IN THE UNITED STATES DISTRICT COURT

FOR THE WESTERN DISTRICT OF WISCONSIN

- -

MAXPOWER CORPORATION,
a Colorado Corporation, and
MAXPOWER WISCONSIN
CORPORATION, a Wisconsin
Corporation,

OPINION AND ORDER

Plaintiffs,

08-cv-150-bbc

v.

GENE ABRAHAM, KEVIN HOBSON
AND BRADY WILKENS,[1]

Defendants.

- -

Thomas Ebner, president of plaintiff MaxPower Corporation, was displeased when defendant Kevin Hobson went to work for a direct competitor after he was terminated from his job with plaintiff MaxPower Wisconsin Corporation in late December or early January 2007. He was even more displeased when defendants Gene Abraham and Brady Wilkins left their employment with MaxPower Wisconsin later in January 2008 and went to work for

[1] Kirk Soe was named as a defendant in the complaint but was dismissed by plaintiffs voluntarily, with prejudice and without fees, at the close of the hearing on plaintiffs' motion for a preliminary injunction.

the same competitor. Plaintiffs brought suit against defendants, alleging that they had committed myriad wrongs in the process of changing jobs. Plaintiffs' claims against defendants include state claims such as misappropriation of trade secrets in violation of Wisconsin's Uniform Trade Secrets Act, Wis. Stat. § 134.90, intentional interference with prospective business opportunity and breach of the duty of loyalty, along with one federal claim of violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. This last claim gives the court federal question jurisdiction over the federal claim under 28 U.S.C. § 1331 (federal question jurisdiction) and, by virtue of 28 U.S.C. § 1367 (supplemental jurisdiction), over the remainder of the case.

Presently before the court is plaintiffs' motion for a preliminary injunction requiring defendants to return any information that they deleted from plaintiffs' servers, barring defendants from using or disclosing plaintiffs' trade secrets and enjoining them from continuing to work for any direct competitor.

In preparation for the April 24, 2008 hearing on the motion, plaintiffs obtained an order from the United States Magistrate Judge directing defendants to turn over their laptops for examination by a forensic expert. The examination gave plaintiffs additional reasons to think that defendants had engaged in the intentional destruction of evidence and had accessed plaintiffs' servers illegally. At the start of the hearing on the motion for preliminary examination, plaintiffs asked for reasonable sanctions, alleging among other

things that the forensic examination of Abraham's laptop drive showed that it had been wiped clean of information after the magistrate judge had approved the forensic examination but before the examination could take place. Plaintiffs argued that it would be proper for the court to impose a reasonable sanction for this action, whether it be drawing an adverse inference from the destruction of evidence or entering judgment against defendants. I took plaintiffs' request under consideration.

From the evidence adduced at the hearing, including the parties' affidavits, I find the following facts, solely for the purpose of deciding the motions for a preliminary injunction and for sanctions.

FACTS

Plaintiff MaxPower Corporation is a Colorado corporation that distributes to resellers uninterruptible power systems that plaintiff purchases primarily from a company known as PowerWare, which is part of Eaton Corporation. The resellers sell the systems to end users.

Defendants Gene Abraham, Brady Wilkens and Kevin Hobson were employed by defendant MaxPower from January 1, 2005 through late December 2007 or January 2008. All three had previously worked for a company known as BestPower, which was a manufacturer of uninterruptible power systems. When Eaton bought BestPower, changed its name to PowerWare and moved it to North Carolina, defendants chose to stay in

Wisconsin, where they obtained jobs with plaintiff MaxPower Corporation. Plaintiff MaxPower Corporation set up MaxPower Wisconsin as a separate Wisconsin corporation for the purpose of employing defendants and others. Plaintiffs touted the experience and backgrounds of their new employees in a publication sent to customers and others in the uninterruptible power systems field.

