

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

MINTEL INTERNATIONAL GROUP,	)	
LTD., a United Kingdom corporation,	)	
	)	
Plaintiff,	)	
	)	Case No. 08-cv-3939
v.	)	
	)	Judge Robert M. Dow, Jr.
MEESHAM NEERGHEEN, an individual,	)	
	)	Magistrate Judge Maria Valdez
Defendant.	)	

**MEMORANDUM OPINION AND ORDER**

On July 11, 2008, Plaintiff Intel International Group, Ltd. (“Intel”) filed a seven-count complaint against Defendant Meesham Neergheen (“Neergheen”), alleging that Neergheen (i) violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et seq.*, (ii) violated non-disclosure, non-compete, and non-solicitation provisions found in his employment contracts with Intel, and (iii) misappropriated Intel trade secrets pursuant to the Illinois Trade Secret Act (“ITSA”), 765 ILCS 1065/1, *et seq.*<sup>1</sup> Intel seeks injunctive relief, restitution, and compensatory and punitive damages. Intel also has moved for sanctions, up to and including entry of default judgment, on the basis of Neergheen’s alleged spoliation of evidence.<sup>2</sup>

---

<sup>1</sup> On January 23, 2009, Plaintiff filed a motion for leave to amend its complaint [207] to add an additional count (Count VIII) for negligence/spoliation of evidence. Because Plaintiff sought “leave to amend a pleading after the passage of the deadline in the trial court’s scheduling order” for amending pleadings, Federal Rule of Civil Procedure 16(b) applied. “To amend a pleading after the expiration of the trial court’s Scheduling Order deadline to amend pleadings, the moving party must show ‘good cause.’” *Trustmark Ins. Co. v. General & Cologne Life Re of America*, 424 F.3d 542, 553 (7th Cir. 2005). Applying the Rule 16(b) standard, the Court could not find “good cause” for the tardiness in Plaintiff’s assertion of a spoliation claim and denied Plaintiff’s motion for leave to amend its complaint.

<sup>2</sup> On January 22, 2009, Magistrate Judge Valdez issued an opinion [205], in which she denied Plaintiff’s motion for sanctions. Plaintiff filed objections [214] to Magistrate Judge Valdez’s opinion. In its April 17, 2009 opinion [243], this Court explained that it would treat Magistrate Judge Valdez’s January 22 order as a report and recommendation subject to *de novo* review and that it would take additional evidence on the spoliation issue. On April 30 and May 1, 2009, the Court heard extensive testimony from

Neergheen filed three counterclaims, but subsequently withdrew one. [See 212.] The remaining two counterclaims seek a declaratory judgment that the restrictive covenants found in his employment contracts are invalid as a matter of law.

On January 26 and 27, April 30, and May 1, 2009, the Court conducted a bench trial and heard testimony in two phases; the first phase focused on fact witnesses, the second on experts. Subsequently, the parties submitted proposed findings of fact and conclusions of law. Having considered the evidence presented at trial as well as the relevant legal standards, the Court finds that Neergheen breached his employment contract with Mintel, but that he did not violate the Computer Fraud and Abuse Act or the Illinois Trade Secrets Act. The Court also concludes that Mintel is not entitled to any award of sanctions on the basis of its allegations that Neergheen engaged in spoliation of evidence. Finally, as to Neergheen's counterclaims, the Court finds that the restrictive covenants, while overly broad in some respects, are not entirely invalid as a matter of law.

### **I. Findings of Fact<sup>3</sup>**

Mintel, headquartered in London, England, provides consumer, product, and market research to its clients around the world. Neergheen worked for Mintel's marketing department from June 30, 1997 until April 30, 2008. His career at Mintel started with a voluntary internship. Approximately three months after Neergheen started, Mintel hired him full-time as Assistant Editor of Global New Products Database in the London office.

---

experts for both parties relating to Plaintiff's charges that Defendant engaged in spoliation of evidence purportedly contained on a laptop computer and several USB devices.

<sup>3</sup> To the extent any finding of fact might be deemed a conclusion of law, it should be considered as a conclusion of law. See *Mitchell v. U.S.*, 2005 WL 2850113, at \*1 (N.D. Ill. Oct. 26, 2005). The same is true as to any stated conclusion of law. See *id.*

As a condition of Neergheen's employment with Intel, on June 24, 1998, he signed and executed a contract of employment. The contract included the following restrictive covenant:

You will not for the first twelve months at the end of your employment with us, either on your own account or on behalf of any other legal person and in competition with the Company, or any subsidiary directly or indirectly engage in, or be connected with, trade or business carried on by us or any of our associates at the end of your employment \* \* \* \* You will not, for the first twelve months after the end of your employment with us, solicit away from us or our associates any person who is and was, when your employment ended, employed by us or an associate as a director, senior manager or sales person for whom you were responsible, or who was a member of any department/project/team in which you worked during the last twelve months of your employment.

The contract also included a confidentiality clause:

In the course of your employment you will have access to certain of Intel's trade secrets and other proprietary or confidential information of Intel, including without limitation, procedures, processes, information related to design, production, marketing or distribution, data, databases, computer software, source codes, all methods and means of design, drawing, recording, reproducing information or storing information (including but not limited to electronic or computerized methods or means), supply sources or potential supply sources, customer lists or potential customer lists, bidding policies or procedures or any information concerning pricing or financing policies or procedures \* \* \* \* You agree that all such records, methods, lists, materials, names and information, as well as any information and documents provided to, generated by or received by you in the course of your employment and the contents thereof, is confidential and is and will remain the sole property of Intel. Such confidential information will not be used or disclosed by you other than in connection with your performance of services for Intel or such confidential information shall be returned to Intel upon the cessation of your employment.

In 2003, Intel transferred Neergheen to its Chicago office. On August 4, 2003, Neergheen signed a non-compete agreement which stated:

The undersigned Employee hereby agrees not to compete, either directly or indirectly, with the business of Intel or any of its subsidiaries, branches or divisions, at any location worldwide at any time during the Employee's term of employment, and for a period of one (1) year following his termination of employment with Intel, regardless of the reason or cause for such termination.

The non-compete agreement contained the following confidentiality clause:

The undersigned Employee acknowledges that Mintel may, in reliance upon the terms of this Agreement, supply or provide the undersigned Employee with access to Mintel's trade secrets, customer lists or other information of a confidential or proprietary nature. In consideration for his employment with Mintel, the undersigned Employee agrees to keep confidential all such information, and not to use such information for his own benefit or to disclose same to any third party.

