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

ARKEYO, LLC,	:	
Plaintiff,	:	CIVIL ACTION
	:	No. 16-4720
v.	:	
	:	
CUMMINS ALLISON CORPORATION,	:	
Defendant.	:	

June 28, 2017 **Anita B. Brody, J.**

MEMORANDUM

I. INTRODUCTION

Plaintiff Arkeyo, LLC ("Arkeyo") brings state law claims against Defendant Cummins Allison Corporation ("Cummins") for breach of contract, misappropriation of trade secrets, conversion, and tortious interference.[1] Arkeyo creates software that integrates with coin counting machines. Cummins manufactures and sells coin counting machines. Prior to working together, the parties entered into a Non-Disclosure Agreement ("NDA") to protect the disclosure of proprietary and confidential information to third parties. Thereafter, Arkeyo collaborated with Cummins to create software compatible with Cummins' MM2 coin counting machine (the "MM2 Machine"). Arkeyo would purchase MM2 Machines from Cummins, attach them to its custom computers and configure them with Arkeyo software, and then resell the MM2 Machines to Metro Bank plc ("Metro Bank") for installation in banks located in the United Kingdom.

Currently before me is Arkeyo's motion for a preliminary injunction. Arkeyo alleges that Cummins misappropriated its trade secret software. Arkeyo moves solely on the basis of its

[1] Cummins also brings counterclaims against Arkeyo and Third-Party Defendants William Tustin and Daniel Taylor. I exercise diversity jurisdiction over the parties' claims pursuant to 28 U.S.C. § 1332.

misappropriation of trade secrets claim to preliminarily enjoin Cummins from selling its coin counting machines directly to Metro Bank, as well as to any other customer in circumstances where the machine is sold as part of a system that includes software derived in whole or in part from the Arkeyo software.

During the course of discovery, Cummins informed the Court that Arkeyo's purported trade secret software had been posted on Arkeyo's website on the internet. Cummins now contends that Arkeyo has no protectable trade secret because of its publication of the Arkeyo software on the internet. On May 2 and 3, 2017, I held an evidentiary hearing to address Arkeyo's motion for a preliminary injunction that was limited to whether Arkeyo can establish a likelihood of success on its claim that Cummins violated the Illinois Trade Secrets Act.[2]

For the reasons set forth below, after consideration of the testimony from the witnesses, the documentary evidence, and the relevant law, I will deny Arkeyo's motion for a preliminary injunction.

II. FINDINGS OF FACT[3]

At the evidentiary hearing, Cummins presented three witnesses: (1) Expert Dan Schonfeld; (2) Expert Peter Fry; and (3) Cummins engineer Kevin Carrera.[4] Arkeyo also

[2] The parties agree that Arkeyo's misappropriation of trade secrets claim is brought under the Illinois Trade Secrets Act because the NDA between the parties mandates that Illinois law governs. *See* Daniel Taylor Declaration Ex. 1 ¶ 5.2.

[3] Cummins seeks admission into evidence of exhibits that it presented at the evidentiary hearing, but were not admitted into evidence. These exhibits are located in Appendix B to Cummins' Post Hearing Memorandum. I will admit them into evidence, and have considered them in reaching the findings of fact.

[4] Arkeyo seeks to preclude the Court from considering the testimony of Cummins' experts: Dan Schonfeld and Peter Fry. Arkeyo contends that their testimony should be precluded because Cummins did not comply with Federal Rule of Civil Procedure 37(c).

Rule 37(c) provides: "If a party fails to provide information or identify a witness as required by Rule 26(a) or (e), the party is not allowed to use that information or witness to supply evidence on a motion, at a hearing, or at a trial, unless the failure was substantially justified or is harmless." Fed. R.

presented three witnesses: (1) Expert Hunter Jones; (2) Arkeyo President Daniel Taylor; and (3) Arkeyo employee Michael Yetter. Upon consideration of the evidence presented, I make the following findings:[5]