Defendant Hobson was employed as an applications engineer; the other two defendants were employed as "inside salesmen." On a daily basis, defendants dealt with plaintiffs' customers, preparing and providing proposals and quotations. They did not have authority to modify the terms of a customer purchase order contract without consulting the outside salesman responsible for the particular contract as well as MaxPower's president Thomas Ebner or the sales manager Tamra Schow.

In carrying out their responsibilities, defendants learned the identity of plaintiffs' existing customers, the identities of prospective customers, pricing information (including prices of products sold to customers and prices of products purchased from manufacturers), as well as plaintiffs' general marketing and business strategies. Much of this information was not new to defendants; they had known a lot of it before they took the jobs with plaintiff MaxPower Wisconsin either as a result of their work with BestPower (PowerWare's predecessor) or because it was of the type generally known in the industry. Names of customers can be obtained readily through computer searches. Pricing information is often

revealed by resellers seeking to obtain a better deal than they have been offered by a competitor.

Plaintiffs limit access to their facilities and they restrict access to much of their computer information through protective passwords. On occasion, plaintiffs discussed with their employees the importance of preventing competitors from learning plaintiffs' customer information and pricing and marketing strategies, but they had no written or oral policy concerning the confidentiality of such information. Plaintiffs never asked defendants to sign a non-disclosure agreement. Plaintiffs did not always require departing employees to turn in their company-issued laptops or to delete confidential information from the laptops.

Plaintiff MaxPower Wisconsin has one computer server of its own and, with plaintiff MaxPower Corporation, shares access to a network drive known as MaxDrive. Pertinent customer information resides on plaintiff MaxPower Corporation's Mail Order Management system (MOM), which is a database created to track all MaxPower sales and product purchases, and an online system called Salesforce.com.

Plaintiffs provided all defendants with networked laptop computers and provided Kevin Hobson and Brady Wilkens with Blackberries. Defendants had access to the MaxPower Wisconsin server, the MaxDrive and the MOM and Salesforce.com databases. Plaintiffs encouraged all employees, including defendants, to use their password-protected

personal directories on the MaxDrive for their personal data in order to reduce the storage demands on their laptops.

Defendant Hobson was terminated from plaintiff MaxPower Wisconsin on January 2, 2008 and warned not to go to work for a competitor. Hobson returned the office telephone and his Blackberry, as requested. He did not delete any contacts from his email account, any notes from his laptop or anything from his laptop hard drive. Before and during his employment with plaintiff, he had obtained and archived information relating to old and obsolete equipment manufactured and distributed by Powerware and its predecessor company, which he found useful in helping customers who still had the equipment and needed maintenance or supplies. All of the archived material was backed up on the MaxDrive; when Hobson left his employment with plaintiff MaxPower Wisconsin, he made a CD of the archive and took it with him. Hobson had gathered most of the information before beginning work with plaintiff MaxPower Wisconsin.

On Friday, January 18, 2008, defendants Abraham and Wilkens sent emails to Tamra Schow, their manager, to say they were resigning, effective February 1, 2008, and going to work for plaintiffs' competitor, H.M. Cragg. Schow told them to reconsider their decisions and sent them home. Both defendants took their laptops with them, expecting to return to honor their two-week notice to plaintiffs. However, later that day, when both called Schow and told her they were not reconsidering, she fired them, effective immediately.

Schow wrote to defendants Abraham and Wilkens on Monday, January 21, 2008, threatening legal action if they used information obtained during their employment with plaintiff MaxPower Wisconsin. Later that day, both defendants returned their laptops to plaintiffs, after deleting information in their email accounts. The email deletions conformed with company policy on laptop maintenance; other relevant material had been stored to the company's hard drives. Neither man deleted material stored on the MaxDrive. In the past, at least one employee was able to keep the laptop issued to him by plaintiff MaxPower Corporation and was not instructed to delete any information from it, although it included information regarding resellers, his communications with them and pricing information.