The non-compete agreement also included a paragraph preventing the solicitation of Mintel employees and customers:

In further consideration of the undersigned Employee's employment with Mintel, the undersigned Employee further agrees \* \* \* he will not solicit or recruit any of Mintel's employees to undertake alternative employment, including any competitive employment, for a period of one (1) year after the undersigned Employee's termination date with Mintel without the express written consent of Mintel's CEO or U.S. General Manager. The undersigned Employee further agrees that in the event of his termination of employment with Mintel, regardless of the reason or cause for such termination, he will not solicit any of Mintel's customers for a period of one (1) year after the undersigned Employee's termination date with Mintel.

In October 2007, Mintel decided to restructure the marketing department in its Chicago office. As a result, Mintel informed Neergheen that his position as Marketing Operations Manager would be eliminated at the end of January 2008. On November 8, 2007, Neergheen interviewed for a new position within the department. However, Sabine Popp, the new head of Mintel's marketing department, did not offer Neergheen the new role because she felt that "[h]e didn't have the project management skills, the marketing experience, the strategic marketing skills that were required for [the new] role." She also informed Neergheen that he had "two realistic options": (1) to "possibly find an alternative role within Mintel;" or (2) "to discuss and finalize an exit strategy."

In a December 4, 2007 e-mail between Mintel executives Steve Charlton and Peter Haigh, Charlton wrote, "I'm going to do it gently and give him a few weeks severance but right now there don't seem to be any other options." On December 7, 2007, Charlton informed Neergheen that his role would be made redundant by the end of January 2008. On December 20,

2007, Neergheen was notified that there was a role available on the services team; however, because the role was distinct from the marketing arena and provided a smaller annual salary than Neergheen's former position, he declined. On January 16, 2008, Neergheen was offered a temporary role. In a letter dated that same day from Charlton to Neergheen, Charlton wrote:

This letter will discuss upcoming changes with regard to your employment relationship with Mintel International. We have had many prior conversations about the pending changes in the Marketing Department and the fact that Mintel has made the business decision to eliminate your position with the company. Although an alternative services role was discussed on the same package, you decided it was too junior and would consider it a demotion. Therefore, we hope you will accept a Temporary role as a PR Executive, reporting to Sabine Popp. It is important to note that this position will end effective April 20, 2008.

Neergheen accepted the temporary role in the public relations department on January 17, 2008.

From January through April 2008, Mintel was aware that Neergheen was interviewing with other companies. On January 11, 2008, Neergheen sent his resume to an acquaintance who worked at Datamonitor, a competitor of Mintel. Neergheen stated that he preferred "to remain in marketing as a marketing manager, with a strong focus on relationship building with clients, trade show management, campaign management and analysis, leveraging all contacts that I have with the current trade associations to secure free booth presence, speaker opportunities, complimentary sponsorships/advertising." Neergheen began interviewing with Datamonitor in February 2008, and in March 2008, Datamonitor offered Neergheen the position of Partnerships and Alliances Manager within the Distributors Business Unit. Neergheen accepted within a few days and began his employment at Datamonitor on May 27, 2008.

Initially, Datamonitor planned to utilize Neergheen in the area of consumer product goods. On February 15, 2008, Jeff Howard of Datamonitor commented to three other Datamonitor employees as follows: "I think this guy would be good for Distributors but, as importantly, excellent for [consumer goods]. I would expect him to go after existing Mintel partnerships

initially.” However, upon learning that Neergheen was subject to a non-compete clause, Datamonitor executives decided that Neergheen’s role would be “a commercial partnership role where he would target trade publications, associations and event organizers across all vertical markets with the exception of Consumer/Retail.” According to Datamonitor witnesses, Neergheen was prohibited from working in the consumer product group area; rather, he was to focus his efforts in two core areas, Pharmaceuticals and Technology.

On April 23, 2008, Neergheen informed Mintel that he would be “leaving the employment of Mintel at the conclusion of [his] temporary contract, effective Wednesday, April 30, 2008.” Concerned that the restrictive covenants in Neergheen’s employment contracts might not withstand scrutiny, Charlton sent an e-mail to Popp on April 28 acknowledging that “severance may be a good idea after all,” and suggesting that Neergheen should be “remind[ed] about the non-compete, however weak it is.” Popp suggested offering Neergheen severance but requiring that he sign a new non-compete. Neergheen was offered \$2,000 in exchange for signing a new non-compete agreement, but he declined. He did not receive any severance pay.

In 2007, Mintel provided Neergheen with a laptop, which he used, along with electronic storage devices, for his work at Mintel. Mintel’s human resources department schedules an exit interview with terminated employees on their last day and arranges for the return of company property, including security fobs, office keys, company manuals and other proprietary information, and any additional company-owned or issued property. During his exit interview, Neergheen was not asked to return his laptop or his electronic storage devices, and he continued to use the laptop that he had received from Mintel to surf the web and check e-mail until July 2008. During trial, Charlton acknowledged that it was his understanding that Mintel’s “IT department \* \* \* was responsible for insuring the return of the laptop computers” as part of the exit interview, but that did not occur at the time of Neergheen’s departure from Mintel.

By reason of Neergheen's employment at Mintel, he had access to Mintel's confidential and proprietary information.<sup>4</sup> On April 23, Mintel began searching and monitoring Neergheen's e-mails. On April 24 and 29, 2008, Neergheen sent eight Mintel files to his personal e-mail address. Those files dealt with Mintel's marketing activities, projects, and initiatives, and included information regarding specific vendors, prospective clients (and their addresses), budgets, trade shows, and a web seminar ("webinar") entitled Comperemedia. Neergheen sent additional Mintel files to his personal e-mail address during the five months between when he learned his position was being eliminated and his resignation date. Neergheen also used USB devices issued by Mintel to hold and transfer Mintel files. Although Mintel was aware prior to Neergheen's last day that Neergheen had sent to his private e-mail address information that Mintel considered proprietary and confidential, no one asked Neergheen about those e-mails until after he left Mintel. At some point shortly after he left, Mintel contacted Neergheen and told him that he should not do anything with any Mintel information.

Mintel filed its complaint for injunctive and other relief on July 11, 2008. On July 15, 2008, counsel filed an appearance on behalf of Neergheen. A hearing on Mintel's motion for a temporary restraining order ("TRO") was held on July 15, 2008. On July 16, the Court entered a TRO that required Neergheen to return to Mintel all copied, printed, or downloaded files, materials, and information taken from Mintel and to provide Mintel with forensic copies of all personal desktop or laptop computers, and prohibited Neergheen from deleting any files from his

---

<sup>4</sup> Mintel does not prohibit its employees from e-mailing documents to their person e-mail accounts, downloading Mintel documents onto hard drives, zip disks, USB sticks, or compact disks, or printing Mintel documents. When Mintel employees send documents to their personal e-mail accounts, the integrity of such documents is not impaired, the availability of such documents is not impaired, and no programs or computer systems are impaired.

personal desktop or laptop computer related to or taken from Intel.<sup>5</sup> Neergheen turned over his laptop computer on July 18, 2008.