On January 4, 2016, Arkeyo emailed Cummins to inform Cummins that it had posted the Arkeyo software, known as the "Metro Bank UK 2.15 software," on its website on the internet. The Arkeyo software remained posted on Arkeyo's website for the next fifteen months. The software was available at the URL: http://arkeyo.com/new_software/. URL stands for Uniform Resource Locator. As explained by the Third Circuit, "the domain name portion of the URL—everything before the '.com'—instructs a centralized web server to direct the user to a particular

---

Civ. P. 37(c)(1). In determining whether to exclude testimony for failure to comply with discovery requirements, a court considers four factors:

> (1) the prejudice or surprise of the party against whom the excluded evidence would have been admitted; (2) the ability of the party to cure that prejudice; (3) the extent to which allowing the evidence would disrupt the orderly and efficient trial of the case or other cases in the court; and (4) bad faith or wilfulness [sic] in failing to comply with a court order or discovery obligation.

Nicholas v. Pa. State Univ., 227 F.3d 133, 148 (3d Cir. 2000).

On April 25, 2017, the parties exchanged responses to discovery requests, and Cummins disclosed to Arkeyo that its expert witnesses would testify regarding eight listed topics. On April 29, 2017, the parties exchanged initial witness and exhibit lists, and summaries of their intended expert testimony. Arkeyo provided Cummins with a thirteen page summary of its intended expert testimony; whereas Cummins again referred to the list of eight topics its experts intended to cover. The parties agreed to exchange demonstrative exhibits one day before the hearing. Accordingly, on May 1, 2017, Cummins provided Arkeyo with a copy of the demonstrative slides that it intended to present in Court.

Arkeyo objects to the last minute receipt of the demonstrative slides, and claims that the slide deck contained expert opinion that was not previously disclosed. The parties agreed, however, not to exchange demonstrative exhibits until the day before the hearing. Although Cummins provided Arkeyo with only a terse summary of its intended expert testimony, the slides addressed the eight topics that Cummins had previously informed Arkeyo would be the subject of its expert testimony. There is no evidence that Cummins failed to comply with any discovery requirements. Regardless, even if Cummins disregarded a disclosure obligation when it failed to provide a more comprehensive expert summary to Arkeyo, consideration of the factors detailed in *Nicholas* weigh against exclusion of Cummins' expert testimony. There is no evidence that Cummins acted in bad faith and Arkeyo suffered little to no prejudice because it received the list of expert topics in advance.

[5] The findings of fact are based on the documentary exhibits and witness testimony presented at the evidentiary hearing.

website, but post-domain name portions of the URL are designed to communicate to the visited website which webpage content to send the user." *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 139 (3d Cir. 2015). Accordingly, the "arkeyo" portion of the URL: http://arkeyo.com/new_software/ instructed a centralized web server to direct the user to Arkeyo's website and the "new_software" portion of the URL informed Arkeyo's website to display the webpage that contained the new software.

When a person visited the URL: http://arkeyo.com/new_software/, the following text would appear: "click to download Metro Bank UK 2.15 software." When a user clicked on the text, a zip file[6] that contained the Arkeyo software would appear on the computer, and the user would be given the option to either open or save the zip file. By simply selecting to save the zip file, a user could download the entire zip file onto a computer in minutes.

Some of the Arkeyo software that could be downloaded from the zip file appeared as source code. However, much of the Arkeyo software that could be downloaded from the zip file appeared as executable code. Source code is the human readable form of software—it is comprised of human words that are written in a programming language. Whereas executable code is the form of software that can be understood by a computer —it is comprised of zeros and ones. Compilation is the process of taking the human readable source code and translating it into executable code. Decompilation is the process of taking executable code and translating it back into human readable source code.

The Arkeyo software that was available in executable code could easily be decompiled and translated back to source code by using a decompiler such as "Dot Peek." Dot Peek is available on the internet to anyone to download for free. By using a decompiler such as Dot

[6] "A 'zip file' is a large computer file that has been compressed to a smaller size so that it can be easily transmitted over the Internet." *United States v. Bobb*, 577 F.3d 1366, 1369 n.5 (11th Cir. 2009).

Peek to decompile Arkeyo's executable code, any user could obtain the full functional equivalent of the Arkeyo source code.

