SUPERIOR COURT OF NEW JERSEY
APPELLATE DIVISION
DOCKET NO. A-4847-17T3

STERIS CORPORATION,

Plaintiff-Appellant,

v.

DAVID SHANNON,

Defendant-Respondent.

Argued April 2, 2019 – Decided June 10, 2019

Before Judges Fisher, Hoffman and Geiger.

On appeal from Superior Court of New Jersey, Chancery Division, Camden County, Docket No. C-000134-16.

David M. Walsh argued the cause for appellant (Jackson Lewis, PC, attorneys; David M. Walsh, of counsel and on the briefs; R. Shane Kagan, on the briefs).

Alan H. Schorr argued the cause for respondent (Schorr & Associates, PC, attorneys; Alan H. Schorr, on the brief).

PER CURIAM

Plaintiff STERIS Corporation appeals from a Chancery Court order granting summary judgment and dismissing its lawsuit against defendant David Shannon, a former employee who began competing against plaintiff, allegedly using legally protected client information owned by plaintiff. Plaintiff contests the court's grant of summary judgment in favor of defendant on all counts of plaintiff's complaint, arguing that genuine issues of material fact remain, warranting a trial.

For the reasons that follow, we reverse and remand for trial.

I.

Plaintiff sells medical equipment and supplies. In 1999, General Econopak, Inc. employed defendant as a sales consultant of medical supplies. In July 2015, plaintiff acquired General Econopak, and on November 5, 2015, plaintiff terminated defendant's employment.

When plaintiff terminated defendant, it asked him to return his "computer, keys, garage door opener[,] and customer files." However, on the morning of November 6, 2015, defendant informed Brad Smoyer, an employee of plaintiff, that he "and his son and daughter stayed up all night and printed STERIS documents from [defendant's] company-issued laptop computer. [Defendant] explained they did this because he was aware he had to return his laptop to

[plaintiff] the next day . . . ." At his deposition, Smoyer added that defendant said he purchased two printers to complete this project.

The record also contains an affidavit by John Tozzi, a forensic computer analyst, who examined defendant's company-issued laptop. According to Tozzi, "on November 5, 2015, at 9:38 p.m., a PNY USB 2.0 device was attached to the laptop for the first time, and was disconnected for the last time a few hours later on November 6, 2015, at 2:38 a.m."

On December 21, 2015, plaintiff and defendant entered into a "Confidential Separation Agreement and General Release" (the Agreement), which provided that, in exchange for thirteen weeks of compensation, defendant agreed to release plaintiff from all claims and liabilities. Defendant also agreed, in relevant part, to "keep confidential and not divulge to any third party . . . any confidential, proprietary, and/or trade secret information of STERIS, including, without limitation, information regarding STERIS's practices, policies, financial data, . . . and customers . . . ." Defendant "further agree[d] to not use any confidential, proprietary, and/or trade secret information of STERIS to [defendant's] own or another's benefit." Defendant was also to "return to STERIS any and all STERIS equipment and property of any kind whatsoever

that [defendant] may have in [his] possession." The Agreement did not include a non-compete clause.

On February 24, 2016, defendant entered into a "mutual nondisclosure agreement" with Technipaq, Inc., one of plaintiff's main competitors. By May 2016, defendant had started his own company, Shannon Aseptic Consulting, LLC, (Shannon Aseptic) which entered into an "independent sales contractor role" with Technipaq.

On October 17, 2017, plaintiff filed a verified complaint, alleging that defendant "was contacting and soliciting certain STERIS' customers on behalf of Shannon Aseptic," and "[t]he solicitations included contacts that were not associated with [defendant]'s former accounts." The complaint asserted that defendant "could not have obtained the identities and contact information for [these] solicitations . . . but for his possession of . . . STERIS' confidential contact and other proprietary information."

According to Julia Madsen, a vice president and general manager for plaintiff, defendant "was using the knowledge from the [Act] [D]ata[]base as well as the financial data base to pursue" plaintiff's customers, in violation of

the severance agreement. The Act Database[1] is a "sophisticated customer relationship management software" that contains "contact information, . . . sales activities, pipeline, opportunities, history, proprietary documents, secondary contact information, relationship information, personal customer information, engagements, and timelines, all related to [plaintiff]'s customers and sales activities." Madsen related that defendant also used "sales report[s] that he had access to which would include all of the customers, where they're located, what they buy, and what they pay and the quantity that they purchase globally"; defendant received a printed version of plaintiff's sales reports on a monthly basis when he worked for plaintiff.

A forensic computer analyst provided the parties with a confidential report comparing plaintiff and Shannon Aseptic's Act Databases. The report stated that plaintiff's Act Database contained 17,400 entries, or contacts, while Shannon Aseptic's Act Database had 5550 entries. Of these entries, it is undisputed that approximately 1750 of the entries were duplicates, containing the exact same companies, contact names, addresses, email addresses, and even the same typographical errors or inaccurate use of all caps or all lowercase. At his

[1] The record frequently refers to the program as the "Act!" or "ACT!" database – for purposes of this opinion we refer to the program as the "Act Database."

deposition, defendant admitted that he synchronized his cell phone with plaintiff's Act Database to the extent of names, telephone numbers, addresses, and email addresses, and he transferred this information from his cell phone into his new company's Act Database.

Madsen further testified that Technipaq acquired a former client of plaintiff's, "Baxter," which previously generated $800,000 in annual revenue for plaintiff. Another salesperson of plaintiff had the Baxter account, but defendant was the salesperson's manager. Madsen testified that defendant solicited business from other customers of plaintiff, specifically "BPL in UK" and "Central Biomedia," which were not connected with defendant when he worked for plaintiff. The record also contains an email from defendant to an individual from "Hospira/Pfizer," a contact of plaintiff, attempting to solicit business.

As to the Central Biomedia account, the record includes a July 26, 2016 price quote from Technipaq and Shannon Aseptic. The quote was attached to an email between plaintiff's employees, which reads that defendant personally "visited" an employee from Central Biomedia, who provided the information to plaintiff. Defendant told the Central Biomedia employee that "he can get the same materials [plaintiff] currently provide[s] at a lower price," and that defendant "also promised lead times to be much shorter . . . ."

Defendant may have solicited or acquired business from other companies that were consumers of plaintiff, but the record is lacking in part because on March 16, 2018, the trial court denied plaintiff's order to compel discovery, which sought to have defendant "identify any and all known current or former customers of [p]laintiff to whom [d]efendant sold competing product since November 4, 2015 . . . ."

The record also lacks a significant amount of defendant's computer history during relevant periods. Defendant certified that between September and December 2015, he "was temporarily using a . . . laptop that used to be [his] son's computer," which he claimed was "antiquated and worthless and we threw it away when we got . . . new computers in May." A forensic computer analyst wrote a report on five computers turned over by defendant, but he found that new operating systems were installed; the analyst explained, "The USB history reports only show the USB activity for the time period AFTER the current [operating system] was installed – any activity that predated the installation was purged from the computer's memory as part of the installation . . . ." Defendant certified he "installed the Windows 10 upgrade on all of the computers . . . . because Windows 10 offered greater security and a free upgrade."

Plaintiff's verified complaint set forth the following causes of action: (1) breach of the severance agreement; (2) breach of implied covenant of good faith and fair dealing; (3) misappropriation of confidential and proprietary information; (4) violation of the New Jersey Trade Secrets Act, N.J.S.A. 56:15-1; (5) violation of the New Jersey Computer Related Offenses Act, N.J.S.A. 2A:38A; (6) unjust enrichment; and (7) unfair competition. Plaintiff sought to enjoin defendant "from destroying, using, revealing, copying, or disseminating . . . any information concerning [plaintiff's] business, including but not limited to . . . [plaintiff's] confidential, proprietary, and trade secret information."[2] Plaintiff also sought compensatory and punitive damages.

After a trial date was set, defendant moved for summary judgment. Following oral argument, the trial judge granted defendant's motion on all counts, and entered an order dismissing plaintiff's complaint. The judge reasoned:

> [W]hatever was contained in the database of [plaintiff] is not really protected information, ... it's names, addresses, and phone numbers of customers who -- all of whom are well known in the industry and all of whom can be contacted and be seen as . . . potential customer[s] for any company. Anybody who is -- even a startup business.

[2] Within thirty days of the filing of plaintiff's complaint, the court entered a consent order granting plaintiff the injunctive relief sought in its complaint.

While the judge noted a potential issue of fact as to whether "defendant downloaded the database information from [plaintiff]'s computer," and withheld boxes of plaintiff's documents after his termination, the judge found these factual issues immaterial, concluding the information was not protected as confidential, proprietary, or trade secret information. This appeal ensued.

II.