Defendant Abraham was served with a summons in this case on March 22, 2008. On April 17, 2008, the magistrate judge issued a discovery order allowing plaintiffs to employ a forensic expert to examine defendants' laptops. The next day, defendant Abraham used a CCleaner to "wipe," that is, remove data from the hard drives on the laptop issued to him by H.M. Cragg, his new employer. His explanation for doing this was that his new laptop was experiencing very long bootup times; he called his former wife's husband who has experience with computers and was told that a CCleaner could wipe a drive clean of excess data, which might improve the bootup times. When plaintiffs' expert examined the laptop, the contents of Drive #2 had been wiped completely and; the contents of Drive #1 were partially wiped. Drive #2 contained no allocated data except for configuration data. Drive

#1 showed trace remnants of certain MaxPower executable files. Defendant testified that he did not use Drive #2, that he did not realize that using the CCleaner would have the effect it did and that he did not think that his computer had any information about plaintiffs or belonging to them. After he used the program, his computer rebooted properly.

Abraham stored all of his price quotes on plaintiffs' MaxDrive. One of plaintiffs' employees went to look for a quote on a particular transaction and was unable to find it on plaintiffs' system. Plaintiffs have no evidence of any document stored on MaxDrive that defendants accessed after they stopped working for plaintiffs.

Plaintiffs' forensic expert found "text strings" on defendant Hobson's new computer that pointed to files such as ChargerTheory.pdf. ("Text strings" seem to be collections of words or symbols that can be found on a computer, even after files have been deleted.) Charger Theory.pdf refers to information about outdated products of the sort collected by defendant Hobson, stored on plaintiffs' servers and duplicated on a compact disc that Hobson uses today to access the information he has accumulated.

According to defendants' forensic expert, a text string could have been created if a "favorite" from a MaxPower computer had been put onto a compact disc as a list of favorites and imported to a new computer before being deleted.

All three defendants now work for H.M. Cragg Company. Defendant Hobson is an applications engineer; the other two defendants are inside salesmen. In their new positions

defendants Abraham and Wilkens are not involved in the solicitation of accounts. Neither deals with vendors or negotiates pricing with resellers. None has been asked for confidential information obtained through their employment with plaintiffs and they have not used any such information. On January 25, 2008, Cragg sent an email to many customers, either its own or ones known to it, announcing the employment of the three defendants.

Defendants live in an area in which business opportunities are limited for people with their skills and experience. Few jobs can match what defendants are earning at Cragg, which provides health benefits. The situation is likely to worsen because two major papermaking companies in the Wisconsin Rapids area have announced plans either to close their Wisconsin plants or cut jobs. If enjoined from working for Cragg, defendant Abraham would either have to take a much lower paying job or move from the area. He is a divorced father, who shares custody of his children. Moving from the area would deprive him of the opportunity to continue his joint custody arrangement.

Defendant Hobson does not want to move from the area in which he lives because he and his wife both have elderly parents who depend on their children for help and support. Hobson is uninsurable after having suffered a stroke a year ago and depends on the insurance coverage he receives as a Cragg employee.

OPINION

American courts tend to be wary of employer-employee arrangements that prevent employees from changing jobs and using their skills and work experience in new employment. E.g., Streiff v. American Family Mutual Ins. Co., 118 Wis. 2d 602, 610-11, 348 N.W.2d 505 (1984) ("Restrictive covenants are prima facie suspect; they must withstand close scrutiny to be considered legally reasonable; they are not construed any further than absolutely necessary, and they are construed in favor of employees."). Plaintiffs do not have non-compete agreements with any of the defendants and they did not extract any promises to keep any of plaintiffs' information confidential.

In the absence of more formal restrictions, plaintiffs are trying to keep defendants from starting over in a competitive business by alleging that they took trade secrets, accessed plaintiffs' computers without authorization, breached a duty of loyalty, interfered intentionally with plaintiff's prospective business advantage, converted confidential and proprietary information and personal property, violated Wis. Stat. § 895.446 by taking property from plaintiffs without consent and with the intent of depriving plaintiffs of it permanently, took possession of electronic data belonging to plaintiffs or destroyed it, in violation of Wis. Stat. § 943.70, violated 18 U.S.C. § 1030 and committed unfair trade practices.