Arkeyo identified ten areas of software functionality in its source code that it claimed were trade secrets.[7] Either immediately upon download of the zip file, or upon completion of the decompilation process, all of the areas of functionality that Arkeyo identified as trade secrets in its source code were obtainable from the software that Arkeyo put on its website.

In order to use the Arkeyo software on a computer, a long sequence of installation steps had to be followed. One of the key installation steps was changing the administrator[8] name to "Metro." If the administrator name was not changed to "Metro," then the installation of the software would fail. Only three people at Arkeyo had knowledge of the installation process. The zip file, however, contained a folder called "Installer," and inside the folder was a text file called "Install Instructions." The text file contained instructions on how to install the software, including an instruction that the user or administrator name had to be changed to "Metro."

In addition to needing the installation instructions, a person who wanted to install the Arkeyo software also needed the base operating software referred to by Arkeyo as version 2.8.1. Thus, the Arkeyo software could not properly be installed and would not work if a computer did not already have the base operating software installed. The zip file, however, contained a piece of software called "Arkeyo Updater," that would install base operating software version 2.8 onto

[7] The ten areas of software functionality that Arkeyo identified are: Receipt, Guessing Game, General User Interface, Charitable Giving, British Currency, Off-Sorting, Remote Management, Bin Reporting Software, Batch Processing Control, and Full Bin Warning. These areas of functionality relate to the different features that Arkeyo provided to enhance the MM2 Machine, some of which assisted with communications between the Arkeyo computer that ran the Arkeyo software and the MM2 Machine.

[8] "An administrator is someone who can make changes on a computer that will affect other users of the computer. Administrators can change security settings, install software and hardware, access all files on the computer, and make changes to other user accounts." Microsoft, *How do I Log on as an Administrator*, https://support.microsoft.com/en-us/help/14028/windows-7-how-log-on-as-an-administrator (last visited June 28, 2017).

the computer and enable a user to then properly install the Arkeyo software. Arkeyo version 2.8 is an earlier version of the base operating software 2.8.1. No discernible differences that would impact the functionality of the Arkeyo software have been identified between these two versions of the base operating software.

The Arkeyo software on the Arkeyo website was a full set of software that could be installed and used immediately in MM2 Machines. All of Arkeyo's source code was readily available from the zip file, which also included the required base operating software and instructions for installing the Arkeyo software.

When Arkeyo placed its full set of software on its website, and made it readily available for download onto any computer, it did not take the standard precautions in the industry to protect the confidentiality of its source code.[9] Although the URL: http://arkeyo.com/new _software/ did not appear as a visible link on the Arkeyo website and would not appear in response to any web searches,[10] Arkeyo did not give the URL a random name, a basic precaution

[9] If source code is particularly important, then the most reasonable reaction is not to put it on the internet. It is only reasonable to put the source code on the internet if it is deemed necessary for ease of use and standard precautions are taken to protect its secrecy.

[10] On April 4, 2017, after Cummins informed the Court that Arkeyo's purported trade secret software had been posted on Arkeyo's website on the internet, Arkeyo removed the URL: http://arkeyo.com/new_software/ and placed the zip file from the referenced webpage into a password protected folder on the Arkeyo server without making a forensic copy of the URL. Cummins contends that Arkeyo spoliated the evidence by removing the URL and seeks sanctions for Arkeyo's alleged spoliation. At a minimum, Arkeyo requests that the Court disregard Arkeyo's evidence concerning the inability to use a search engine to locate the URL because it is impossible to test Arkeyo's claim that the URL would not appear in response to any web searches. At a maximum, Arkeyo requests that the Court dismiss Arkeyo's misappropriation of trade secrets claim and award Cummins attorneys' fees, expert fees, and expenses incurred in addressing the spoliation issue.

"Spoliation occurs where: the evidence was in the party's control; the evidence is relevant to the claims or defenses in the case; there has been actual suppression or withholding of evidence; and, the duty to preserve the evidence was reasonably foreseeable to the party." *Bull v. United Parcel Serv., Inc.*, 665 F.3d 68, 73 (3d Cir. 2012). Additionally, "a finding of bad faith is pivotal to a spoliation determination." *Id.* at 79.