Neergheen testified that he occasionally would e-mail documents to his personal account and use USB drives to save his documents in order to work outside the office. Neergheen testified that he did not delete from the laptop any files relating to Intel after July 11, 2008. Neergheen maintains that he did not share any of the Intel documents with Datamonitor and did not transfer the documents in electronic format to any other device or computer. Intel did

---

<sup>5</sup> By agreement of the parties, the TRO has remained in effect until the issuance of today's opinion. It stated in full as follows:

- A. Defendant, his agents, servants, employees, officers, attorneys, successors and assigns, and all persons, firms, and corporations acting in connection or participation with him or on his behalf, are enjoined from using, referencing, evaluating, or copying all originals and copies of information or documents misappropriated from Intel in hard copy or electronically stored;
- B. Defendant, his agents, servants, employees, officers, attorneys, successors and assigns, and all persons, firms, and corporations acting in connection or participation with him or on his behalf, are enjoined from revealing or disclosing in any manner information and documents misappropriated from Intel in hard copy or electronically stored;
- C. Defendant is required to return to Intel all copied, printed, and/or downloaded files, materials, and information taken from Intel;
- D. Defendant is required to produce forensic copies of all personal desktop and/or laptop computers;
- E. Defendant, his agents, servants, employees, officers, attorneys, successors and assigns, and all persons, firms, and corporations acting in connection or participation with him or on his behalf, are prohibited from deleting any files from Defendant's personal desktop and/or laptop computer related to or taken from Intel;
- F. Defendant is prohibited from contacting or soliciting any Intel customer or client that Defendant had contact with during the last twelve (12) months of his respective employments with Intel;
- G. Defendant is prohibited from soliciting or contacting any Intel employee for purposes of working at Datamonitor or any other competitor of Intel.



not offer any evidence from which the Court could conclude that it is more likely than not that confidential Mintel documents were transferred from Neergheen's laptop or USB devices to Datamonitor. Nor has Mintel offered evidence that it is more likely than not that Neergheen engaged in the destruction of any relevant documents in this case. Normal computer usage, even leaving a computer on without actively using it, can result in the changing or overwriting of data on a computer.

In addition, Mintel has not offered any evidence that Neergheen has solicited any of Mintel's customers or accepted orders for products or services competitive with Mintel from customers he dealt with during his employment with Mintel. Perhaps this is not surprising, given that shortly before Neergheen left Mintel, Steve Charlton emailed Jon Butcher, CEO of Mintel Americas, stating, "I'm not as concerned about the TAs [trade associations]. He has been transitioning out of that role over the last six months anyhow." Mintel also has not offered any evidence that it lost any customers, goodwill, or continuity of business relationships as a result of Neergheen's activity or his employment with Datamonitor.

## **II. Conclusions of Law**

In deciding whether to grant injunctive relief, a court considers: (1) whether the plaintiff has a reasonable likelihood of success on the merits; (2) whether the plaintiff will have an adequate remedy at law or will be irreparably harmed if the injunction does not issue; (3) whether the threatened injury to the plaintiff outweighs the threatened harm the injunction may inflict on the defendant; and (4) whether the granting of the injunction will harm the public interest. *N.L.R.B. v. Electro-Voice, Inc.*, 83 F.3d 1559, 1567 (7th Cir. 1996); *Faheem-El v. Klinicar*, 841 F.2d 712, 716 (7th Cir. 1988). A permanent injunction is not provisional in nature, but rather is a final judgment. See *Walgreen Co. v. Sara Creek Property Co.*, 966 F.2d 273, 275 (7th Cir. 1992). Thus, when the plaintiff is seeking a permanent injunction, the first of the four

traditional factors is slightly modified. The issue is not whether the plaintiff has demonstrated a reasonable *likelihood* of success on the merits, but whether he has *in fact* succeeded on the merits. See *Amoco v. Village of Gambell*, 480 U.S. 531, 546 n. 12 (1987); *Plummer v. American Institute of Certified Public Accountants*, 97 F.3d 220, 229 (7th Cir. 1996).

Mintel seeks injunctive relief on the following claims: (1) violations of the Computer Fraud and Abuse Act; (2) violations of the non-compete, non-disclosure, and non-solicitation covenants within his employment contracts; and (3) misappropriation of trade secrets. Additionally, while Mintel does not have a “claim” for spoliation of evidence, Mintel has moved for default judgment against Neergheen as a discovery sanction for allegedly destroying evidence related to this lawsuit. In the event that the Court declines to grant a default judgment, Mintel asks the Court to draw an adverse inference that the allegedly “lost evidence” would weigh against Neergheen on the underlying claims.

#### **A. Spoliation**

On August 29, 2008, Plaintiff filed a motion for rule to show cause, for discovery sanctions, and for sanctions because of evidence spoliation [61]. Mintel argued that Neergheen had a duty to preserve the hard drive on the laptop from the date the complaint in this case was filed, and that he failed to do so. On January 22, 2009, Magistrate Judge Maria Valdez, who handled several discovery issues in this case, denied Plaintiff’s motion [205]. In reaching that decision, Magistrate Judge Valdez determined that Neergheen’s acts of turning on the computer, accessing the Internet, and allowing an automated defragmentation (“defrag”) program to run during the one week period at issue (July 11 through July 18) did not result in the destruction of relevant evidence [205 at 7]. Furthermore, she determined that Mintel failed to demonstrate that any actions by Neergheen were motivated by bad faith or, put another way, that any destruction of data had been done intentionally for the purpose of hiding adverse information [205 at 7-8].

On January 30, 2009, Intel filed objections [214] to Magistrate Judge Valdez's Order [205]. In an Order [242] dated April 17, 2009, this Court reserved ruling on Plaintiff's objections to Magistrate Judge Valdez's Order [205] until after completion of the bench trial, at which experts for both sides presented extensive testimony on the spoliation issue. The Court now considers, *de novo*, the issues presented by Plaintiff's motion for sanctions for alleged spoliation [61].

A party asserting spoliation must show by "clear and convincing evidence" that the opposing party intentionally destroyed evidence. *Rodgers v. Lowe's Home Ctrs., Inc.*, 2007 WL 257714, at \*7 (N.D. Ill. 2007) (citing *Miksis v. Howard*, 106 F.3d 754, 763 (7th Cir. 1997), and *Crabtree v. Nat'l Steel Corp.*, 261 F.3d 715, 721 (7th Cir. 2001)). "Absent exceptional circumstances, a court may not impose sanctions under [the Federal Rules of Civil Procedure] on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system." Fed. R. Civ. P. 37(e). "A prerequisite to the imposition of sanctions for spoliation is a determination that the party, which destroyed the documents, had an obligation to preserve them." *Cohn v. Taco Bell Corp.*, 1995 WL 519968, at \*5 (N.D. Ill. Aug. 30, 1995). Parties in litigation have a duty to preserve relevant evidence "over which the non-preserving party had control and reasonably knew or could reasonably foresee was material to a potential legal action." *China Ocean Shipping (Group) Co., v. Simone Metals, Inc.*, 1999 WL 966443, at \*3 (N.D. Ill. Sep. 30, 1999).

