) The attachments also contained information compiled by HUB for its sales reports.

18) Pricing within HUB's industry is competitive. HUB's prices are set by its Pricing Department and are dependant upon many variables. Due to the unstable nature of dependent variables, i.e. gas prices and other costs, HUB's prices fluctuate regularly.

19) Although Clancy, as a Sales and Account Manager, had some input and worked with the Pricing Department, he did not set HUB's final prices.

20) Clancy has extensive experience within the transport industry. He has a good working knowledge and understanding of the specific price ranges charged by HUB and other companies in the industry.

21) HUB's prices are readily available from its current and former customers.

[1] A Hotmail account is a free web-based email service. Once an account is opened, it may be accessed by the account-holder from any computer linked to the internet.

22) HUB regularly prepares sales reports for its account managers based upon the manager's volumes, revenues, and profit margins on individual accounts. Clancy received these reports.

23) Clancy emailed the confidential information with the intention of advancing his ability to do his job as an employee of TTS.

24) There is no evidence that Clancy has used the information to compete with HUB.

25) There is uncontroverted evidence that Clancy did not actually use the information he emailed from his HUB computer to his wife's email account.

26) Clancy first interviewed with TTS in February of 2005. During that interview process, Clancy had expectations about the amount of business he could transfer over from HUB to TTS.

27) Before leaving HUB, Clancy received a solicitation from Carlisle Tire & Wheel Co., a customer of HUB's, requesting a price quote for a specific shipping lane. Clancy waited on the request, did not inform any of his HUB supervisors, and then while working for TTS gave Carlisle Tire a TTS price quote. Carlisle Tire conducted the business with TTS.

28) A computer forensic expert hired by HUB, Robert O'Leary, testified that "an attachment" had been sent from Clancy's TTS computer to his wife's Hotmail account, but could not testify as to the contents of this attachment.

29) According to Robert O'Leary, "something" was attached to the USB storage port on Clancy's TTS computer on March 26, 2005. HUB infers that a thumbnail memory storage drive was attached to the USB port, but that evidence was inconclusive.

30) Clancy testified that he never used the data he sent from his HUB computer to his wife's Hotmail account. This testimony was credible and was not controverted by any other testimony.

31) On May 4, 2005, this Court entered a temporary restraining order preventing Clancy from using the information he emailed to his wife's Hotmail account to unfairly compete against HUB.

II. DISCUSSION

A. Subject Matter Jurisdiction

In order for this Court to have proper subject matter jurisdiction to hear this case, a federal claim must be alleged pursuant to 28 U.S.C. § 1331, or diversity jurisdiction must be invoked in accordance with 28 U.S.C. § 1332. HUB alleges to have both types of federal subject matter jurisdiction.

1. Plaintiff's Claim Under the Computer Fraud and Abuse Act

According to Clancy, HUB fails to allege a proper claim under the Computer Fraud and Abuse Act ("CFAA") because it does not meet the CFAA's damage requirements. The pertinent section of the CFAA, 18 U.S.C. § 1030 provides:

Fraud and related activity in connection with computers:

(a) Whoever--

(4) 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, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $ 5,000 in any 1-year period;

(5) (A) (i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused-- (i) 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;

(e) (8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

18 U.S.C. § 1030.

HUB argues that the integrity of its computer database was damaged through Clancy's unauthorized access to confidential information. In support of this contention, HUB cites Shurgard Storage Ctrs, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1126-27 (W.D. Wash. 2000) (CFAA applied in plaintiff employer's suit against defendant for actively soliciting plaintiff's former employees and requesting that they transmit confidential files to defendant); Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1196-97 (E.D. Wash. 2003) (CFAA case in which the court looked to the history of the Act and concluded that it could be applied to prevent a former employee from using wrongfully acquired trade secret information in order to compete with former employer); EF Cultural Travel BV, EF v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001) (former employee's use of a "scraper program" to copy otherwise public information on the former employer's website likely exceeded the authorized access in violation of the CFAA); George S. May Int'l Co. v. Hostetler, No. 04-C-1606, 2004 U.S. Dist. Lexis 9740 (N.D. Il. 2004) (Kocoras, J.) (CFAA claim was properly stated where a former consultant accessed copyrighted materials while still an employee of the consulting firm to be used for his personal benefit); I.M.S Inquiry Mgmt. Sys, Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 525 (S.D.N.Y. 2004) (Cause of action under the CFAA was adequately plead where plaintiff alleged the integrity of their copyrighted data system was impaired by defendant's copying it); and Book Wholesalers, Inc. v. Rooth, No. 04 CV 2428 DMS

(Southern District of California court found a CFAA cause of action after a former employee downloaded the former employer's database onto her personal computer).

Based upon the cases cited above, and the Third Circuit's recent opinion in P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC, Civ. No. 04-4254, (November 7, 2005) HUB has adequately invoked this Court's federal question subject matter jurisdiction. Clancy admitted that he took the information to use as a TTS employee. For purposes of federal question jurisdiction, Clancy exceeded the scope of his authorization into the database, thereby giving HUB the ability to plead a cause of action under the CFAA. Further, under the cases cited above, the damages alleged by HUB are of the type covered under the Act.