Daniel Taylor, the President of Arkeyo, removed the URL from the Arkeyo website to protect the materials on the zip file because he noticed a sudden increase in traffic to the website that he was

that should be taken any time sensitive information is posted on the internet. Rather, Arkeyo named the URL "new_software," which described exactly what was posted at that internet address. Moreover, Arkeyo's website at http://arkeyo.com/new_software/ was not secure because Arkeyo elected to use an HTTP site rather than an HTTPS site.[11] Therefore, any transmission of data between a user's browser and the website was not encrypted. Additionally, Arkeyo had no other encryption protection. Arkeyo also had no password protection—no password was required to enter the website, to access the zip file, or to access the individual files within the zip file once it was downloaded. Arkeyo did not employ any code obfuscation, a standard tool used to protect executable code from reverse engineering, which makes it difficult to convert executable code to human readable source code. Furthermore, Arkeyo did not identify the software as confidential. It did not require visitors to the website to agree to any terms of use that would limit their use of the Arkeyo software. The source code itself also did not include any standard legal language to protect its use. As a consequence, anyone who visited the "new_software" URL had unlimited access to Arkeyo's full set of software.

III. STANDARD OF REVIEW

In deciding whether to grant a preliminary injunction, a district court should balance the following four factors so long as the moving party meets the requisite showing on the first two: (1) the movant has shown a likelihood of success on the merits; (2) the movant will suffer

---

concerned might be driven by nefarious motives to steal the Arkeyo software or hack into the website. When he removed the URL and placed the zip file from the referenced webpage into a password protected folder on the Arkeyo server, he did not intend to destroy any evidence because he knew Cummins already had downloaded a copy of the zip file from the internet. Taylor never received a document hold notice that informed him of his duty to preserve documents and no one ever informed him of his obligation to preserve documents. Arkeyo did not spoliate evidence because Taylor did not act in bad faith when he removed the URL: http://arkeyo.com/new_software/ and placed the zip file from the referenced webpage into a password protected folder on the Arkeyo server.

[11] HTTP stands for Hyper Text Transfer Protocol and HTTPS stands for Hyper Text Transfer Protocol Secure.

irreparable harm in the absence of a preliminary injunction; (3) the possibility of harm to other interested persons from a grant or denial of the injunction; and (4) the public interest. *Reilly v. City of Harrisburg*, ---F.3d---, No. 16-3722, 2017 WL 2272114, at *2 (3d Cir. May 25, 2017). Accordingly,

> a movant for preliminary equitable relief must meet the threshold for the first two "most critical" factors: it must demonstrate that it can win on the merits (which requires a showing significantly better than negligible but not necessarily more likely than not) and that it is more likely than not to suffer irreparable harm in the absence of preliminary relief. If these gateway factors are met, a court then considers the remaining two factors and determines in its sound discretion if all four factors, taken together, balance in favor of granting the requested preliminary relief.

Id. at *4 (footnotes omitted).

IV. ANALYSIS AND CONCLUSIONS OF LAW

Arkeyo cannot prevail on its motion for preliminary injunction because it cannot meet the threshold requirement of a demonstration of likelihood of success on the merits under the Illinois Trade Secrets Act ("ITSA"), 765 Ill. Comp. Stat. Ann. 1065/1 *et seq.* "To prevail on a claim for misappropriation of a trade secret under the Act, the plaintiff must demonstrate that the information at issue was a trade secret, that it was misappropriated and that it was used in the defendant's business." *Learning Curve Toys, Inc. v. PlayWood Toys, Inc*., 342 F.3d 714, 721 (7th Cir. 2003). Under the ITSA, a trade secret means:

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

765 Ill. Comp. Stat. Ann. 1065/2(d). These two requirements for a trade secret focus on different aspects of secrecy:

> The first requirement . . . "precludes trade secret protection for information generally known or understood within an industry even if not to the public at large." The second requirement . . . prevents a plaintiff who takes no affirmative measures to prevent others from using its proprietary information from obtaining trade secret protection.