"Because a default judgment deprives a party of a hearing on the merits, the harsh nature of this sanction should usually be employed in extreme situations where there is evidence of willfulness, bad faith, or fault by the noncomplying party." *Danis v. USN Communications, Inc.*, 2000 WL 1694325, at \*33 (N.D. Ill. Oct. 23, 2000). "Bad faith" means destruction "for the purpose of hiding adverse information." *Mathis v. John Morden Buick, Inc.*, 136 F.3d 1153, 1155 (7th Cir. 1998). "[W]illfulness and bad faith are associated with conduct that is intentional or

reckless \* \* \*.” *Long v. Steepro*, 213 F.3d 983, 987 (7th Cir. 2000). “Fault” is unconcerned with the non-complying party’s subjective motivation, but rather describes the reasonableness of the conduct. *Langley v. Union Electric Co.*, 107 F.3d 510, 514 (7th Cir. 1997). Fault may include “gross negligence” or “a flagrant disregard” of the duty to “preserve and monitor the condition” of material evidence. *Marrocco v. Gen. Motors*, 966 F.2d 220, 224 (7th Cir. 1992).

The destruction of evidence presumption has two elements: (1) the totality of the circumstances must show that the destruction was in bad faith, and (2) if the first prong is met, then the court “may \* \* \* infer from this state of mind that the contents of the evidence would be unfavorable to the party if introduced in court.” *S.C. Johnson & Son, Inc. v. Louisville & Nashville Railroad Co.*, 695 F.2d 253, 258 (7th Cir. 1983). “An employe[e]’s destruction of or inability to produce a document, standing alone, does not warrant an inference that the document, if produced, would have contained information adverse to the employe[e]’s case.” *Park v. City of Chicago*, 297 F.3d 606, 615 (7th Cir. 2002). Rather, in order to draw an inference that destroyed evidence contained adverse information, “[the court] must find that [the party] intentionally destroyed the documents in bad faith.” *Faas v. Sears, Roebuck & Co.*, 532 F.3d 633, 644 (7th Cir. 2008); see also *Trask-Morton v. Motel 6 Operating L.P.*, 534 F.3d 672, 681 (7th Cir. 2008). “Thus, the crucial element is not that evidence was destroyed but rather the reason for the destruction.” *Faas*, 532 F.3d at 644 (quoting *Park*, 297 F.3d at 615) (internal quotation marks omitted). “A document is destroyed in bad faith if it is destroyed for the purpose of hiding adverse information.” *Rummery v. Ill. Bell Tel. Co.*, 250 F.3d 553, 558 (7th Cir. 2001); see also *Trask-Morton*, 534 F.3d at 681. More than mere speculation is necessary to find that the documents contained adverse information. *Rummery*, 250 F.3d at 558.

Mintel’s expert contends that because Neergheen used the laptop at all, spoliation occurred. However, what this Court forbid in the temporary restraining order – drafted by

Mintel and entered at its request – was the deletion of any files relating to or taken from Mintel. The Court did not forbid Neergheen from turning on the computer, accessing the internet, or deleting files not related to Mintel. If Mintel had wanted such restrictions, it should have requested them. During trial, Mintel’s expert admitted that he did not find any evidence that any confidential Mintel files were ever transmitted from Neergheen’s computer to Datamonitor.<sup>6</sup> In regard to the alleged “wiping” of the USB devices, there are contradicting opinions of two forensic experts regarding the hexadecimal value “FF” found on the unallocated space of both drives. Mintel’s expert found no traces of a wiping program on the USB drives apart from the presence of the “FF” pattern and he did not state that he was familiar with any wiping program that leaves an “FF” hexadecimal pattern. Neergheen’s expert offered a reasonable explanation for the “FF” pattern in the absence of any other evidence of wiping. In addition, the fact that two Mintel-related documents – neither of which has been shown to have been transferred to any Datamonitor device – actually remained on the USB devices provides evidence that there was no intentional “wiping” of the device. See *Bryant v. Gardner*, 2008 WL 4966589, at \*15 (N.D. Ill. 2008) (“Had Defendants purposefully deleted unfavorable evidence from the laptop, the Court finds it unlikely that [ ] other documents favorable to Plaintiff would have remained”). In any event, it seems rather unlikely that if Neergheen – whom Mintel has portrayed as a sophisticated computer user – had wished to “wipe” the laptop and the USB devices, he would have used one of the many wiping programs that Mintel’s expert acknowledged are commercially available. Tr. 384-389.

---

<sup>6</sup> Mintel’s forensic expert conduct a forensic analysis of the USB drives produced by Neergheen and found that a document contained on one USB drive had been printed on Datamonitor’s print server “Thames.” With respect to the Thames printer, it was determined that Neergheen had printed his resignation letter on a Datamonitor printer. His resignation letter was not a confidential document nor was it proprietary Mintel information. The document has no bearing on any of the claims or defenses in the present litigation.

The parties do not dispute that data and/or “metadata” on the laptop at issue was destroyed after the filing of the complaint on July 11, 2008. However, there has been no evidence presented that the data that was destroyed was relevant. Mintel argues that the “evidence” at issue is not just the existence of Mintel confidential documents on the laptop, but also the metadata which shows the activities done by or through the laptop, including the attachment of USB devices, the calling up of Microsoft Office programs, and links to documents or websites. Mintel’s expert opined that Neergheen undertook activities which rendered the ability to fully document all of that activity (from May 2008 through the date of imaging) impossible. On the other side, Neergheen’s expert admits that data was destroyed and overwritten, but opines that nothing Neergheen did (or allowed to take place by virtue of using the computer to check e-mail and “surf the web”), on a computer that he thought was his own, was the least bit suspicious or out of the ordinary.

In regard to Mintel’s allegations concerning programs on the laptop that would have destroyed metadata or overwritten files, the Court finds that the expert testimony presented at trial, as well as expert affidavits and deposition testimony, lead to the conclusion that those programs were not user initiated. Rather, they were automated programs that had virtually no effect on the hard drive. Specifically, the automated antivirus program did not have any effect on the last access dates of any substantive files relating to this litigation. The virus scan software did not alter the file metadata of the files being scanned. The only files that would have had their last access dates updated are the few files associated with the McAfee program itself, rather than substantive documents. Additionally, any defrag program that was run on the computer was not user initiated; rather, the laptop’s operating system was set to run a “boot optimization” automatically, and the effect of the automatic defrag on the hard drive was “virtually none.”

The facts surrounding the alleged spoliation do not support an inference that any unrecoverable material would have been unfavorable to Neergheen. No inference is appropriate because the evidence did not establish that it was more likely than not that any of Neergheen's actions were taken in bad faith. As the Seventh Circuit opined in *Rummery*, 250 F.3d at 558, more than mere speculation is necessary to find that the documents contained adverse information, and looking at the totality of circumstances, the result urged by Intel is grounded in too much speculation. In short, Neergheen's conduct really was "innocent-looking actions that meld[ed] into what could be construed as 'typical' computer usage," rather than a *pattern* that is easily recognized by forensic experts as spoliation. Accordingly, like Magistrate Judge Valdez,<sup>7</sup> the Court concludes that none of the sanctions sought by Intel, including default or adverse inferences, are warranted here.<sup>8</sup>

## **B. Violation of the Computer Fraud and Abuse Act**

The Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, provides for the entry of civil injunctive relief as well as the recovery of money damages for a violation of its provisions.<sup>9</sup> See 18 U.S.C. § 1030(g) (providing that "[a]ny person who suffers damage or loss

---

<sup>7</sup> Consistent with the discussion above, the Court overrules Intel's objections [214] to Magistrate Judge Valdez's order of January 22, 2009 [205].

<sup>8</sup> That Neergheen continued to use the laptop computer after his separation from Intel strikes the Court as neither surprising nor sinister in view of the facts that (1) Intel did not ask him to return the laptop at his exit interview and (2) even at the outset of this litigation, Intel was unclear as to whether the laptop belonged to Neergheen or Intel. For instance, in Intel's Motion for Rule to Show Cause, filed on July 22, 2008, and in Intel's second Motion for Rule to Show Cause for Discovery Sanctions and for Sanctions because of Evidence Spoliation, filed on August 29, 2008, Intel makes repeated reference to "Defendant's personal computer," "Defendant's computer," or "Neergheen's computer." [See, e.g., 21 & 61.]

<sup>9</sup> Congress amended several portions of the CFAA effective September 2008. However, the Court will apply the terms of the CFAA that were in effect during the time of the complained of conduct. See, e.g., *Motorola v. Lemko Corp.*, 609 F. Supp. 2d 760, 765 (N.D. Ill. 2009) ("Congress recently amended several sections of the CFAA [however] the court will apply the terms of the CFAA as they existed during the course of the defendants' alleged conduct.").

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”). Mintel alleges that Neergheen violated the CFAA because he “copied, emailed to his personal address and/or printed confidential and proprietary trade secret information from his work computer on April 29, 2008.” With respect to specific provisions, Mintel appears to allege that Neergheen violated §§ 1030(a)(5)(B)(iii), 1030(a)(4), and 1030(a)(2)(C) of the CFAA, although Mintel’s proposed conclusions of law do not make reference to the specific provisions.

The CFAA provides for civil liability if one “intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage \* \* \*.” 18 U.S.C. § 1030(a)(5)(A)(iii). A plaintiff must demonstrate damage in order to recover under this provision of the CFAA. See *Motorola, Inc. v. Lemko Corp.*, 609 F. Supp. 2d 760, 766 (N.D. Ill. Feb. 11, 2009); *Garelli Wong & Associates, Inc. v. Nichols*, 551 F. Supp. 2d 704, 708-09 (N.D. Ill. 2008). The CFAA defines “damage” as “impairment to the integrity or availability of data, a program, a system, or information.” 18 U.S.C. § 1030(e)(8).

Neergheen argues that his allegedly unauthorized acts of copying and e-mailing Mintel’s computer files did not impair the integrity or availability of the information in Mintel’s system, and this Court concurs. As several judges in this district have recently found (or confirmed), the “underlying concern of the Act [is] damage to data” and “the statute was not meant to cover the disloyal employee who walks off with confidential information.” *Kluber Skahan & Assocs. v. Cordogan, Clark & Assocs.*, 2009 WL 466812, at \*8 n. 14 (N.D. Ill. Feb. 25, 2009); see also *Garelli Wong & Assocs., Inc.*, 551 F. Supp. 2d at 708-09; *Sam’s Wines & Liquors, Inc. v. Hartig*, 2008 WL 4394962 (N.D. Ill. Sept. 24, 2008) (finding no damage where an employee stole plaintiff’s customer data from plaintiff’s computer and took the information to one of plaintiff’s competitors). Instead, the plain language of the statute appears to refer to situations in which



data is lost or impaired because it was erased or otherwise destroyed, or in which computer networks or databases are disabled. Thus, this Court, like other courts in this district, finds that copying, e-mailing or printing electronic files from a computer database is not enough to satisfy the damage requirement of the CFAA. Rather, there must be destruction or impairment to the integrity of the underlying data. Neergheen did not erase any files from Mintel's database, nor did he install any destructive software that would compromise the integrity of the data or disable Mintel's computers or its networks. Thus, Mintel has not demonstrated that it suffered the type of damage contemplated by § 1030(a)(5)(A)(iii) of the CFAA.

To the extent that Mintel is attempting to assert claims under §§ 1030(a)(2) or (a)(4),<sup>10</sup> Mintel must demonstrate either "damage or loss." See 18 U.S.C. § 1030(g); *SKF USA, Inc. v. Bjerkness*, 636 F. Supp. 2d 696, 720 (N.D. Ill. 2009); *Motorola*, 2009 WL 383444, at \*4. Since the Court has already determined that Mintel has not demonstrated damage as it is contemplated by the CFAA, it must demonstrate "loss." Like damage, the term "loss" also has a specific meaning under the CFAA: it refers to "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage 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).

