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

ABRASIC 90 INC., d/b/a CGW CAMEL GRINDING WHEELS, USA, Plaintiff, v. WELDCOTE METALS, INC., JOSEPH O'MERA, and COLLEEN CERVENCIK, Defendants.	)	No. 18 C 05376 Judge John J. Tharp, Jr.

MEMORANDUM OPINION

After some 18 years as President of Abrasic 90, Inc., a manufacturer of grinding and sanding discs doing business as Camel Grinding Wheels, U.S.A. ("CGW"), defendant Joe O'Mera left to set up a competing abrasives business for Weldcote Metals, Inc. ("Weldcote"). He took with him some CGW files containing, the company contends, trade secret information about its pricing, customers, and suppliers. CGW has moved for a preliminary injunction against Weldcote, O'Mera, and Colleen Cervencik, another CGW employee who left to work for Weldcote, seeking to bar the defendants from operating in the abrasives industry and from using its trade secrets. But CGW has failed to show that a preliminary injunction is warranted. Largely because it did not protect its supposedly secret information, CGW has not shown that it is likely to succeed on the merits of its claims under any legal theory that could serve as the basis for a preliminary injunction. The injunction it seeks, moreover, is disproportionate to any harm it is likely to suffer and disserves the public's interest in fostering competitive markets. Accordingly, the motion for preliminary injunction, ECF No. 44, is denied.

I. BACKGROUND

CGW is a company based in Niles, Illinois that manufactures and sells over 5,000 abrasive products. CGW purchases materials from about 45 suppliers and sells its finished abrasive products through its internal sales force and a cadre of independent sales agents to roughly 4,000 distributors. About half of CGW's distributors receive prices from CGW that are discounted against CGW's "Mix & Match" catalogue, which is CGW's product-by-product starting point for pricing that is distributed to thousands of recipients. A software program tracks CGW's many thousands of pieces of transactional data and exports that data into various Excel spreadsheets. CGW stored its business and financial information—which included these Excel spreadsheets, the Mix & Match catalogue, sales reports containing information such as CGW's profitability by customer and by item, and other information such as shipping packaging weights—on CGW's shared drive (collectively, the "information at issue"). CGW's employees could access and work on the information on the shared drive as desired, and CGW sent some of the information, such as the sales reports, to its independent sales representatives.

From 2000 to January 29, 2018, Joseph O'Mera was CGW's President. O'Mera was also a director of CGW beginning at least as early as 2005.[1] Many of O'Mera's customers from his previous employer followed him to CGW. At CGW, O'Mera developed and oversaw various aspects of CGW's operations, identified at least 40 of CGW's 45 suppliers, and played the primary role in negotiating costs with suppliers. O'Mera also set CGW's prices for its entire product line

[1] During the period relevant to this law suit, CGW was owned by Gamal, an Israeli corporation. CGW's only two board members based in the United States were O'Mera, who served on CGW's board of directors from 2005 until 2018, and Colleen Cervencik, who served on the board from 2008 until 2015. CGW's other board members were based in Israel.

and approved all pricing discounts. During O'Mera's tenure, CGW's annual sales increased from $2.8 million to $33 million.

O'Mera had an employment agreement with CGW from 2002 through 2007[2] that included a nine-month non-compete provision and confidentiality requirements. The employment agreement required O'Mera to keep CGW information confidential during the term of his employment and to return the exclusive property of CGW when the agreement or his term of employment ended. Although CGW's parent company, Gamal, presented O'Mera with another employment agreement in 2013, that agreement was never executed because the parties could not agree on a long-term compensation plan.

So far as the record reflects, no other CGW officer or employee has ever been subject to a non-compete or confidentiality provision in an employment contract. CGW's employee handbook, which O'Mera approved in 2010, provides that employees may not "reveal or discuss information about CGW, its customers or its employees when outside of the company," Joint Ex., Hr'g on Mot. for Prelim. Inj. ("Joint Ex.") 1, at 3, but it does not impose any obligations on employees after their employment at CGW ends. CGW's independent sales representatives signed agreements informing them that "[c]ustomer information, pricing, strategies and sales analysis records" were considered confidential and requiring them to return CGW property when their relationships with CGW ended, Pl.'s Prelim. Inj. Ex. ("Pl.'s Ex.") 45 ¶¶ 11, 14, but nothing in the record suggests that others with access to the information at issue—such as CGW's own employees—entered into similar agreements or were likewise instructed regarding the confidentiality of certain categories of information. CGW also did not generally require others who had access to some of the

[2] The term of the agreement may have been extended to 2012, but there is no evidence that the agreement extended past 2012.

information at issue, such as CGW's suppliers and distributors, to sign confidentiality or non-disclosure agreements.

Defendant Colleen Cervencik began working at CGW in 1998. She served as CGW's IT Manager from 2012 until approximately April 2018 when she was effectively demoted to a position as a "Special Projects Manager." During her tenure as the IT Manager, Cervencik maintained the shared drive where the information at issue was stored. She generally granted "office personnel" access to the shared drive if they asked for it (there is no evidence that any employee who sought access to the shared drive was denied such access), and about 39 of 108 CGW employees were given access. If an employee was given access to the shared drive, no inquiry was made as to whether the employee needed access to any particular subset of the information at issue, and there were no restrictions as to which folders within the shared drive that the employee could access; that employee had access to the entire shared drive. Nor were any restrictions imposed on what could be saved to the shared drive. None of the folders or files were password protected or encrypted. There were also no restrictions placed on the employee's ability to download the files, save them to his or her hard drive or an external storage device, print them, or email them. Until April 2018, all employees were instructed to use the same password so that another employee could log in using the other employee's login credentials if necessary. CGW only labeled certain research and development files as "proprietary information," *see, e.g.*, Defs.' Ex., Hr'g on Mot. for Prelim. Inj. ("Defs.' Ex.") 18; none of the sales and financial information at issue in this case was marked confidential or proprietary. It is undisputed that the shared drive included information that even CGW acknowledges was distributed publicly, such as the widely available Mix & Match pricing catalogue and shipping packaging weights.

In February 2017, CGW hired Ana Maria Gheciu, who holds a degree from DeVry in network and telecommunications management, to work for Cervencik. Around April 2018, Gheciu replaced Cervencik as IT Manager. Gheciu suggested that CGW implement additional security measures, including limiting employees' access to certain files within the shared drive and implementing an "Acceptable Device Use Policy" requiring that employees remove company data from their personal devices at the time of their separation. *See, e.g.*, Joint Ex. 3. CGW did not implement those measures. Indeed, notwithstanding her recommendation to limit the dissemination of company materials via personal devices, Gheciu sent some of the information at issue to O'Mera's personal email account.

In 2017, O'Mera began engaging in business talks with Zika Group Ltd. ("Zika") about Zika's plans to start an abrasives business that would compete with CGW (among others). Those talks ultimately culminated in plans for Zika to acquire and expand the business of Weldcote, historically a manufacturer of welding products, to sell abrasives and safety products to welders. O'Mera accepted Zika's offer to work as CEO of Weldcote on January 28, 2018. But while O'Mera was still President of CGW, in April 2017, O'Mera sent an email to a Zika executive informing the Zika executive that O'Mera had obtained from VSM, a CGW supplier, a commitment to "work with [him] under the same exact pricing terms on their entire product line." Pl.'s Ex. 44, at 1. Other emails in the same thread suggest that O'Mera was engaging in similar discussions with CGW's major China vendor, Ningbo. O'Mera told Zika that O'Mera generally had "all the suppliers lined up." *Id.* at 5. O'Mera also wrote in the thread that he had "spent an enormous amount of time on new product testing," and that it would be best if he left CGW before CGW could benefit from his work. *Id.* O'Mera denies ever having conducted due diligence for Zika with respect to its acquisition of Weldcote, but he at least provided advice about the focus of some of Zika's due

diligence work and met with Zika in North Carolina, where the Weldcote facility was then located, to discuss matters related to that potential acquisition. *See* Pl.'s Ex. 44; Tr. of Proceedings, Prelim. Inj. Hr'g, Oct. 19 & 22, 2018 ("Hr'g Tr.") 47:19–48:25, 160:21-23.

O'Mera resigned from CGW on the afternoon of January 29, 2018, to join Weldcote as its President. Shortly before resigning, O'Mera gathered his CGW laptop and other equipment from his home and turned it in to CGW. O'Mera kept, however, a flash drive storage device containing both personal files and some of the information at issue. Included among the files O'Mera kept was CGW's "All Items File," which contained a comprehensive summary of CGW's transactional information, including sales data, prices, and costs for its products and the identities of suppliers and distributors. When O'Mera left CGW, neither Cervencik nor Gheciu nor anyone else at CGW asked or instructed him to delete company information that had been emailed to his personal email address or that he had otherwise copied or stored on or in personal devices and accounts.

Jay Hickman worked in sales at CGW from 2005 until February 20, 2018. When Hickman joined CGW, he brought with him the business of 30 to 50 of the more than 200 distributors with whom he had previously worked. Fritz Klug worked in sales at CGW from 2000 until February 20, 2018. When Klug joined CGW, approximately 25% of his prior customers followed him to CGW. Both Hickman and Klug joined O'Mera at Weldcote a few days after resigning from CGW. When Klug resigned from CGW, he told a CGW human resources employee that he was dropping "everything" off, Hr'g Tr. 227:22-23, but he retained a memory stick that contained some of the information at issue.

A few months later, O'Mera offered Cervencik a position at Weldcote as its Purchasing manager. On June 16, 2018, Cervencik accepted O'Mera's offer. Over the following week, O'Mera and Hickman asked Cervencik to obtain some of the information at issue from the CGW

shared drive. O'Mera asked Cervencik to supply CGW data regarding "VSM roll ordering," information regarding a price increase given to CGW by Inter Abrasives, and data regarding CGW's consumption of flap disc rolls. Pl.'s Ex. 16. Hickman also asked Cervencik to obtain some of the information at issue, explaining that he could use her help "with sales from western sales areas that I cover now, and had not for the last 5 years." Pl.'s Ex. 17. Cervencik obtained the information O'Mera and Hickman requested before she resigned from CGW on June 22. O'Mera, however, placed the order for which the VSM roll ordering data he requested from Cervencik was relevant before Cervencik had an opportunity to provide him with that data. Cervencik also took with her when she resigned from CGW three thumb drives containing information at issue because she believed it might be helpful to her at Weldcote. When O'Mera, Klug, and Cervencik separated from CGW, no one asked them whether they had any confidential CGW information in their possession or demanded that they return it.

Within a few weeks after Cervencik resigned, Gheciu discovered that Cervencik had deleted her working folder from the CGW network and that O'Mera had texted Cervencik to obtain CGW information. As a result, CGW hired QDiscovery LLC, d/b/a Forensicon, to examine the integrity of its network. The damage assessment cost CGW more than $20,000. First Am. Compl. for Inj. and Other Relief ("Am. Compl.") ¶ 190, ECF No. 41.

After joining Weldcote, O'Mera, Klug, and Hickman discussed the CGW information at issue, much of which had been uploaded to Weldcote computers. They used the data as a general reference point and a benchmark when determining some of Weldcote's initial needs. Some of the information at issue was used to confirm that CGW suppliers were charging Weldcote the same prices they were charging CGW. Weldcote employees have also sent some of the CGW information at issue to Weldcote's sales reps and instructed them to target key CGW distributors.

Cervencik claims that she has not used any of the information at issue beyond opening one of the spreadsheets before quickly closing it. O'Mera has obtained at least some of the information at issue, including CGW's prices, from distributors, and other information such as the identity of suppliers can be readily ascertained from publicly available sources. Although suppliers generally do not disclose to a manufacturer the exact prices that they charge other manufacturers, suppliers generally provide information about which products are the best-sellers and the level at which those products should be priced.

In August 2018, this Court entered a temporary restraining order (the "TRO") preventing the defendants from using the information they obtained from CGW. ECF No. 12. By agreement, that restriction has remained in effect pending the Court's ruling on CGW's preliminary injunction motion. This Court also ordered Weldcote to produce to Forensicon the imaging of the defendants' devices onto which the information at issue had been saved, ECF No. 28, before holding a preliminary injunction hearing on October 19 and 22, 2018. In addition to various emails and text messages, CGW introduced at the hearing the results of the forensic evaluation. According to the forensic analysis, Weldcote accessed at least 136 of over 3,100 files on Weldcote devices that contained "CGW" in the file name or file path, were authored by CGW employees, or both. The defendants appear to have also saved some of the information at issue on a "cloud" server where it may be difficult to detect further duplication or transmission of files.

As of the preliminary injunction hearing, Weldcote was working with approximately six abrasives suppliers and planned to sell about 900 abrasives products once its abrasives business is operating. Weldcote had already purchased approximately one-year's worth of inventory from suppliers, invested over $3 million, and had incurred $2 million in debt in connection with its abrasive business. CGW concedes that as of November 30, 2018, it cannot point to lost profits as

a result of the defendants' conduct, but nevertheless maintains that a preliminary injunction is necessary to protect it from the future irreparable harm it will suffer once Weldcote begins selling abrasive products. CGW's preliminary injunction motion seeks to bar Weldcote from entering the abrasives business, from doing business with CGW's suppliers or distributors, and from using the information at issue. The defendants request that the Court deny CGW's motion for a preliminary injunction or, in the alternative, enter a preliminary injunction of a narrower scope.

II. DISCUSSION

The Seventh Circuit recently has provided a definitive statement of the standard that governs requests for preliminary injunctions:

> An equitable, interlocutory form of relief, a preliminary injunction is an exercise of a very far-reaching power, never to be indulged in except in a case clearly demanding it. It is never awarded as a matter of right. To determine whether a situation warrants such a remedy, a district court engages in an analysis that proceeds in two distinct phases: a threshold phase and a balancing phase.
>
> To survive the threshold phase, a party seeking a preliminary injunction must satisfy three requirements. It must show that: (1) absent a preliminary injunction, it will suffer irreparable harm in the interim period prior to final resolution of its claims; (2) traditional legal remedies would be inadequate; and (3) its claim has some likelihood of succeeding on the merits.
>
> If the moving party satisfies each of these requirements, the court proceeds to the balancing phase of the analysis. In the balancing phase, the court weighs the irreparable harm that the moving party would endure without the protection of the preliminary injunction against any irreparable harm the nonmoving party would suffer if the court were to grant the requested relief. In so doing, the court employs a sliding scale approach: the more likely the plaintiff is to win, the less heavily need the balance of harms weigh in his favor; the less likely he is to win, the more need it weigh in his favor. Where appropriate, this balancing process should also encompass any effects that granting or denying the preliminary injunction would have on nonparties (something courts have termed the public interest).