Learning Curve, 342 F.3d at 722 (citation omitted). In determining whether a trade secret exists, "the most important [consideration] is whether and how an employer acts to keep the information secret." *Alpha Sch. Bus Co. v. Wagner*, 910 N.E.2d 1134, 1152 (Ill. App. Ct. 2009). A court need not reach the first requirement—whether a purported trade secret derives economic value from not being generally known—if the plaintiff has not met the second requirement because it failed to take reasonable measures to maintain secrecy. *Seng-Tiong Ho v. Taflove*, 648 F.3d 489, 504-05 (7th Cir. 2011) (declining to decide whether the purported trade secret had economic value because the plaintiffs had not taken reasonable steps to maintain secrecy and thus could not succeed on the ITSA claim).

In order to meet the second requirement, a plaintiff must take "affirmative measures to prevent others from using its proprietary information." *Glob. Material Techs., Inc. v. Dazheng Metal Fibre Co.*, No. 12-1851, 2016 WL 4765689, at *10 (N.D. Ill. Sept. 13, 2016). While the ITSA requires that a plaintiff take reasonable measures under the circumstances to maintain the secrecy of a purported trade secret, "it does not require perfection." *Learning Curve*, 342 F.3d at 725. Considerations of "the size and sophistication of the parties, as well as the relevant industry" may factor into the reasonableness inquiry. *Id.* at 726. However, "[b]y definition a trade secret has not been placed in the public domain." *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 484 (1974). "If an individual discloses his trade secret to others who are under no

obligation to protect the confidentiality of the information, or otherwise publicly discloses the secret, his property right is extinguished." *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1002 (1984). It is "well established that there can be no confidential disclosure where there has been a prior disclosure to the public without reservation." *Skoog v. McCray Refrigerator Co*., 211 F.2d 254, 257 (7th Cir. 1954).

Cummins contends that Arkeyo's decision to make its software publicly available on the internet for fifteen months without taking standard precautions to protect its confidentiality demonstrates that it did not take reasonable steps to protect its trade secrets. Arkeyo counters that it did not make its software publicly available on the internet, and that even if it did so, it took reasonable efforts to protect its trade secrets.

A. Public Availability of Arkeyo's Software

Because the zip file contained mostly executable code and not human readable source code, Arkeyo claims that it did not publicly disclose its trade secret software on the internet. Arkeyo's executable code, however, could be translated into source code through the relatively simple process of decompilation—a process as simple as translating French into English. Arkeyo's contention that its software was not publicly available because it only appeared on the internet in executable code and not in source code is unjustifiable. It is no different than arguing that a trade secret posted on the internet in French would not be publicly available to an English speaker because it would require translation. Arkeyo misses the point when it argues that its trade secret software was not publicly available because it was immediately understood by computers and not by people. The Arkeyo software was immediately ready to install and download onto any computer, and could be used in any MM2 Machine without modification, precisely because it was available in executable code on the zip file.

Arkeyo also claims that its source code was not publicly available because the URL: http://arkeyo.com/new_software/ was not linked to the main Arkeyo website and would not appear on any internet search engines. Although the URL was unlisted, Arkeyo named the URL "new_software," which described exactly what was posted at that internet address. The URL was guessable to anyone who wanted to access the zip file because Arkeyo did not take the basic precaution of giving the URL a random name, and the website was publicly available to anyone who typed the URL into the address bar. The evidence refutes Arkeyo's contention that it did not make its trade secrets publicly available on the internet.

B. Reasonable Measures to Maintain Secrecy

Alternatively, Arkeyo argues that even if its software was on the internet, it took reasonable measures to protect its secrecy, and that its publication on the internet does not destroy the software's trade secret status. Arkeyo argues that regardless of publication, its software was protected because the zip file did not contain the installation instructions or the base operating software necessary to deploy the Arkeyo software and therefore, the source code could not be used by a competitor. To the contrary, the evidence demonstrates that the zip file contained installation instructions, base operating software, and a full set of the Arkeyo software. Regardless, even if the zip file had not contained any base operating software or new installation instructions, a competitor still could have installed and used the software immediately on Metro Bank MM2 Machines, which already possessed these prerequisites. Moreover, Arkeyo does not claim that the installation instructions or base operating software are trade secrets. Most importantly, all of the software that Arkeyo contends is a trade secret was available on the zip file.