Here, Mintel claims that its losses consist of the fees that it paid to its expert to assess Neergheen's allegedly improper actions. However, Mintel's expert was not assessing whether Neergheen had "damaged" Mintel's computers or data, as the CFAA contemplates "damage";

---

<sup>10</sup> A person violates § 1030(a)(2) if he intentionally accesses a "computer without authorization or exceeds authorized access and thereby obtains information from any protected computer if the conduct involved an interstate or foreign communication." A person violates § 1030(a)(4) if he "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 something of value \* \* \*."

rather, the expert was hired for assistance in Intel's lawsuit against Neergheen. While that is certainly a legitimate business concern, it does not transform any harms allegedly suffered by Intel into "losses" under the CFAA. The alleged loss must relate to the investigation or repair of a computer or computer system following a violation that caused impairment or unavailability of data or interruption of service. See 18 U.S.C. § 1030(e)(11); *Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands Int'l Inc.*, 2009 WL 743215, at \*4 (N.D. Ill. Mar. 19, 2009); *First Mortgage Corp. v. Baser*, 2008 WL 4534124, at \*3 (N.D. Ill. Apr. 30, 2008). Thus, costs that are not related to computer impairment or computer damages are not cognizable "losses" under the CFAA. See *Cassetica Software, Inc. v. Computer Sciences Corp.*, 2009 WL 1703015, at \*4 (N.D. Ill. June 18, 2009) (finding that to state a claim based upon a loss, "the alleged loss must relate to the investigation or repair of a computer system following a violation that caused impairment or unavailability of data"); *SKF USA*, 636 F. Supp. 2d at 721 (lost revenue caused by copying confidential information not compensable "loss" under CFAA); *Del Monte*, 2009 WL 743215, at \*4 (in absence of impairment or unavailability of computerized data, costs incurred for "damage assessment" not recoverable under the CFAA). Because Intel has not demonstrated that it suffered costs related to damage to its computers or that it suffered any service interruptions, it has failed to show any loss redressable under the CFAA.

### **C. Violation of the Illinois Trade Secret Act**

To prevail on a claim under the Illinois Trade Secrets Act, a plaintiff must prove (1) the existence of a "trade secret" and (2) "misappropriation" of that trade secret. *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262, 1268 (7th Cir. 1995); see also *Strata Marketing, Inc. v. Murphy*, 740 N.E.2d 1166, 1176 (Ill. App. Ct. 1st Dist. 2000) (finding that plaintiff must establish that the information at issue was (i) a trade secret, (ii) that was misappropriated, and (iii) that was used in the defendant's business); *Magellan Intern. Corp. v. Salzgitter Handel GmbH*, 76 F. Supp. 2d

919, 927 (N.D. Ill. 1999). Under Section 2(d) of the Act (765 ILCS 1065/2(d)), a trade secret is defined as follows:

[I]nformation, including but not limited to, technical or non-technical data, a formula, pattern, compilation, program, device, method, technique, drawing, process, financial data, or list of actual or potential customers or suppliers, that: (1) is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use; and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality.

The protection afforded trade secrets reflects a balancing of conflicting social and economic interests. Where an employer has invested substantial time, money, and effort to obtain a secret advantage, the secret should be protected from an employee who obtains it through improper means. See *ILG Industries, Inc. v. Scott*, 273 N.E.2d 393, 396 (Ill. 1971). Nevertheless, in a competitive market, an employee must be entitled to utilize the general knowledge and skills acquired through experience in pursuing his chosen occupation. See *Service Centers of Chicago, Inc. v. Minogue*, 535 N.E.2d 1132, 1135 (Ill. App. Ct. 1st Dist. 1989).

The key factor to establishing secrecy “is the ease with which the information can be readily duplicated without involving considerable time, effort or expense.” *Stampede Tool Warehouse, Inc. v. May*, 651 N.E.2d 209, 215 (Ill. App. Ct. 1st Dist. 1995). Where information is not “readily ascertainable” from a public source but is developed over time with a substantial amount of effort and expense, the information is “secret.” *Id.* at 216. Information meeting the ITSA “secrecy” criterion includes customer lists that are not readily ascertainable (*id.*); pricing, distribution, and marketing plans (*PepsiCo*, 54 F.3d at 1268); and sales data and market analysis information (*Barrier, Inc. v. Stanley Works*, 79 F.3d 1112, 1117 (Fed. Cir. 1996)).

The documents that Neergheen e-mailed to himself are trade secrets. Those files dealt with Mintel’s marketing activities, projects, and initiatives, and included information regarding specific vendors, prospective clients (and their addresses), budgets, trade shows, and the web

seminar Comperemedia. The information contained in those documents meets the standard of being sufficiently secret to derive economic value from not being generally known to others who can obtain economic value from its disclosure or use. Moreover, Mintel took reasonable steps to safeguard its confidential information. The testimony at trial demonstrated that only those employees who needed to know the contents of these documents to perform their job functions were given access to the documents. See *Elmer Miller, Inc. v. Landis*, 625 N.E.2d 338, 342 (Ill. App. Ct. 1st Dist. 1993) (finding only the employees who needed to know the information had access to it). Mintel had security measures in place that restricted access to certain information, and only employees in Mintel’s marketing department had access to the documents at issue. See *Service Centers of Chicago, Inc. v. Minogue*, 535 N.E.2d 1132, 1136 (1st Dist. 1989) (finding trade secret protection maintained when the information is used by a person in his business operations and is known only by such person and such limited other persons to whom it may be reasonably necessary to confide it). Furthermore, Mintel required Neergheen to sign non-disclosure agreements, which clearly stated that such information was not to be disseminated and needed to be returned at the end of his employment. See *RKI, Inc. v. Grimes*, 177 F. Supp. 2d 859, 875 (N.D. Ill. 2001) (considering the signing of a non-disclosure agreement as one factor in determining whether company took reasonable steps to safeguard its confidential information).

In addition to demonstrating that the documents at issue are trade secrets – which Mintel successfully has done<sup>11</sup> – Mintel also must demonstrate that Neergheen “misappropriated” the

---

<sup>11</sup> Prior to trial, Mintel requested that certain documents introduced at trial be placed under seal because those documents constitute trade secrets. Mintel appropriately has parsed its trial exhibits to eliminate from its request portions of documents that clearly do not satisfy the standard for protection as a trade secret. Neergheen objected to this request, arguing that the documents were not trade secrets. Generally, documents that “influence or underpin [a] judicial decision are open to public inspection unless they meet the definition of trade secrets or other categories of bona fide long-term confidentiality.” See *Baxter Intern., Inc. v. Abbott Laboratories*, 297 F.3d 544, 545 (7th Cir. 2002). Since the Court has concluded that the documents at issue are trade secrets, the Court orders that the following documents be placed under seal: MN0000704-MN0000873 (within Joint Ex. 6); MNTL00558-MNTL00588 (within Joint Ex.

trade secrets. Put another way, Mintel must show that Neergheen used the trade secrets at issue “for purposes other than serving the interests of” Mintel. *RFI*, 177 F. Supp. 2d at 875. The evidence presented at trial indicated that when Neergheen sent the documents to himself, he was upset about losing his job and had ulterior motives. However, he was “caught” by Mintel almost immediately and simply was told by Mintel representatives not to use the information. Mintel has not shown that since that time Neergheen used or disclosed to a third party (particularly, Datamonitor) the trade secrets at issue. Mintel has not demonstrated that Neergheen (or Datamonitor) solicited business from Mintel’s customers, or that Neergheen or Datamonitor has used the documents at issue in any way. In fact, as a condition of Neergheen’s employment, Datamonitor required him to sign an agreement prohibiting him from disclosing any confidential information or trade secrets to Datamonitor or even discussing his former employment with Mintel. Datamonitor also has prohibited Neergheen from contacting any customers with whom he was in contact while employed at Mintel. See *id.* at 876 (finding that one of the factors to consider when determining whether trade secrets will inevitably be used is “the actions the new employer has taken to prevent the former employee from using or disclosing trade secrets of the former employer.”). Finally, Datamonitor has prohibited Neergheen from working in the consumer product goods and retail sectors, which comprised approximately eighty percent of Neergheen’s work at Mintel.