One threshold issue needs to be addressed before taking up the plaintiffs' motions for

a preliminary injunction and for sanctions: the law to be applied to the case. The parties have not discussed the issue. Plaintiffs made a footnote reference to the application of Colorado law but bring most of their claims under Wisconsin law. Both sides cite law from both states. I will apply Wisconsin law, for three reasons. Defendants' acts are alleged to have taken place in Wisconsin; three of the claims are alleged to arise under Wisconsin law; and most important, neither side has identified any critical difference between the laws of the two states.

A. Motion for Preliminary Injunction

To obtain a preliminary injunction, a movant must first prove that his claim has "at least some merit." Digrugilliers v. Consolidated City of Indianapolis, 506 F.3d 612, 618 (7th Cir. 2007) (citing Cavel International, Inc. v. Madigan, 500 F.3d 544, 547 (7th Cir. 2007)). If it does, the inquiry proceeds to the adequacy of a legal remedy and on to the balance of harms. The final factor is the public interest.

1. Chances of success on the merits

Although plaintiffs alleged eight claims for relief against defendants in their complaint, they discussed only four in their brief in support of their motion for preliminary injunction hearing: breach of the duty of loyalty; misappropriation of trade secrets; violation

of 18 U.S.C. § 1030, the Computer Fraud and Abuse Act; and violation of Wis. Stat. § 943.70.

a. Breach of the duty of loyalty

Plaintiffs alleged a violation of the duty of loyalty in their complaint, but did not cite any Wisconsin case holding that this duty continues after an employee has left the employer, unless the employee had been an officer who had a fiduciary duty to the employer. Modern Materials v. Advanced Tooling Specialists, 206 Wis. 2d 435, 446-47, 557 N.W.2d 835 (Ct. App. 1996). Plaintiffs have not alleged that defendants were officers or that they accessed the MaxPower servers improperly while they were still in plaintiffs' employ. In short, they have failed to show any reason for thinking that defendants breached any duty of loyalty that might support a judgment against them as former employees. Given the lack of argument and citations in support of the claim, there is no need to give it any further attention.

b. Violation of Wisconsin's Uniform Trade Secrets Act, § 134.90

To prevail on this claim, plaintiffs would have to show that they have a good chance of succeeding on its merits. However, it is unlikely that they can prove that their customer information, pricing and marketing strategies are trade secrets within the meaning of the

Uniform Trade Secrets Act, Wis. Stat. § 134.90. To do so they would have to show that the information "derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use" *and* that "[t]he information is the subject of efforts to maintain its secrecy that are reasonable under the circumstances." Wis. Stat. § 134.90(1)(c).

Plaintiffs fail to making the necessary showing on two grounds. First, they failed to rebut defendants' evidence that much of the alleged trade secret information is common knowledge in the industry or easily ascertainable, Burbank Grease Services, LLC v. Sokolowksi, 2005 WI App 28, ¶ 18, 278 Wis. 2d 698, 712, 693 N.W.2d 89, 96 (if names, addresses and contact persons of customers are readily ascertainable, they do not qualify as trade secrets) (rev'd on other grounds, 2006 WI 103, 278 Wis. 2d 274, 717 N.W.2d 781). Second, they failed to show that they took reasonable measures to protect the confidentiality of the information. Abbott Laboratories v. Norse Chemical Corp., 33 Wis. 2d 445, 457, 147 N.W.2d 529 (1967) ("The subject matter of a trade secret must be secret . . . . [a] substantial element of secrecy must exist, so that, except by the use of improper means, there would be difficulty in acquiring the information.").