Arkeyo also points to its non-disclosure agreements with Cummins and Metro Bank as evidence that it took reasonable measures to protect its trade secrets. "Although a confidentiality agreement is a factor to consider, it is not the only factor." *Arcor, Inc. v. Haas*, 842 N.E.2d 265, 271 (Ill. App. Ct. 2005). These agreements became ineffectual once Arkeyo published its trade secrets on the internet because Arkeyo made its software publicly available to individuals who owed no duty of non-disclosure to Arkeyo. *Arcor*, 842 N.E.2d at 271 (holding that the plaintiff did not take reasonable steps to keep customer information secret and it did not qualify as a trade secret where plaintiff had employees sign a confidentiality agreement, but did not "take[] additional measures such as limiting access to its customer information by computer password or keeping track of the hard copies of the information").

Arkeyo published a full set of its software on the internet without employing any of the industry standard protections for its source code—it did not use encryption, password protection, code obfuscation, confidentiality provisions, or require users to abide by any terms of use for its software.

In *Harleysville Insurance Company v. Holding Funeral Home, Inc.*, the district court addressed whether the plaintiff had waived attorney-client privilege with regard to information it had posted for six months on an internet-based electronic file sharing service referred to as Box Site. 2017 WL 1041600, at *1 (W.D. Va. Feb. 9, 2017). The information was not password protected and "any person who had access to the internet could have accessed the Box Site by simply typing in the url address in a web browser." *Id.* at *1. The district court concluded that the plaintiff had not taken any precautions to prevent disclosure of the information and held that the plaintiff had waived attorney-client privilege. *Id.* at *4-5. In reaching this decision, the district court reasoned:

> [The plaintiff's] actions were the cyber world equivalent of leaving its claims file on a bench in the public square and telling its counsel where they could find it. It is hard to image an act that would be more contrary to protecting the confidentiality of information than to post that information to the world wide web.

Id. at * 5.

Similar to the plaintiff in *Harleysville*, Arkeyo committed the cyber equivalent of leaving its software on a park bench. It posted its software for fifteen months on the internet and made it publicly available to anyone who simply typed the "new_software" URL into a web browser, without taking any affirmative measures to prevent others from using its proprietary information. As the Ninth Circuit has explained:

> Internet publication is a form of "aggregate communication" in that it is intended for a broad, public audience, similar to print media. In both print and Internet publishing, information is generally considered "published" when it is made available to the public. Once information has been published on a website or print media, there is no further act required by the publisher to make the information available to the public.

Oja v. U.S. Army Corps of Engineers, 440 F.3d 1122, 1131 (9th Cir. 2006) (footnotes omitted). The posting of materials on the internet without any confidentiality protections makes the information publicly available and renders the materials incapable of trade secret status. *See Delaware Cty. Chamber of Commerce v. USI Ins. Servs., LLC*, No. 12-2280, 2013 WL 6847001, at *11 (E.D. Pa. Dec. 30, 2013) (holding that a member list was not a trade secret because it was publicly available on the internet and in a membership directory); *Am. Hearing Aid Assocs., Inc. v. GN Resound N. Am.*, 309 F. Supp. 2d 694, 706 (E.D. Pa. 2004) (holding that materials readily available on the plaintiff's website were available to the public and did not qualify as trade secrets). Arkeyo published its software on the internet without taking any reasonable measures to protect its confidentiality. Because Arkeyo publicly disclosed its software, it is not a trade

secret. *See Ruckelshaus*, 467 U.S. at 1002; *Kewanee*, 416 U.S. at 484. Therefore, Arkeyo is not likely to succeed on its claim that Cummins violated the ITSA.

V. CONCLUSION

For the reasons set forth above, I will deny Arkeyo's motion for a preliminary injunction because Arkeyo has not demonstrated a likelihood of success on the merits of its ITSA claim.

s/Anita B. Brody

_____

ANITA B. BRODY, J.

Copies **VIA ECF** on _____ to:

Copies **MAILED** on _____ to: