[DO NOT PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 14-14943
Non-Argument Calendar

D.C. Docket No. 1:11-cv-02061-HLM

WAREHOUSE SOLUTIONS, INC.,

Plaintiff-Counter
Defendant-Appellant,

versus

INTEGRATED LOGISTICS, LLC,
Individually,
DAN WOTRING,
Individually,
DAVID IVIE,
Individually,
MICHAEL HEYDEN,
Individually,

Defendants-Counter Claimants-
Appellees.

Appeal from the United States District Court
for the Northern District of Georgia

(May 8, 2015)

Before TJOFLAT, HULL and WILSON, Circuit Judges.

PER CURIAM:

Plaintiff-Appellant Warehouse Solutions, Inc. ("WSI") appeals the district court's order granting summary judgment to Defendants-Appellees Integrated Logistics, LLC and its owners Dan Wotring, David Ivie, and Michael Heyden (collectively, "ILL") on WSI's claim for misappropriation of trade secrets under the Georgia Trade Secrets Act of 1990 ("GTSA"), O.C.G.A. § 10–1–760 et seq. After review, we affirm.[1]

I. BACKGROUND

A. The Parties' Business Relationship

Plaintiff-Appellant WSI is a logistics business formed in 1996 by Joseph Lebovich. In 1998, Lebovich developed a software program called Intelligent Audit. Intelligent Audit is a web-based program that interfaces with UPS and FedEx tracking systems to allow companies to track their packages and collect

[1] We review de novo the district court's grant of summary judgment, viewing all facts in the light most favorable to the non-moving party. Morales v. Zenith Ins. Co., 714 F.3d 1220, 1226 (11th Cir. 2013). Summary judgment is appropriate only when there exists no genuine factual dispute and the movant is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(a).

funds for late or missing packages. Intelligent Audit generates customer reports, performs e-bill audits, and allows customers to view real-time data regarding their packages. Lebovich hired Scott Langley and Langley's company to help sell the Intelligent Audit program. Langley received a 20% interest in the software in return for his services.

Defendant-Appellee ILL is a logistics company that, like WSI, provides users with package-tracking software. In 2002, after seeing Langley's demonstration of Intelligent Audit, ILL hired Langley and ILL began reselling the program to its own customers under the name "ShipLink." For each parcel audited by the ShipLink program, ILL paid WSI a transaction fee of $.015. WSI and ILL never executed a written agreement with regard to this resale arrangement or any other aspect of their business relationship.

To log into the Intelligent Audit program, a user must enter an authorized user identification ("ID") and password. As a reseller of the software, ILL "actively managed" its customers' accounts and was authorized to create and give user IDs and passwords to its customers. Because ILL was the most active user of the system, it had greater access to the program's features than other resellers or end-users, i.e., customers. However, it is undisputed that ILL never had access to Intelligent Audit's source code.

On several occasions, Lebovich told ILL that Intelligent Audit was highly confidential and proprietary. Lebovich instructed ILL not to share the program with anyone outside of ILL, with the exception of ILL's customers who had signed a contract containing a confidentiality provision that expressly forbade disclosure.

In 2004, without WSI's knowledge, ILL hired Platinum Circles Technologies ("Platinum") to develop its own web-based tracking program that was visually and functionally similar to Intelligent Audit. ILL gave Platinum a user ID and password to log onto the Intelligent Audit program. Like ILL, however, Platinum never had access to the program's source code.

On September 30, 2005, ILL terminated its business relationship with WSI and began selling the program developed by Platinum under the "ShipLink" name.

B. District Court Proceedings

WSI sued ILL for copying the Intelligent Audit software. ILL filed an answer raising nine counterclaims against WSI, including a counterclaim for tortious interference with business relations.[2]

On September 25, 2012, WSI filed an amended complaint against ILL raising various federal and state law claims, including a claim for misappropriation of trade secrets. WSI alleged that Intelligent Audit was a trade secret that ILL had

[2] This counterclaim arose from WSI's alleged refusal to recognize ILL's ownership interest in the software, which caused ILL to lose prospective customers.

misappropriated by creating a functionally identical program. The parties cross-moved for summary judgment.

As to the misappropriation of trade secrets claim, ILL contended that it only had access to the program's visible output, which does not constitute a trade secret, and, in any event, WSI failed to protect the program's secrecy. WSI argued that it took all reasonable means to prevent disclosure of its complicated software program, including the use of technologically-advanced password protection and encryption and end-user confidentiality provisions.

On July 7, 2014, the district court granted ILL summary judgment on all of WSI's claims and granted WSI summary judgment on all but one of ILL's counterclaims. Only ILL's counterclaim for tortious interference with business relations remained.

In relevant part, the district court found that (1) Intelligent Audit was not a trade secret within the meaning of the GTSA because the program's visible output (i.e., interactive screen displays) was readily apparent to users of the software, and (2) WSI did not make reasonable efforts to maintain the program's secrecy.

In doing so, the district court drew a distinction between a software program's underlying source code, which may be a trade secret, and the program's "look and feel" and "functionality," which cannot. Unlike source code, which is written in a programming language and is not accessible to program users, a user of Intelligent Audit can "readily ascertain the appearance and functionality of the system and, thus, the visible output cannot be a trade secret pursuant to O.C.G.A. § 10–1–761(4)(A)." Here, the parties agreed that ILL did not have access to Intelligent Audit's source code.

The district court rejected WSI's contention that, because WSI took steps to preserve the confidentiality of Intelligent Audit, the "self-revealing nature" of the program's functionality did not preclude the program's status as a trade secret. The district court noted that there was no evidence that WSI required ILL to sign a confidentiality agreement. The only efforts WSI actually took to maintain secrecy—verbally warning ILL of the confidential nature of the program and requiring customers to access the system with a username and password—were not reasonable under the circumstances to keep the program's visible output secret. Accordingly, the district court granted ILL summary judgment on WSI's misappropriation of trade secrets claim.

On October 9, 2014, the district court granted WSI's unopposed motion for entry of final judgment under Federal Rule of Civil Procedure 54(b). The court found that "pressing needs for a prompt resolution of the issues concerning [WSI's] claim for misappropriation of trade secrets warrant certifying the dismissal of that claim as a final judgment." On the same day, the clerk entered a separate judgment in favor of ILL on WSI's claim for misappropriation of trade secrets.

WSI timely appealed.[3]

II. DISCUSSION

A claim for misappropriation of trade secrets under the GTSA requires a plaintiff to prove that "(1) it had a trade secret and (2) the opposing party misappropriated the trade secret." Penalty Kick Mgmt. Ltd. v. Coca Cola Co., 318 F.3d 1284, 1290-91 (11th Cir. 2003) (quotation omitted). Whether information constitutes a trade secret is a question of fact. Id. at 1291. The GTSA defines a "trade secret" as

> information, without regard to form, including, but not limited to, technical or nontechnical data, a formula, a pattern, a compilation, a program, a device, a method, a technique, a drawing, a process, financial data, financial plans, product plans, or a list of actual or potential customers or suppliers which is not commonly known by or available to the public and which information:
>
> > (A) Derives economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and
> >
> > (B) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

O.C.G.A. § 10–1–761(4).

Here, the only dispute concerns two of the required statutory elements: whether Intelligent Audit was (1) not "readily ascertainable by proper means" and

[3] We conclude that the district court did not abuse its discretion in finding "no just reason for delay" and certifying the July 7, 2014 order as a final judgment under Rule 54(b). See Fed. R. Civ. P. 54(b).

(2) "the subject of efforts that are reasonable under the circumstances to maintain its secrecy." See id.

WSI relies heavily on an unpublished decision from the Northern District of Georgia, AirWatch, LLC v. Mobile Iron, Inc., No. 1:12-cv-3571, 2013 WL 4757491 (N.D. Ga. Sept. 4, 2013). Based on that decision, WSI argues that the functional aspects of Intelligent Audit, such as its report generation and data-processing features, were kept sufficiently secret to qualify as trade secrets under Georgia law.

The district court in AirWatch acknowledged case law distinguishing between a software program's underlying source code and its visible output, but nevertheless found that "information regarding [the plaintiff's security software for mobile phones] may still be a trade secret, if [the plaintiff] can show that it worked to preserve the secrecy of its program's functions, specifications, and pricing." 2013 WL 4757491, at *4. The nature of the software in AirWatch was "not such that a typical [smartphone] user . . . would be exposed to the software's capabilities by using the program." Id. Thus, offering free trials of the program to licensees who were subject to confidentiality provisions did not "per se forfeit the program's trade secret status." Id. Accordingly, the district court denied the defendant's motion to dismiss for failure to state a claim. Id. at *5.

In contrast to the software in AirWatch, dissemination of Intelligent Audit to users necessarily revealed the information WSI alleges to be secret (i.e., the program's "features and functions"). We note that WSI did not allege misappropriation of the program's source code, and the parties do not dispute that no one outside of WSI had access to the source code. Even assuming the functionality of the Intelligent Audit program was not "readily ascertainable by proper means," a review of the record reveals that WSI's efforts to maintain secrecy were not reasonable under the circumstances.

The record indicates that Lebovich verbally instructed ILL to keep Intelligent Audit confidential, and there is some evidence that ILL required its own customers to sign confidentiality agreements. Yet it is undisputed that WSI did not require ILL to sign any written agreement before granting ILL "high-level administrative access" to Intelligent Audit. Though not dispositive, the absence of a written non-disclosure agreement is relevant to assessing whether WSI took reasonably available steps to preserve the program's secrecy. WSI points to use of "numerous confidentiality measures," including limiting access to authorized users as well as employing encryption and password protection. However, these security measures served to restrict access to customer data—which WSI does not claim as trade secrets—rather than the functionality of the program itself. How Intelligent

Audit looked and worked was readily apparent to authorized users with an ID and password.

In sum, WSI failed to meet its burden of presenting sufficient evidence from which a reasonable jury could find that the "features and functions" of Intelligent Audit qualify as trade secrets under the GTSA. We therefore affirm the district court's grant of summary judgment in favor of ILL on WSI's claim for misappropriation of trade secrets.

AFFIRMED.