It is not enough simply to restrict access to the facility and require passwords; these are normal business practices in any business. An employer must use additional measures

to protect the confidentiality of information he considers to be a trade secret. E.g., La Calhene, Inc. v. Spolyar, 938 F. Supp. 523, 530 (W.D. Wis. 1996) (finding that plaintiff had proven trade secret nature of its plans for business strategies, marketing, research, development and integration of manufacturing and engineering; plans were seen by only small number of plaintiff's officers (salespeople received only one page of document), plaintiff did not allow visitors to plant except with escorts, plaintiff made confidentiality condition of employment with defendant and other high ranking employees and plaintiff itself was subject to its parent company's confidentiality requirements when licensing plaintiff's products).

Plaintiffs had no confidentiality agreements with their employees; they did not make a point of emphasizing the importance of keeping the customer lists and pricing information confidential; the information was generally available to all employees; and it does not appear that plaintiffs made any efforts in the past to insure that former employees deleted allegedly confidential information from their laptops when they left. Defendants' departures seem to be the first to have elicited concern about any so-called trade secrets.

Moreover, plaintiffs adduced no evidence that since defendants left they have disclosed any of the alleged trade secrets or used the secrets themselves to further their work for H.M. Cragg. They did offer a letter from a customer-reseller who expressed surprise at receiving a notice from Cragg that it had hired defendants, but it is hard to conclude from

this that defendants disclosed their customer lists, given the ease of obtaining the names of customers and prospective customers from public sources. In the absence of any persuasive showing that the information at issue constituted trade secrets or that defendants used the information for their own or their new employer's benefit, I cannot find that plaintiffs have any likelihood of succeeding on the merits of this claim. Even if they did, they could not meet the other prerequisites for a preliminary injunction. See § B, C and D, infra.

c. Violation of Computer Fraud and Abuse Act, 18 U.S.C. § 1030

18 U.S.C. § 1030 makes it a crime to access a protected computer without authorization and with intent to defraud if the computer owner suffers loss or damage of more than $5000. In their briefs and opening statement, plaintiffs alleged that defendants had intentionally accessed plaintiffs' computers to obtain confidential and proprietary information belonging to plaintiffs, that they intentionally destroyed electronic data by deleting it from plaintiffs' servers and that they changed the passwords to plaintiffs' servers, but continued to access the servers, and that they did not turn over the correct passwords to plaintiffs. Plaintiffs alleged that defendants are using confidential information and trade secrets and that plaintiffs have suffered damages in excess of $5000.

At the hearing however, plaintiffs produced no evidence that any passwords had been changed or that defendants had deleted any electronic data from plaintiffs' servers. They

presented only weak evidence that defendants had accessed plaintiffs' computers to obtain information they had not possessed as employees. On the other hand, defendants adduced evidence that their only deletions were from their laptops and that those deletions conformed to company policy for clearing unnecessary data from laptops.

The evidence that plaintiffs' forensic expert identified was ambiguous. It was not possible to tell whether it indicated improper access or represented the residue of information defendants were entitled to possess while employed. In several instances, it appeared that "text strings" identified by the expert were innocuous. For example, the expert found "text strings" pointing to files such as ChargerTheory.pdf. Charger Theory.pdf refers to information about outdated products of the sort collected by defendant Hobson, stored on plaintiffs' servers and duplicated on a CD that Hobson continues to use. This does not suggest improper access.

Some of the data the expert found seems to have come from material that was on defendants' laptops or personal digital assistants while they were employed and could have been transferred to defendants' new laptops when they synchronized their personal digital assistants, transferred their personal data from the laptops plaintiffs had provided them to CDs for transfer to their Cragg laptops or when their cell phone information was transferred to new phones.