Valencia v. City of Springfield, Illinois, 883 F.3d 959, 965–66 (7th Cir. 2018) (internal quotations, citations, and punctuation omitted).

Applying this standard, CGW's request for preliminary injunctive relief falls short. As to its principal claim—that the defendants misappropriated its trade secrets—CGW has shown neither an adequate likelihood of success on the merits nor that it would suffer irreparable harm without injunctive relief. To the extent that CGW's state law theories rely on similar allegations about the misappropriation of confidential information, they too are unlikely to succeed as they are preempted by the relevant trade secret statutes. And to the extent that any claims are not preempted, those claims fail because CGW has not shown (or even argued) that non-preempted conduct continues to cause irreparable harm.

A. DTSA and ITSA

CGW's lead claim is that the defendants are liable for their misappropriation of trade secrets under the Defend Trade Secrets Act ("DTSA"), 18 U.S.C. § 1831 *et seq.* and the Illinois Trade Secrets Act ("ITSA"), 765 ILCS 1065/1 *et seq.* CGW has not demonstrated the propriety of granting preliminary injunctive relief based on this claim, however, because it has not shown a likelihood of success on the merits or that the alleged misappropriation of trade secrets is causing irreparable harm.

1. Likelihood of Success on the Merits

"A party moving for preliminary injunctive relief need not demonstrate a likelihood of absolute success on the merits. Instead, he must only show that his chances to succeed on his claims are better than negligible." *Valencia*, 883 F.3d at 966 (internal quotations and citation omitted). Despite this low bar, the Court concludes that CGW is unlikely to succeed on a theory

that the defendants misappropriated CGW's trade secrets in violation of the DTSA or ITSA.[3] Although some of the information at issue may have been ***protectable*** as a trade secret, CGW did not adequately ***protect*** it for it to qualify as a trade secret.

To prevail on a misappropriation of trade secrets claim, CGW must show that the information taken by the defendants was "(i) secret (that is, not generally known in the industry), (ii) misappropriated (that is, stolen from it rather than developed independently or obtained from a third source), and (iii) used in the defendants' business." *Composite Marine Propellers, Inc. v. Ven Der Woude*, 962 F.2d 1263, 1265–66 (7th Cir. 1992). It cannot be reasonably disputed that the defendants copied information from CGW and used it, at least in some limited fashion, in setting up Weldcote's business. The relevant question is whether the CGW information at issue was truly secret.

Although courts have identified many factors that can be relevant to an assessment of whether information qualifies as a trade secret, there are two basic elements to the analysis. For the information at issue to be considered a trade secret, it must have been "sufficiently secret to impart economic value because of its relative secrecy" and CGW must have made "reasonable efforts to maintain the secrecy of the information." *Learning Curve Toys, Inc. v. PlayWood Toys, Inc.*, 342 F.3d 714, 722 (7th Cir. 2003); *see also* 18 U.S.C. § 1839(3) (to qualify as trade secret, owner must have "taken reasonable measures to keep such information secret" and the information must "derive[] independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain

[3] The Court analyzes the DTSA and ITSA together "because the pertinent definitions of the two acts overlap." *Molon Motor and Coil Corp. v. Nidec Motor Corp.*, 2017 WL 1954531, at *2 (N.D. Ill. May 11, 2017).

economic value from the disclosure or use of the information"); 765 ILCS § 1065/2(d)(2) (trade secret must be "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 "the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality"). Information does not qualify as a trade secret if it is "generally known or understood within an industry even if not to the public at large." *Pope v. Alberto-Culver Co.*, 694 N.E.2d 615, 617 (Ill. App. Ct. 1998). And the owner must have taken "'affirmative measures' to prevent others from using [the] information" for it to qualify as a trade secret. *Jackson v. Hammer*, 653 N.E.2d 809, 816 (Ill. App. Ct. 1995).

a) Nature of the Information at Issue

Here, much (though not all) of the information at issue is "publicly available" in the sense that parties other than CGW have access to that information, but the compilation of those pieces of information may nevertheless be protectable as a trade secret. Business and financial information, including lists of actual or potential customers or suppliers, can qualify as a trade secret. *See* 18 U.S.C. § 1839(3) ("trade secret" defined to include "financial," "business," and "economic" information); *see also* 765 ILCS § 1065/2(d) ("trade secret" defined to include "financial data" and "list[s] of actual or potential customers or suppliers"). Moreover, a compilation of data, even if the component parts are in the public domain, may be protectable as a trade secret if it would require substantial time, effort, and expense to recreate the compilation. *Computer Care v. Serv. Systems Enterprises, Inc.*, 982 F.2d 1063, 1074 (7th Cir. 1992) (endorsing principle that "[a] trade secret can exist in a combination of characteristics and components, each of which, by itself, is in the public domain, but the unified process design and operation of which in unique combination affords a competitive advantage and is a protectable trade secret.") (citation

omitted); *see also SFK USA, Inc. v. Bjerkness*, 636 F. Supp. 2d 696, 714 (N.D. Ill. 2009) (As to the requirement "that the materials not be widely known in the industry, . . . even if they are just compilations of otherwise readily known facts, the compilations themselves are not available to competitors and presumably have some value by gathering the materials into one place."); *Master Tech Products, Inc. v. Prism Enterprises, Inc.*, No. 00 C 4599, 2002 WL 475192, *5 (N.D. Ill. 2002) ("Courts often look to how easily information can be duplicated without involving substantial time, effort, or expense" when "ascertaining whether information is a trade secret."); 18 U.S.C. § 1839(3) (including "compilations" in definition of trade secret); 765 ILCS 1065/2(d) (same).

At least some of the information at issue satisfies these criteria. Undoubtedly the best example is CGW's "All Items File." That voluminous file—which O'Mera acknowledged he took with him when he left CGW—included both public and non-public information on the pricing and sales of all of CGW's products, its suppliers and costs, and financial metrics derived from this data such as its profit margins on each product. Much of the information included in the file—in particular, any information that could also be found in CGW's publicly available Mix & Match pricing catalogue—was widely known throughout the industry and to CGW's competitors, and individual suppliers and distributors knew the details of their own transactions with CGW. But there is no evidence that suppliers, distributors, or others in the industry had the data as it was compiled in the All Items File or the financial information derived from its compilation. Compiling that data required substantial time, effort, and expense. O'Mera testified that it took him 40 hours every 18–36 months to compile the All Items File, and the spreadsheets contain many thousands of data points. Even though the information in the All Items File was known to O'Mera and others at CGW, it nevertheless had at least some value to the defendants—beyond the information the

defendants already possessed in their heads and the relationships they developed during their many years in the industry—because the information was so detailed that it was virtually impossible to remember all of it.

The manner in which the information shared with suppliers and distributors was compiled could, in theory, transform the bits of information that on their own are not trade secrets into trade secrets in their compiled format. Accordingly, the Court has no difficulty concluding that some of the CGW information at issue was protectable as a trade secret. The problem for CGW, however, is that it did virtually nothing to protect that information to preserve its status as a trade secret.

b) Secrecy of the Information at Issue

CGW took almost no measures to safeguard the information that it now maintains was invaluable to its competitors. The company's almost total failure to adopt even fundamental and routine safeguards for the information at issue belies its claim that the information has economic value to its competitors and makes it quite unlikely that CGW will ultimately prevail on its trade secret claim. *See Fail-Safe, LLC v. A.O. Smith Corp.*, 674 F.3d 889, 893 (7th Cir. 2012) (holding that plaintiff "failed to take reasonable protective measures for its claimed trade secret under the circumstances, and thus cannot claim trade secret protection").

CGW's data security was so lacking that it is difficult to identify the most significant shortcoming, but the company's failure to require those with access to its supposed trade secrets to enter into non-disclosure and confidentiality agreements has to be counted among the most fundamental omissions by the company. Failure to enter into nondisclosure or confidentiality agreements often dooms trade secret claims. *See, e.g.*, *Arjo, Inc. v. Handicare USA, Inc.*, No. 18 C 2554, 2018 WL 5298527, at *4 (N.D. Ill. Oct. 25, 2018) ("Pricing information shared freely with customers without confidentiality requirements is insufficiently secret to garner protection.");

Dryco, LLC v. ABM Industries, Inc., No. 07 CV 0069, 2009 WL 3401168, at *6 (N.D. Ill. Oct. 16, 2009) (concluding that plaintiff failed to protect alleged trade secrets because plaintiff did not require confidentiality agreements or label information confidential); *Conxall Corp. v. Iconn Sys., LLC*, 61 N.E.3d 1081, 1093 (Ill. App. Ct. 2016) (holding that where plaintiff could not prove it had a confidentiality agreement, "its trade secret claim . . . suffered a total failure of proof as to a critical element, namely that the designs were a trade secret"); *Liebert Corp. v. Mazur*, 827 N.E.2d 909, 923–24 (Ill. App. Ct. 2005) (affirming finding of no trade secrets where plaintiff did not, among other things, require employees to sign confidentiality agreements).[4]

The failure to use confidentiality agreements is symptomatic of the non-existence of any CGW policy concerning the confidentiality of its business information. So far as the record reflects, there was no policy at CGW regarding confidentiality beyond a vague, generalized admonition about not discussing CGW business outside of work. That admonition did not define, delineate, or specify which information was considered confidential. *See Gillis Associated Indus., Inc. v. Cari-All, Inc.*, 564 N.E.2d 881, 885–86 (Ill. App. Ct. 1990) (noting that plaintiff's failure to specify which information it deemed confidential was inadequate to protect subset of information). The confidentiality language in the employee handbook stating that employees are "not to reveal or discuss information about CGW, its customers or its employees when outside of the company" is too broad and vague to confer meaningful protection over the information at issue. Joint Ex. 1, at 3. Not every shred of CGW information is a confidential trade secret; an employee would not

[4] Of course, even if CGW had used non-disclosure or confidentiality agreements, "such an agreement, without more, is not enough." *Opus Fund Servs. (USA) LLC v. Theorem Fund Servs. LLC*, 17 C 923, 2018 WL 1156246, at *3 (N.D. Ill. Mar. 5, 2018); *see also Arcor, Inc. v. Haas*, 842 N.E.2d 265, 271 (Ill. App. Ct. 2005) (holding that the "limited security measure" of a confidentiality agreement was not sufficient for trade secret protection).

be said to have violated the employee handbook or revealed a trade secret for having had a conversation with his wife about how his work day at CGW went, a discussion that would inevitably include "information about CGW."

In the absence of an articulated and developed confidentiality policy, it is not surprising to find that CGW did nothing to train or instruct employees as to their obligation to keep certain categories of information confidential. *See Jackson*, 653 N.E.2d at 817 (denying trade secret status where "record contain[ed] no evidence that plaintiff took steps to explain the secrecy or confidentiality of the lists to his employees"); *see also Gillis*, 564 N.E.2d at 192 (concluding that information did not qualify as trade secret based, in part, on plaintiff's failure to conduct "entrance and exit interviews imparting the importance of confidentiality").[5] Those employed by or doing business with CGW who had access to the information at issue in its compiled or uncompiled format were not required to agree not to disclose it. CGW did not have exclusive relationships with its suppliers or distributors, yet, according to the testimony of multiple witnesses, CGW's suppliers and distributors were not generally required to keep the information confidential or enter non-disclosure agreements.[6] Nor did CGW insist that its own employees with access to the information at issue sign non-disclosure agreements or otherwise agree not to disclose it.

---

[5] The possible exception to this condition is CGW's efforts (themselves fairly minimal) to protect the confidentiality of its research and development work. None of the information at issue in this case, however, involves research and development materials. And the fact that CGW's took some steps to protect a particular category of information bolsters the inference that it was not concerned about the confidentiality of other information as to which it took virtually no steps to protect.

[6] CGW has not disputed this claim. *See, e.g.*, Pl.'s Resp. 3 (mentioning but not disputing defendants' contention that suppliers and distributors could share CGW's information with competitors); *see also Dryco, LLC v. ABM Indus., Inc.*, No. 07 CV 0069, 2009 WL 3401168, at *6 (N.D. Ill. Oct. 16, 2009) (holding that information was not trade secret where plaintiffs did "not dispute [defendant's] assertions that [p]laintiffs required no confidentiality agreements" and did not mark documents confidential).

O'Mera's employment agreement required that he return CGW documents that he had in his possession upon the termination of the agreement or his employment, but that agreement was only in effect through 2012 at the latest and then was not renewed in 2013. O'Mera's agreement also did not delineate which CGW information was subject to heightened confidentiality protections. The company's contracts with independent sales representatives instructed them that certain information was considered confidential and required that they return CGW property when their relationships with CGW ended, but those agreements governed only independent sales representatives who were not a part of CGW's internal sales team (*e.g.*, not Klug or Hickman), which is only a subset of the dozens of people who had access to the information at issue. And there is no evidence of record that CGW took any steps to ensure that such information was actually returned to the company when those relationships ended.

CGW seems to have employed a similar policy of benign neglect when employees left the company. Although employees were instructed to return CGW property when they separated from CGW, they were not asked whether they possessed any of the information at issue or instructed to return or delete such information. Requiring that departing employees or contractors return company property when their relationship with the company ends is a routine, normal business practice, but precautions must go "beyond normal business practices" for the information to qualify for trade secret protection. *Weather Shield Mfg., Inc. v. Drost*, 17 C 294, 2018 WL 3824150, at *3 (W.D. Wis. Aug. 10, 2018) (internal quotation marks and citation omitted). Indeed, CGW's requests that its employees return company property but not the information at issue highlights that CGW believed its equipment was valuable but did not have the same view of the value of the information at issue. When O'Mera, Cervencik, and Klug separated from CGW, so far as the record reflects, no one asked them what information they possessed, admonished them

about the confidentiality of certain information, or demanded that they return any specific information. *See Gillis*, 564 N.E.2d at 192 (concluding that information did not qualify as trade secret based, in part, on plaintiff's failure to conduct "exit interviews imparting the importance of confidentiality"). Gheciu and Martinez were aware that O'Mera had some of the information at issue on his personal devices; in fact, Gheciu emailed some of the information at issue to O'Mera's personal email address. But neither Gheciu nor anyone else asked O'Mera to delete such emails or the information contained therein when he left CGW. *See CMBB LLC v. Lockwood Mfg., Inc.*, 628 F. Supp. 2d 881, 885 (N.D. Ill. 2009) (The company's "failure to *ensure* that [defendant]'s laptop was stripped of [allegedly protected Information] when she left the company goes to show that it did not treat such Information as confidential or a trade secret.") (emphasis in original).