The question remains whether it is “inevitable” that Neergheen will use the information that he obtained through improper means in his current job at Datamonitor. *RFI*, 177 F. Supp. 2d

---

6); MN0000529-MN0000575 (within Joint Ex. 7); MNTL00437-MNTL00481 (within Joint Ex. 7); MN0000315 (within Ex. 101C); MN0000579-MN0000589 (within Ex. 101D); MN000627-MN000642 (within Ex. 101E); MN0000893 (within Ex. 101I); MN0000875-MN0000882 (within Ex. 101L); MN0000329-MN0000370 (within Ex. 101N); MN0000221-MN0000234 (within Ex. 101O); MN0000885-MN0000886 (within Ex. 101Q); MN0000505-MN0000509 (within Ex. 101R); MN0000102-MN0000110 (within Ex. 101U); MN0000113-MN0000114 (within Ex. 101Z); MN0000191-MN0000209 (within Ex. 101CC); MN0000117-MN0000172 (within Ex. 101II); MN0000505-MN0000509 (within Ex. 101MM).

at 875; see also ITSA § 3 (permitting an injunction to issue to prevent even threatened use or disclosure of trade secrets). The factors to consider in determining whether disclosure of trade secrets is inevitable are: (1) the level of competition between the former employer and the new employer; (2) whether the employee's position with the new employer is comparable to the position he held with the former employer; and (3) the actions that the new employer has taken to prevent the former employee from using or disclosing trade secrets of the former employer. *PepsiCo, Inc. v. Redmond*, 1996 WL 3965, at \*20 (N.D. Ill. Jan. 2, 1996). In this case, Intel and Datamonitor are direct competitors. In addition, Intel has demonstrated that Datamonitor hired Neergheen to fill a role that is somewhat similar to his former role at Intel in that Neergheen continues to work in marketing and with trade associations, as he did at Intel. However, at Intel, Neergheen's focus was on consumer packaged goods and retail sectors, while at Datamonitor he works primarily in the pharmaceuticals and technology sectors. Therefore, although the basic knowledge and experience he gained while working at Intel – e.g., marketing techniques, negotiating partnerships, how to approach and/or deal with trade associations, etc. – is being utilized by Datamonitor, Neergheen's specific experience related to consumer packaged goods and retail, as well as his connections in those sectors and the particular insight to be gleaned from the trade secrets at issue, has been shelved. The second factor therefore cuts both ways – although it is worth repeating that Neergheen's boss at Intel, Steve Charlton, stated around the time of Neergheen's departure that he was “not as concerned about the TAs [trade associations]” because Neergheen had been “transitioning out of that role” during his last six months at Intel. Finally, Datamonitor has taken several steps to ensure that Neergheen does not use or disclose Intel's trade secrets, including requiring him to sign an agreement prohibiting him from disclosing any confidential information or trade secrets to

Datamonitor, prohibiting him from discussing his former employment with Intel, and forbidding him to contact any customers with whom he was in contact while employed at Intel.

Although Intel alleges that, unless Neergheen is enjoined under the ITSA, he “will continue to have access and the ability to make use of Intel’s trade secrets,” such allegations of the “potential” for use of Intel’s trade secrets are not enough to state a claim under the ITSA. See *Teradyne, Inc. v. Clear Communications Corp.*, 707 F. Supp. 353, 356-57 (N.D. Ill. 1989). Based on the foregoing, Intel has not demonstrated that Neergheen used or has designs on using the improperly acquired information to Intel’s detriment in the future and thus its misappropriation claims fails.<sup>12</sup>

**D. Breach of Contract: Violations of the Non-Compete, Nondisclosure, and Non-Solicitation Covenants in Neergheen’s Non-Compete Agreement and Contract of Employment**

Illinois courts disfavor and closely scrutinize restrictive covenants because they are “repugnant to the public policy encouraging an open and competitive marketplace.” *Roberge v. Qualiteck Int’l, Inc.*, 2002 WL 109360, at \*4 (N.D. Ill. Jan. 28, 2002) (citing *Bishop v. Lakeland Animal Hosp.*, 268 Ill.App.3d 114, 644 N.E.2d 33, 36 (Ill. App. Ct. 1994)). The basic test applied by Illinois courts in determining the enforceability of a restrictive covenant is “whether the terms of the agreement are reasonable and necessary to protect a legitimate business interest of the employer.” *Outsource Intern., Inc. v. Barton*, 192 F.3d 662, 666 (7th Cir. 1999) (quoting *Office Mates 5, North Shore, Inc. v. Hazen*, 234 Ill. App. 3d 557, 599 N.E.2d 1072, 1080 (1992)). This determination “necessarily turns on the facts and circumstances of each case.” *Id.* Illinois law requires that in order be enforceable, a covenant not to compete must secure a “protectable interest” of the employer. *Curtis 1000, Inc. v. Suess*, 24 F.3d 941, 944 (7th Cir.

---

<sup>12</sup> In any event, the Court is in a position to make sure that Neergheen can never use the improperly acquired information, and has crafted its ruling on Intel’s breach of contract claim, see *infra*, to prohibit Neergheen from ever using this information.

1994). Illinois courts recognize at least two such protectable interests: (1) where the customer relationships are near-permanent and but for the employee's association with the employer the employee would not have had contact with the customers; and (2) where the former employee acquired trade secrets or other confidential information through his employment and subsequently tried to use it for his own benefit. *Outsource Int'l, Inc. v. Barton*, 192 F.3d 662, 666 (7th Cir. 1999).

Restrictive covenants should be narrowly tailored so as to encompass only the protectable interest of the employer. *Outsource Int'l*, 192 F.3d at 669; *Lawrence and Allen, Inc. v. Cambridge Human Resource Group, Inc.*, 292 Ill.App.3d 131, 138, 685 N.E.2d 434, 441 (Ill. App. Ct. 1997). In particular, the temporal and geographic limitations must be reasonably necessary to protect a legitimate business interest of the employer. *Roberge*, 2002 WL 109360, at \*4. A restrictive covenant that does not contain a geographic limitation still may be enforceable if the covenant includes an "activity restraint." *Id.* at \*6. The most common type of activity restraint is a prohibition against soliciting the former employer's customers. *Eichman v. Nat'l Hosp. and Health Care Servs., Inc.*, 308 Ill.App.3d 337, 719 N.E.2d 1141, 1147 (Ill. App. Ct. 1999).

Neergheen commenced employment with Mintel in its London office on or about June 30, 1997. As a condition of Neergheen's employment with Mintel, on June 24, 1998, he signed and executed a contract of employment. The contract included a restrictive covenant that prohibited Neergheen from working for a competitor of Mintel for one year or from soliciting other Mintel employees to leave the company. The contract also included a confidentiality clause that prohibited Neergheen from using or disclosing confidential information that he came into possession of during his time at Mintel. In August 2003, Neergheen transferred to Mintel's Chicago office. As a condition of his continued employment with Mintel in Chicago, Neergheen



agreed to sign a non-compete agreement. In signing the non-compete agreement, Neergheen again consented not to work for a competitor of Mintel for one year or solicit away from Mintel other Mintel employees. The non-compete agreement also contained a confidentiality clause that prohibited Neergheen from using Mintel trade secrets and other confidential or proprietary information for his own benefit or from disclosing such information to any third party, and prohibited Neergheen from soliciting Mintel's customers for a period of one year from the termination date.

Restrictive covenants that lack geographical limitations may be upheld where, as here, the employer competes for customers on a worldwide basis. See *Victaulic Co. v. Tieman*, 499 F.3d 227, 235 (3d Cir. 2007) (“In this Information Age, a *per se* rule against broad geographic restrictions would seem hopelessly antiquated, and [courts] have found broad geographic restrictions reasonable so long as they are roughly consonant with the scope of the employee’s duties.”); see also *Quaker Chemical Corp. v. Varga*, 509 F. Supp. 2d. 469 (E.D. Penn. 2007) (emphasizing that the notion of a too-broad geographic scope has become “antiquated” in light of the “Information Age” and the increasingly global economy). Mintel is an international business with a global presence, and Mintel and its competitors compete for a worldwide market. Neergheen could live and work in many places throughout the world and compete with Mintel. Thus, the broad geographical scope of the agreements, when viewed in conjunction with the reasonable duration of the agreements (one year), does not render the non-compete and non-solicitation provisions unreasonable.

However, to the extent that the agreements Neergheen signed are a “blanket prohibition” on Neergheen working for any competitor, as opposed to an “activity restraint” in which Neergheen is prohibited from engaging in particular types of activities or from soliciting customers he actually had contact with while working for Mintel, they are overbroad. The Court

will not enforce the agreements so as to restrict Neergeen's ability to work for a competitor in any manner whatsoever. See *Roberge*, 2002 WL 109360, at \*4-5. Rather, the Court will continue in place the terms to which Datamonitor and Neergeen agreed, in writing, when Neergeen began his employment with Datamonitor. That is, for a definite period of time, Neergeen will continue to be enjoined from (1) contacting any customers with whom he was in contact while employed at Mintel, and (2) working in the consumer product goods and retail sectors at Datamonitor.

With respect to the length of injunctions, "courts have recognized that where an employee violates a covenant not to compete, the time period may be extended beyond that specified in the contract." *Loewen Group Intl., Inc. v. Haberichter*, 1998 U.S. App. LEXIS 28514, at \*21-22 (7th Cir. Sept. 15, 1998); see, e.g., *JAK Prod. Inc. v. Wiza*, 986 F.2d 1080, 1090 (7th Cir. 1993) ("because the [defendant] violated the covenant not to compete from November 25, 1991 until the injunction, and the covenant requires [defendant] to refrain from such competition for a period of one year, the district court did not err in determining the period of one year as March 11, 1992 to March 11, 1993. To hold otherwise would reduce the covenant from twelve to eight months \* \* \*"). It is within the Court's equitable powers to determine the length of such an extension. *Loewen Group*, 1998 U.S. App. LEXIS 28514, at \*24-25. Thus, the Court determines that the appropriate sanction for Neergeen's conduct in accepting employment with a Mintel competitor in violation of his non-compete agreements is that he be permanently enjoined from contacting any Mintel clients or employees for a period of nine months following the entry of this Order and that he be permanently enjoined from working in the consumer packaged goods and retail sectors of Datamonitor or any other Mintel competitor for a period of six months following entry of this Order.

With respect to the non-disclosure provisions, “[a]n employer’s trade secrets are considered a protectable interest for a restrictive covenant under Illinois law.” *Pepsico, Inc. v. Redmond*, 54 F.3d 1262, 1271 (7th Cir. 1995). The Court already has determined that the Mintel documents that Neergheen e-mailed to himself after he resigned from Mintel were trade secrets. Thus, Neergheen violated the nondisclosure covenant when he retained those documents after his termination. Since there has been no evidence presented that Neergheen used those documents for his benefit or the benefit of a third party, Neergheen’s sanction for breaching the non-disclosure provisions is limited to permanently enjoining him from using any of Mintel’s confidential, proprietary, and trade secret information that was the subject of this lawsuit.

**E. Irreparable harm, Balance of Harms, and Public Interest**

The Court finds that the remedies fashioned by the Court adequately balance the harms at issue and serve the public interest. Moreover, the injunctions that the Court has deemed appropriate account for the irreparable harm of allowing Neergheen to use Mintel’s trade secrets for his own benefit or the benefit of a third party.

**III. Conclusion**

Based on the foregoing, Mintel’s request for sanctions on the basis of alleged spoliation is respectfully denied. The Court enters judgment in favor of Neergheen and against Mintel on Mintel’s claims against Neergheen under the ITSA and the CFAA, and enters judgment in favor of Mintel and against Neergheen on Mintel’s breach of contract claims. Neergheen’s counterclaims seeking a declaratory judgment that the restrictive covenants found in his employment contracts are invalid as a matter of law are dismissed. Having established actual success on the merits of its breach of contract claims, an inadequate remedy at law, and that the balance of harms and public interest weigh in its favor, Mintel is entitled to the foregoing relief:

- (1) Neergheen is enjoined from contacting any Mintel clients or employees for a period of nine months following the entry of this Order.
- (2) Neergheen is enjoined from working in the consumer packaged goods and retail sectors of Datamonitor or any other Mintel competitor for a period of six months following entry of this Order; and
- (3) Neergheen (as well as his agents, servants, employees, officers, attorneys, successors and assigns, and all persons, firms, and corporations acting in connection or participation with him or on his behalf) continue to be enjoined from using, referencing, evaluating, or copying all originals and copies of information or documents misappropriated from Mintel in hard copy or electronically stored, and from revealing or disclosing in any manner information and documents misappropriated from Mintel in hard copy or electronically stored.



Dated: January 12, 2010

---

Robert M. Dow, Jr.  
United States District Judge