2. Diversity Jurisdiction

In the alternative, and assuming that this is not a federal question case, the two parties are diverse. It appears this claim is in excess of $75,000 as well.

The value of injunctive actions, for diversity purposes, is measured by the right sought to be protected. In re Corestates Trust, 39 F.3d 61, 65 (3d Cir. 1994). In this case, HUB has alleged that the value of keeping its database secret exceeds $75,000. No evidence has been presented by Clancy to contest that claim, nor is there any reason to believe it was made in bad faith. As a result, the court has diversity jurisdiction over this case.

III. PRELIMINARY INJUNCTION

A. Standard of Review

In order to obtain a preliminary injunction, HUB must establish that it suffered irreparable harm by Mr. Clancy's actions. HUB must also prove a reasonable probability of success on the merits, that the harm to HUB outweighs the possible harm to other interested parties, and that the injunction is in the public interest. See Continental Group, Inc. v. Amoco Chem. Corp., 614 F.2d 351, 356-57 (3d Cir. 1980); Frank Russell Co. v. Wellington Mgmt. Co., 154 F.3d 97, 101 (3d Cir. 1998).

B. Discussion

1. Has HUB Shown Irreparable Harm?

Clancy argues that HUB has failed to show irreparable harm by not showing actual damages to the HUB database or actual losses due to Clancy's actions. HUB has, however, shown that it will suffer serious financial injury if the information protected within its database is made known to its competitors. HUB's showing is not enough to grant a preliminary injunction on these facts. See Campbell Soup Co. v. ConAgra, Inc., 977 F.2d 86 (3d Cir. 1992) (reversing a district court's preliminary injunction based upon a lack of evidence of irreparable injury). In particular, the court in Campbell found that "in order to demonstrate irreparable harm the plaintiff must demonstrate potential harm which cannot be redressed by a legal or an equitable remedy following a trial. The

preliminary injunction must be the only way of protecting the plaintiff from harm." Id. at 91.

Although HUB has not demonstrated any actual damages caused by Clancy's unauthorized access and copying of parts of its database, the threat of harm is present. Clancy currently works for one of HUB's direct competitors and the information contained within the email attachments sent by Clancy to his wife's computer could cause injury to HUB. That injury, however, would not be "irreparable harm" as any profits made on a transaction by TTS using HUB's information could be recovered in a claim for damages. This is not a situation where Clancy has continuing access to the HUB database. The threat to HUB is that Clancy will use the information emailed to his wife's Hotmail account to compete improperly with HUB. There are adequate remedies at law available to HUB as a means of redressing that threat.

2. Has HUB shown that it will likely succeed on the merits of its case?

The evidence presented at the preliminary injunction hearing does not establish likelihood of success on the merits of this case. The evidence indicates that the pricing data taken by Clancy is already obsolete due to fluctuating fuel prices and other general rate changes. In fact, the pricing information had a very short life. Given the dramatic increase in fuel prices alone since the hearing, the information Clancy allegedly took with him to TTS is likely useless. Further, the information regarding contacts with former clients is the type of knowledge Clancy acquired through his years of experience, or could

have easily obtained through a few well-placed phone calls. Contact information is readily available to someone with Mr. Clancy's experience with a minimum of research.

3. Does the harm to Clancy outweigh the harm to HUB?

Enjoining Clancy from conducting any business with thirty separate entities, some of which he serviced prior to working at HUB, is a drastic and unwarranted measure in this case. The evidence presented relating to HUB's losses that could be saved or mitigated through this injunction was slight, whereas the proposed injunction places a severe restriction on Clancy's ability to work.

4. The Public Interest

HUB argues that adopting a "no harm, no foul" attitude towards Clancy's actions would legitimize the type of theft alleged in this case and undermine business confidentiality agreements generally. This is not a situation where the court ignores improper conduct because of a lack of proof of harm. Rather, the court has evaluated the plaintiff's evidence and found it inadequate to sustain an injunction.

IV. CONCLUSION

Based upon an inability to show irreparable harm in accordance with Campbell, or a likelihood of success on the merits, and after weighing the potential harm to each side by the granting of an injunction, I deny HUB's request for a preliminary injunction. An appropriate Order follows.

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

HUB GROUP, INC.,	**:**	**CIVIL ACTION**
Plaintiff	**:**	
	:	
v.	**:**	**NO. 05-2046**
	:	
JEFFREY M. CLANCY,	**:**	
Defendant	**:**	

ORDER

STENGEL, J.

AND NOW, this 25th day of January, 2006, upon consideration of plaintiff's motion for a temporary injunction (Docket # 2), it is hereby ORDERED that the motion is DENIED. The temporary injunction entered on May 4, 2005, (Docket # 13) is DISSOLVED. A telephone status conference will be held with counsel on February 10th, 2006 at 9:30 a.m. Plaintiff's attorney shall initiate the call.

BY THE COURT:

_____/s/_____
LAWRENCE F. STENGEL, J.