The most damning evidence is Abraham's use of a drive cleaner on his laptop after

he was served with the summons in this case and before the laptop could be examined by plaintiffs. Neither side's computer expert was persuaded that use of a CCleaner would have been the first resort for slow rebooting. Plaintiffs' expert was sure that resorting to such a method was evidence of a deliberate effort to destroy incriminating evidence. I am not persuaded that the evidence is so clear. The idea of wiping out unnecessary data to improve computer performance does not seem particularly implausible. It is possible however that plaintiffs would be able to prove at trial that defendant Abraham's action is evidence of illegal access to company servers after he left plaintiffs' employ. If so, they may be entitled to money damages under § 1030 and possibly under Wis. Stat. § 943.70 as well. Any claim for injunctive relief would depend on plaintiffs' ability to show that defendants are continuing to access plaintiffs' computers or use the information they obtained improperly.

d. Violation of Wisconsin's Computer Crimes Act, Wis. Stat. § 943.70

In pertinent part, § 943.70 makes criminal modifying, destroying, copying or taking possession of data, computer programs or supporting documentation, accessing computer programs or supporting documentation or disclosing restricted access codes willfully, knowingly and without authorization. As I noted above, there is at least a chance that plaintiffs will be able to prove that one or more defendants did any of the acts prohibited by this statute, in which case plaintiffs will be entitled to money damages and, as noted above,

injunctive relief if they can prove continuing harm. This does not mean, however, that plaintiffs are entitled to *preliminary* injunctive relief.

2. Irreparable injury and adequacy of remedy at law

Even if the evidence that plaintiffs produced had been more incriminating and therefore supportive of a finding that they would be likely to prevail ultimately on any of their claims against defendants, plaintiffs would not be entitled to an injunction. A showing of likelihood of success is only one of the factors necessary to obtain preliminary injunctive relief. A second one is that the movant has incurred an irreparable injury for which it has no adequate remedy at law. In fact, plaintiffs' president, Thomas Ebner, agreed that the damage done to plaintiffs by the alleged improper acquisition of confidential information could be quantified, although he believes it would be difficult.

This point is even stronger with respect to plaintiffs' claims under the state and federal computer crimes statutes. If plaintiffs are able to prove violations of those statutes, their remedy is limited to monetary damages unless they can prove ongoing acts causing harm to their computers or to their business interests.

3. The balance of harms

On this factor, the equities lie with defendants. If plaintiffs win the injunctive relief

they are seeking, defendants would be barred from continuing to work for H.M. Cragg Company. As they testified at the hearing, the economic conditions in their areas are not good; few jobs pay what defendants are earning at H.M.Cragg. Two of the major employers have announced plans either to close their Wisconsin papermaking plants or cut jobs. If defendants were forced to move, it would be particularly hard on defendant Abraham, who has joint custody of his children, and on defendant Hobson, whose parents and in-laws need his help. In addition, it might mean that Hobson would be left without health insurance if he is forced to take a job that does not have a group health policy, because he is uninsurable as an individual.

If no injunction issues and plaintiffs are correct about defendants' improper use of confidential materials, plaintiffs may lose some sales they would otherwise have made. But any such losses can be compensated by money. Forcing defendants to move or to take large pay cuts to obtain jobs that do not provide group health insurance would be devastating to them. The balance of harms is not a close question.

4. The public interest

The last factor is a wash. The public has an interest in preventing departing employees from taking property of value from their employers and it has an interest in protecting employees' rights to leave one employer for another. In this case, neither interest

is so much more important than the other that it would carry the day.

5. Summary

In summary, I conclude that plaintiffs have not established that they meet the factors necessary for obtaining a preliminary injunction. The remaining question is whether plaintiffs are entitled to sanctions for any actions they took to destroy evidence.

B. Motion for Sanctions

As the discussion of plaintiffs' motion for a preliminary injunction suggests, plaintiffs have not made their case for the application of sanctions at this time. The motion will be denied, but plaintiffs are free to reopen the subject if they obtain additional evidence through discovery that supports their allegations that defendants deleted data from plaintiffs' servers, accessed those servers improperly or took any act in violation of plaintiffs' rights, including their right to discovery materials.

ORDER

IT IS ORDERED that the motions for preliminary injunction and for sanctions filed

by plaintiffs MaxPower Corporation and MaxPower Wisconsin Corporation are DENIED.

Entered this 29th day of April, 2008.

BY THE COURT:
/s/
BARBARA B. CRABB
District Judge