Apart from the absence of non-disclosure and confidentiality requirements to safeguard the information at issue, Cervencik was put in charge of maintaining the security of CGW's data and information, but she had no training in data security (or virtually any other area of IT management) and was ill-equipped to identify, much less champion, sound data security practices. Neither side presented any expert testimony on the subject (understandable in light of the expedited proceedings), but no expert is needed to know that the practices CGW followed during Cervencik's tenure as IT manager were grossly inadequate to prevent unauthorized access and use of the company's purportedly valuable proprietary information and completely inconsistent with the company's claim that the information at issue includes trade secrets.

Cervencik granted access to the shared drive where the information at issue was located to 39 of CGW's 108 employees. "Restricting access to sensitive information by assigning employees passwords on a need-to-know basis is a step in the right direction" to obtain trade secret protection. *Liebert*, 827 N.E.2d at 923; *see also Segerdahl Corp. v. Ferruzza*, No. 17-CV-3015, 2019 WL

77426, at *3 (N.D. Ill. Jan. 2, 2019) ("disclosing the information on a need to know basis" constitutes part of reasonable security measures to protect trade secret information). But when Cervencik decided whether to grant someone access to the shared drive, so far as the record reflects, she did not make any meaningful inquiry into whether the person needed access to the information. In fact, Cervencik appears to have granted access to individuals when they requested it if they fell into the broad category of "office personnel," Hr'g Tr. 184:21–185:7, and there is no evidence that she ever denied anyone access to the shared drive who asked for it.

Consistent with this laissez-faire approach to data security, Cervencik assigned the same password to many CGW employees to facilitate their access to the shared drive, files were not encrypted, and there were no restrictions on employees' ability to access, save, copy, print, or email the information at issue. *See Arcor, Inc. v. Haas*, 842 N.E.2d 265, 271 (Ill. App. Ct. 2005) (denying trade secret protection and distinguishing from another case where adequate protections were used such as "limiting computer access through the use of passwords, allowing only managers the ability to print [allegedly protected] files, limiting internet and e-mail availability of the information, and keeping physical copies of the information in a file cabinet in an office in which permission was necessary to access the cabinet"); *see also Fleetwood Packaging v. Hein*, 14 C 9670, 2014 WL 7146439, at *4 (N.D. Ill. Dec. 15, 2014) ("Customer lists can constitute trade secrets only where reasonable steps to preserve secrecy have been taken, such as encrypting the lists or requiring review in only restricted-access rooms."); *Starsurgical, Inc. v. Aperta, LLC*, 40 F. Supp. 3d 1069, 1082 (E.D. Wis. 2014) (noting that "normal business practices like restricting access and requiring passwords" were not even enough for trade secret protection) (internal quotation marks and citation omitted); *Arko Plumbing Corp. v. Rudd*, 230 So.3d 520, 529–30 (Fla. Dist. Ct. App. 2017) (finding that maintaining customer pricing information in a password-

protected file and limiting access to two employees were "the sorts of reasonable efforts to maintain secrecy required by the trade secret statute"). Indeed, there is no evidence that supports the notion that employees even needed Cervencik's authorization to access the shared drive; to the contrary, the testimony establishes that any employee could have, with a modicum of knowledge or the aid of another employee, enabled their own workstation to access the shared drive. *See Cumulus Radio Corp. v. Olson*, 80 F. Supp. 3d 900, 912 (C.D. Ill. 2015) (expressing "serious doubts" that plaintiff would succeed on ITSA claims where the "information was readily accessible on a shared computer network that could be reviewed by anyone who had access to the computer system") (internal quotation marks omitted).

Although presumably as President, O'Mera made the decision to put Cervencik in a position overseeing IT security, others—such as those on Gamal's board or others on CGW's board—could have insisted on greater protections over CGW's purported trade secrets but did not. And when Gheciu was brought on board, she suggested that CGW take some basic steps to improve the security of the information at issue, such as segregating access to documents on a need-to-know basis and adopting an "Acceptable Device Use Policy" requiring that employees remove company data from their personal devices at the time of their separation. But CGW did not implement even those modest suggestions, further undermining its trade secret claim. *See Meade Elec. Co. v. Wicks*, No. 1-09-2933, 2011 WL 9933759, at *6 (Ill. App. Ct. May 9, 2011) (finding information not to be trade secret in part because plaintiff allowed project managers to take information home on laptop computers).

Perhaps the most telling evidence that CGW did nothing in particular to safeguard its supposed trade secrets is that it took no measures to protect that information that were in any way different (much less more exacting) than the steps that it took to protect information that was

indisputably not a trade secret. *See Opus Fund Servs. (USA) LLC v. Theorem Fund Servs., LLC*, No. 17 C 923, 2018 WL 1156246, at *3 (N.D. Ill. Mar. 5, 2018) (rejecting trade secret claim where plaintiff did "nothing to differentiate its protective measures for the alleged proprietary trade secrets from those imposed on any other corporate information"). CGW concedes that some of the information on the shared drive was publicly available, including the Mix & Match catalogue and shipping packaging weights. Pl.'s Prelim. Inj. Post-Hr'g Mem. ("Pl.'s Mem.") 25, ECF No. 58. But CGW did not treat the alleged trade secret information any differently on the shared drive, for example, by placing it in a more secure folder within the shared drive. CGW labeled some of its documents relating to its research and development efforts as "proprietary," *see, e.g.*, Defs.' Ex. 18, but those are not among the documents implicated by CGW's claims in this case. It takes virtually no effort and little sophistication to include a header on an Excel spreadsheet identifying a document as "proprietary" or "confidential," yet CGW failed even to do that much with respect to the information at issue in this case. *See Fail-Safe*, 674 F.3d at 893 (concluding that plaintiff did not take reasonable efforts to protect confidentiality of information based, in part, on plaintiff's failure to mark information as confidential and plaintiff's failure to use safeguards that plaintiff should have known were available); *see also Gillis*, 564 N.E.2d at 192 (concluding that information did not qualify as trade secret based, in part, on plaintiff's failure to use confidentiality stamps). The logical implication is that while CGW considered its research and development materials to be confidential, it did not hold that view of the information at issue in this case.

In the absence of meaningful security measures taken to safeguard its putatively valuable trade secrets, CGW argues that no amount of computer security could have stopped high-ranking officers like O'Mera and Cervencik from accessing and copying the data they wanted to take with them. That argument fails to persuade for several reasons. Most fundamentally, it is likely wrong

and in any event hardly a given; a robust and well-articulated data security program may well have deterred the retention and use of such information by O'Mera and other departing employees. Beyond that, the argument misses the mark. The question is not whether CGW could have prevented the misappropriation it alleges but rather whether it took steps to safeguard data that were commensurate with CGW's claim that the information has economic value by virtue of its secrecy. That test is objective: Did CGW employ data security measures reasonably consistent with its claim that the information at issue was valuable? Here, where the evidence shows that CGW did nothing to distinguish the information at issue from other information about the company, the answer is plainly no. CGW did not take "the kinds of affirmative measures courts have recognized as secrecy-preserving under Illinois law, such as limiting access to the information to certain employees only, keeping the information encrypted, password-protected, or locked, preventing copying of the protected information, or requiring employees to sign confidentiality agreements." *Am. Ctr. for Excellence in Surgical Assisting Inc. v. Cmty. Coll. Dist. 502*, 315 F. Supp. 3d 1044, 1058 (N.D. Ill. 2018) (internal quotation marks, brackets, and citation omitted). CGW's conduct was consistent not with its assessment that the information at issue would be of significant value to a competitor, but rather with O'Mera's assessment that it "would have negligible value" to a competitor like Weldcote. Hr'g Tr. 18:20-23.

2. Irreparable Injury

Even if CGW could show a better than negligible likelihood of success on the merits of its trade secret claim, CGW has failed to establish that Weldcote's access to the information at issue is likely to cause CGW to suffer irreparable harm for which it has no adequate remedy at law. *See Winter v. Natural Resources Defense Council, Inc.*, 555 U.S. 7, 22 (2008) (holding that plaintiff seeking preliminary injunction must "demonstrate that irreparable injury is *likely* in the absence of

an injunction") (emphasis in original). To be sure, the information at issue had some value to the defendants; otherwise, they would not have copied it. But the evidence has shown that it is likely of minimal marginal value to the defendants relative to the information they already possess through their extensive experience in the industry or could obtain through other sources. Further, the information at issue is already many months old and becomes increasingly stale and less valuable as market conditions, prices, and profit margins change and industry relationships evolve.

Given the defendants' experience in the industry and publicly available information, the defendants likely already knew or could have learned which suppliers and distributors they should approach. Even if O'Mera could not have memorized all of the data contained in the information at issue (indeed, his inability to remember it is likely why he wanted it), he had a deep understanding of the most important data, including prices and profit margins for the best-selling products from his nearly two decades of experience as CGW's president. What he likely could not remember—and what he likely needed to reference the data for—were the lower volume products and the precise numbers for those data points of which he already had a general sense. Many of O'Mera's customers (as well as those of Klug and Hickman) followed them from their previous jobs to CGW; these relationships were forged over decades and it is reasonable to infer that many customers of CGW would willingly follow O'Mera to Weldcote regardless of whether it had access to the information at issue. The evidence established that a number of factors other than price also influence the choices of customers in the abrasives market, including the quality and brand of the product, the personal relationship between the individuals negotiating, and other factors that are unrelated to whether the defendants have a marginally better understanding of how products should be priced by virtue of knowing how CGW's products were priced many months ago.

Further, CGW has not shown that having access to the information at issue has allowed or will allow the defendants to negotiate more effectively with suppliers by enabling the defendants to confirm whether CGW was getting a better price from a given supplier than Weldcote. For example, although CGW's supplier VSM may have agreed to provide O'Mera with the same price it provided to CGW, obtaining that promise had (so far as the record shows) nothing to do with O'Mera's access to CGW's historical pricing information. Any supplier could promise as much; there is no evidence that O'Mera extracted that agreement by confronting VSM with evidence that it was quoting a higher price to Weldcote than it had charged CGW. Nothing suggests that it was O'Mera's access to the information at issue that contributed to O'Mera's ability to obtain such a commitment from VSM—as opposed to, for example, his personal relationship with the company.

Weldcote has also already been able to obtain, or could obtain relatively easily, at least some of the information at issue directly from CGW's distributors. As to CGW's discount pricing, Weldcote can obtain substantially similar information by simply asking its customers what price it needs to beat as to any given product. Although the information provided by distributors might be anonymized—*e.g.*, a distributor might tell Weldcote that its price needs to be at a certain level to get the distributor's business—knowing the price at which Weldcote needs to set to get the distributor's business is what is valuable to Weldcote, not that a certain named competitor of Weldcote's is selling at that price.

Cervencik testified that she only opened one document but did not use it before closing it because she discovered the information was not useful. And although the VSM roll ordering data O'Mera asked Cervencik to obtain from CGW must have had at least some value to O'Mera (again, otherwise he would not have asked for it), clearly that information was not pivotal because O'Mera went ahead and placed the order for which that data would have been relevant without receiving

the data. Using the information as a reference point, benchmark, or confirmation for the defendants that their memory served them as to a particular product's price or profit margin may have some value to the defendants. But to say that the information had some value is not to say its value is great enough for the Court to conclude that irreparable harm to CGW for which there is no adequate remedy at law is likely to flow from the defendants' use of such information.

If CGW ultimately sustains damages as a result of the defendants' alleged wrongful conduct, it may be challenging to quantify such damages, but CGW has not shown that such damages would be unreasonably difficult to quantify if they do materialize. Although "[a] plaintiff may suffer irreparable harm if the nature of the loss makes monetary damages difficult to calculate," *E. St. Louis Laborers' Local 100 v. Bellon Wrecking & Salvage Co.*, 414 F.3d 700, 705 (7th Cir. 2005), an adequate remedy at law exists when damages can be quantified "to a reasonable, which is not to say a high, degree of precision," *Nicolet Instrument Corp. v. Lindquist & Vennum*, 34 F.3d 453, 456–57 (7th Cir. 1994). How much CGW suffered in lost profits could likely be quantified to a reasonable level of precision by analyzing profits CGW lost on any given product as a result of the defendants' use of the information at issue. *See Cullen Elec. Co. v. Cullen*, 578 N.E.2d 1058, 1063 (Ill. App. Ct. 1991) ("If the loss of future profits is also proved, there is no evidence that these could not be estimated with reasonable certainty by relying on plaintiff's many years of successful operation.").

B. State Law Causes of Action

CGW's poor prospects of establishing that the information at issue is entitled to trade secret protection necessarily means that it cannot show a better than negligible chance of success on its remaining state law causes of action—breach of fiduciary duty, unfair competition, and unjust enrichment—at least to the extent those causes of action are based on the alleged misappropriation

of CGW's confidential business information. That is because they are preempted by either the ITSA or the Delaware Uniform Trade Secrets Act ("DUTSA"), 6 Del. C. § 2001 *et seq*. And to the extent those state law causes of action are not based on the alleged misappropriation, they cannot provide a basis for injunctive relief because CGW has alleged no prospect of future irreparable harm flowing from anything other than the alleged, and preempted, claim that confidential information was misappropriated for use in Weldcote's business operations.

1. Preemption

State law causes of action that are based upon the misappropriation of confidential business information are preempted by ITSA or DUTSA[7] even when the information does not rise to the level of a trade secret. *See Spitz v. Proven Winners N. Am., LLC*, 759 F.3d 724, 733 (7th Cir. 2014) (holding that ITSA preempts claims that are "essentially claims of trade secret misappropriation, even when the alleged 'trade secret' does not fall within the Act's definition"); *see also Alarm.com Holdings, Inc. v. ABS Capital Partners, Inc.*, No. 2017-0583-JTL, 2018 WL 3006118, at *11 (Del. Ch. June 15, 2018) ("Delaware has joined the 'majority view' that section 7 of DUTSA precludes common law claims based on misappropriation of business information even in cases in which the claim does not meet the statutory definition of 'trade secret' under the Code.") (citing *Atl. Med. Specialists, LLC v. Gastroenterology Assocs., P.A.*, No. 15C-06-245 CEB, 2017 WL 1842899, at *15 (Del. Super. Apr. 20, 2017)).

[7] The parties agree that Delaware law applies to CGW's breach of fiduciary duty cause of action whereas Illinois law applies to CGW's other state law causes of action. The relevant preemptive language of Delaware's DUTSA is identical to that of Illinois's ITSA. *Compare* 6 Del. C. § 2007 (The DUTSA preempts "other law of this State [Delaware] providing civil remedies for misappropriation of trade a trade secret."), *with* 765 ILCS 1065/8 (The ITSA preempts "other laws of this State [Illinois] providing civil remedies for misappropriation of a trade secret.").

To the extent that CGW's state law theories of liability are premised on conduct other than the misappropriation of CGW's confidential business information, however, they are not preempted. *See* 765 ILCS § 1065/8 (The ITSA does not displace "other civil remedies that are not based upon misappropriation of a trade secret.").[8] For example, an "assertion of trade secret in a customer list does not wipe out claims of theft, fraud, and breach of the duty of loyalty that would be sound even if the customer list were a public record." *Hecny Transp., Inc. v. Chu*, 430 F.3d 402, 405 (7th Cir. 2005). "[T]he crux of the [preemption] question [is] whether the claim would lie if the information at issue were not confidential." *IPOX Schuster, LLC v. Nikko Asset Mgmt. Co.*, 191 F. Supp. 3d 790, 802 (N.D. Ill. 2016).

What this means in this case is that to the extent that CGW's remaining state law theories depend on the characterization of the information at issue as trade secret, confidential, or proprietary information, they are preempted by ITSA or DUTSA (and are therefore unlikely to succeed on the merits).[9] But if those theories would be viable even were it accepted that the information itself was not secret or confidential, there is no preemption. Put another way, a breach of fiduciary duty claim is not preempted by ITSA or DUTSA simply because it may involve the misappropriation of a trade secret; the question is whether the conduct at issue would give rise to liability without regard to whether the information in question was confidential or not.

---

[8] *See also* 6 Del. C. § 2007(b)(2) (The DUTSA does not affect "[o]ther civil remedies that are not based upon misappropriation of a trade secret.").

[9] In reaching this decision, the Court acknowledges a seeming anomaly that arises from the extension of ITSA preemption to any common law claim predicated on the misappropriation of information whether or not it rises to the level of a trade secret. Under the current state of the law, a plaintiff who asserts a claim based on the confidentiality of his business information may find himself in a proverbial "no man's land" where he cannot succeed on a trade secret claim because the information does not rise to the level of a trade secret and cannot pursue a misappropriation claim as to such information because it is nevertheless preempted.

In large measure, CGW's state law claims are premised on the purported confidentiality of the information at issue. If the information at issue were not confidential—that is, if CGW had posted all of the information at issue on its website for the general public's consumption—then it is difficult to imagine how the defendants could be said to have unjustly enriched themselves, unfairly competed, or breached the fiduciary duty they owed to CGW by copying and referencing the information just as any other member of the public could. Rather, if the information at issue were publicly available, then the defendants would have been entitled to do with that information exactly as they did. CGW's state theories of relief depend almost entirely on the purported confidentiality of the information at issue and are therefore preempted. And even if CGW has some better than negligible prospect for success on the merits of a state law claim that is not preempted, CGW has not shown that there is any continuing conduct relating to such a claim to enjoin.

2. Irreparable Harm and Adequacy of Remedy at Law

CGW has failed to establish that it is entitled to a preliminary injunction because it has not shown a better than negligible likelihood of success on any claim from which it alleges a threat of future irreparable harm. A claim for injunctive relief requires ongoing or impending harm. *Swanigan v. City of Chicago*, 881 F.3d 577, 583 n.2 (7th Cir. 2018). Yet CGW's entire irreparable harm argument is based on the alleged misappropriation of its confidential business information. *See, e.g.*, Pl.'s Mem. 29 ("Until entry of the TRO, Weldcote was using that non-public information to assist it to negotiate lower prices to suppliers and to target CGW distributors.") (internal citations and quotation marks omitted); *id.* 32–33 ("It will be near impossible for CGW to calculate the value of [the information at issue] to Weldcote and the damages [CGW] will suffer as it will be difficult for CGW to prove what prices Weldcote would have otherwise paid suppliers and what raw materials and finished products it would have otherwise purchased from suppliers without the

[information at issue]."); Pl.'s Post-Hr'g Resp. Mem. ("Pl.'s Resp.") 16–17, ECF No. 61 ("It will be extraordinarily difficult for CGW to determine what sales it will have lost (or what smaller profit margins it will have earned) but for Weldcote charging lower prices due to it having had on hand CGW supplier Data when it negotiates *its* prices with suppliers based on the prices those suppliers are charging CGW.") (emphasis in original).

CGW makes no argument (and cannot) that it faces impending harm from ongoing tortious conduct not involving misappropriation of confidential information. CGW's claim that O'Mera breached his fiduciary duty by working with Zika while still employed by CGW, for example, is not based on the misappropriation of CGW's confidential business information and is not preempted. But that claim cannot serve as the basis for a preliminary injunction because the alleged breach is complete; the individual defendants no longer owe any fiduciary duties to CGW, and CGW has not alleged an ongoing breach or a threat of future irreparable harm flowing from it that is separate and apart from the alleged misappropriation. Indeed, the only injunctive relief that CGW seeks in the breach of fiduciary counts in its Amended Complaint is to prevent the defendants from using the information at issue. *See* Am. Compl., Counts III – VIII, Prayers for Relief, (requesting that Court enjoin defendants "from using or disclosing, directly or indirectly, any Third-Party Transaction Information or other derivative information contained" in allegedly misappropriated files). The Amended Complaint simply identifies no ongoing harm arising from tortious conduct that is not preempted by the ITSA or DUTSA. CGW does not (and cannot) allege that O'Mera (or Cervencik, for that matter) is engaged in an ongoing breach of a fiduciary duty to CGW. Accordingly, such a claim cannot support its request for injunctive relief to prevent ongoing irreparable injury.

C. CFAA

CGW similarly fails to establish that the defendants' alleged violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, is causing any ongoing irreparable injury. CGW has not alleged any future threat of the kind of harm CFAA protects against: damage to computer systems. To bring a civil cause of action under CFAA, CGW must have suffered "damage or loss." 18 U.S.C. § 1030(g). CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). This definition of "damage" includes the "destruction, corruption, or deletion of electronic files" and "any diminution in the completeness or usability of the data on a computer system," but it does not include "the mere copying of electronic information from a computer system." *Farmers Ins. Exch. v. Auto Club Grp.*, 823 F. Supp. 2d 847, 852 (N.D. Ill. 2011); *see also Del Monte*, 616 F. Supp. 2d at 811 ("[C]opying electronic files from a computer database—even when the ex-employee emails those files to a competitor—is not enough to satisfy the damage requirement of the CFAA.").

CFAA defines "loss" as "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 the interruption of service." 18 U.S.C. § 1030(e)(11). There is no evidence in the record that the defendants' copying or transferring of CGW's data destroyed or impaired CGW's data causing "damages" to CGW. But the majority view in this district is that "a plaintiff can satisfy the CFAA's definition of loss by alleging costs reasonably incurred in responding to an alleged CFAA offense, even if the alleged offense ultimately is found to have caused no damage as defined by the CFAA." *PolyOne Corp. v. Lu*, No.

14-cv-10369, 2018 WL 4679577, at *14 (N.D. Ill. Sept. 28, 2018) (citing *Farmers Ins. Exch.*, 823 F. Supp. 2d at 854).

CGW retained Forensicon to conduct an assessment of the consequences of defendants' actions that, at the time, CGW reasonably could have believed resulted in deletion or impairment of CGW's data. Gheciu discovered that Cervencik had deleted files from her working folder at CGW, and especially when considered in the context of O'Mera's and Cervencik's transfers of CGW information, CGW reasonably could have believed that more substantial impairment or destruction of CGW's data had occurred and ordered a forensic analysis to assess the potential damages. Forensicon's forensic analysis cost more than $20,000, Am. Compl. ¶ 190, well above the $5,000 in costs to meet the magnitude of loss required for CGW to bring a civil cause of action under the CFAA, *see* 18 U.S.C. § 1030(c)(4)(A)(i)(I).

But CGW does not allege that it needs an injunction to protect it from future "damage" or "loss" as defined in CFAA. CGW's alleged "loss" from retaining Forensicon to conduct a damage assessment has already been incurred. *See* Pl.'s Resp. 13 (arguing CGW suffered loss under CFAA, but not alleging any threat of future damages or losses). The kind of harm the CFAA protects against is not the kind of harm from which CGW seeks protection through its preliminary injunction motion. *See Kluber Skahan & Assoc., Inc. v. Cordogen, Clark & Assoc., Inc.*, No. 08-cv-1529, 2009 WL 466812, at *8 (N.D. Ill. Feb. 25, 2009) ("The [CFAA] statute was not meant to cover the disloyal employee who walks off with confidential information. . . . Losses are monetary harms attenuated from the underlying concern of the Act: damage to data.") (internal quotations and citation omitted). The CFAA cause of action therefore cannot serve as the basis for a preliminary injunction.

D. Balancing of Harms

CGW has not shown a better than negligible chance of success on the merits or a likelihood of irreparable harm for which there is no adequate remedy at law to establish that it is entitled to a preliminary injunction of any scope. But even it had, the balance of harms analysis would still favor Weldcote when considering whether to bar Weldcote from operating in the abrasives industry. The point of assessing the balance of harms is to apportion the risk that injunctive relief is granted, or denied, in error. *AM Gen. Corp. v. DaimlerChrysler Corp.*, 311 F.3d 796, 831 (7th Cir. 2002) (the "court appraises the risk of irreparable harm to the parties not simply by reference to what they will lose by an unfavorable ruling . . . but rather by reference to the harm of error" in that ruling). Barring the defendants from engaging in the abrasives business would be disproportionate to any harm caused by defendants' alleged wrongful conduct, and the irreparable harm to Weldcote from doing so would far outweigh any irreparable harm to CGW from declining to do so.

No injunction bond could fully compensate for the harm to the innocent Weldcote employees who would likely lose their jobs if the Court were to enter a preliminary injunction as broad as CGW requests. *See Roland Mach. Co. v. Dresser Indus., Inc.*, 749 F.2d 380, 387 (7th Cir. 1984) ("[T]he Court must also consider any irreparable harm that the defendant might suffer from the injunction—harm that would not be either cured by the defendant's ultimately prevailing on the merits or fully compensated by the injunction bond that Rule 65(c) of the Federal Rules of Civil Procedure requires the district court to make the plaintiff post."). The injunction CGW seeks would bar Weldcote's entry into the abrasives market, render millions of dollars of investment a waste, and leave a number of its innocent employees without jobs, whereas it would only protect

CGW from damages that CGW has not shown are likely to materialize or would jeopardize CGW's ongoing viability.

Weldcote also currently plans to operate in a narrower part of the abrasives industry than CGW, selling fewer products (approximately 900 products rather than 5,000 or more) and working with fewer suppliers (6 rather than 45). Given that Weldcote intends to do business with only a subset of the abrasives industry in which CGW has widespread ties, barring Weldcote from doing business with CGW's suppliers and distributors could be tantamount to an outright ban from the abrasives industry. At worst, for CGW, it faces a new competitor (as to a small portion of its products) who can offer highly competitive prices by virtue of knowing what CGW's costs and prices were as of June 2018. By contrast, the injunction CGW demands would stop Weldcote's entry into the abrasives business in its tracks. As such, on one side of the scale we have somewhat lower profits; on the other, the elimination of an entire business line. The latter would not be an equitable result.

E. Public Interest

Barring the defendants from operating in any subset of the abrasives industry would also disserve the public interest. The protection of trade secrets reflects a "balancing of social and economic interests." *Sw. Whey, Inc. v. Nutrition 101, Inc.*, 117 F. Supp. 2d 770, 776 (C.D. Ill. 2000). Although an "individual who has put forth the time, money, and effort to obtain a secret advantage should be protected from a party who obtains the secret through improper means," that individual is nevertheless "entitled to utilize the general knowledge and skills acquired through experience in pursuing his chosen occupation." *Id.* at 777. Barring the defendants from utilizing their general knowledge and skills by entering the abrasives business would not show due regard for this balancing of social and economic interests.

The public has an interest in free and fair competition. Prohibiting a company from operating is an especially severe remedy that restrains free trade. "The primary purpose of trade secret law is to encourage innovation and development, and the law should not be used to suppress legitimate competition." *Am. Can Co. v. Mansukhani*, 742 F.2d 314, 329 (7th Cir. 1984). Entering a preliminary injunction as broad as that sought by CGW would deny the marketplace of the benefits attendant to competition and could result in distributors (and end users) paying more for lower-quality products than they would if CGW had to compete against Weldcote for their business. *See Vienna Beef, Ltd. v. Red Hot Chicago, Inc.*, 833 F. Supp. 2d 870, 877 (N.D. Ill. 2011) (public interest disfavored granting injunctive relief because doing so would only "curtail commercial competition when [the plaintiff] has not carried its burden to show that such an order is necessary to prevent harm"). While enabling corporations to protect legitimate trade secrets provides benefits to the public as well as to corporations, that interest is not compelling where—as here—it appears that a corporation has done little, if anything, to safeguard its supposed secrets. In the Court's view, the public's interest here clearly favors an outcome that promotes, rather than restricts, competition: that is, a denial of CGW's motion for a preliminary injunction preventing Weldcote's entry into the abrasives market.

* * *

To recap: The Court concludes that CGW has failed to demonstrate a better than negligible chance that it will prevail on the merits of its trade secret claim. Any non-preempted conduct presents no prospect of continuing harm and therefore does not warrant the imposition of injunctive relief. CGW also does not allege any threat of future damages to its computer systems. And the balance of harms and the public interest weigh in Weldcote's favor. CGW's amended motion for entry of preliminary injunction, ECF No. 44, is denied.

Dated: March 4, 2019

John J. Tharp, Jr.
United States District Judge