We review a grant of summary judgment under the same standard that governs the trial court. Henry v. N.J. Dep't of Human Servs., 204 N.J. 320, 330 (2010). Summary judgment must be granted if "the pleadings, depositions, answers to interrogatories and admissions on file, together with affidavits, if any, show that there is no genuine issue as to any material fact challenged and that the moving party is entitled to a judgment or order as a matter of law." R. 4:46-2(c). There is a genuine issue of material fact precluding summary judgment when "the competent evidential materials presented, when viewed in the light most favorable to the non-moving party, are sufficient to permit a rational factfinder to resolve the alleged disputed issue in favor of the non-moving party." Brill v. Guardian Life Ins. Co. of Am., 142 N.J. 520, 540 (1995).

Here, the severance agreement between the parties explicitly states that defendant was not to retain or use "confidential, proprietary and/or trade secret

information of [plaintiff], including, without limitation information regarding [plaintiff]'s practices . . . financial data . . . and customers . . . ." (emphasis added). While "customers" is listed in the contract as a trade secret, and the trial judge observed there is a potential issue of fact as to whether defendant stole 1750 consumer and contact entries from plaintiff's Act Database, she ruled for defendant by finding the database information "is not really protected information." Since defendant himself conceded that he synchronized contacts from plaintiff's Act Database, and then transferred them into Shannon Aseptic's Act Database, the issue is whether the information taken was legally protected.

To be legally protectable, information need not rise to the level of a trade secret and may otherwise be publicly available. Lamorte Burns & Co. v. Walters, 167 N.J. 285, 299 (2001). The key to determining the misuse of information is the relationship of the parties at the time of disclosure and the intended use of the information, ibid.; however, matters of general knowledge within an industry may not be classified as confidential. Whitmyer Bros., Inc. v. Doyle, 58 N.J. 25, 33-34 (1971).

Customer lists can be considered confidential and subject to protection. "In all instances, a substantial measure of secrecy must exist in order for information to be treated as a trade secret." Lamorte Burns, 167 N.J. at 299.

The Supreme Court enumerated six factors to consider in determining whether information, such as the customer data in question, constitutes a trade secret:

> (1) the extent to which the information is known outside of the business; (2) the extent to which it is known by employees and others involved in the business; (3) the extent of measures taken by the owner to guard the secrecy of the information; (4) the value of the information to the business and to its competitors; (5) the amount of effort or money expended in developing the information; and (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.
>
> [Ingersoll-Rand Co. v. Ciavatta, 110 N.J. 609, 637 (1988) (citing Restatement of Torts § 757 cmt. b (1939) (Am. Law Inst., amended 1979)); see also Hammock by Hammock v. Hoffmann-Laroche, 142 N.J. 356, 384 (1995).]

In Lamorte Burns, the court reaffirmed these principles, 167 N.J. at 298-99, and applied them to the facts and holdings of Platinum [Mgmt.], Inc. v. Dahms, 285 N.J. Super. 274, 295 (Law Div. 1995):

> In Platinum, [the] plaintiff sued its former employee for breach of the duty of loyalty, claiming that [the defendant] discussed its customers with his new employer. [The d]efendant argued that the information was not protectable because it was publicly available. Ibid. The court disagreed, and found that the information the plaintiff sought to protect went beyond mere names, but also included buying habits, mark-up structure, merchandising plans, projections, and product strategies. Ibid. The court stated that the customer's names may have been listed in readily

> obtainable trade directories, but the fact that they were the plaintiff's customers was not. Ibid. The court concluded that the identity of the customers is "entitled to protection when divulged in confidence to a key employee . . . where [the defendant] is a party to a covenant not to compete." Ibid.
>
> [Lamorte Burns, 167 N.J. at 298-300.]

Here, it is undisputed that defendant was never bound by a covenant not to compete. However, Lamorte Burns involved two former employee defendants – only one of whom was subject to a non-compete – that left the plaintiff company to establish a new business and compete directly against it. Id. at 291-93. The defendants developed a targeted solicitation list based on information from the plaintiff's client files. Ibid. The Court disagreed with our "conclusion that a trial [was] needed to determine whether the information secretly gathered by defendants was legally protected," id. at 301, and instead held that the plaintiff was "entitled to summary judgment on its . . . claims . . . that [both of the] defendants misappropriated [the] plaintiff's confidential and proprietary information and committed unfair competition." Id. at 309.

In concluding the information the defendants took from plaintiff was legally protected, the Court found:

> The information surreptitiously gathered by [the] defendants from [the] plaintiff was not generally available to the public, but was shared between plaintiff

> and its clients. [The d]efendants would not have been aware of that information but for their employment. The information went beyond the mere names of plaintiff's clients. It included specific information concerning the clients' claims . . . . [The d]efendants admitted that that information gave them an advantage in soliciting [the] plaintiff's clients once they resigned. But, the information was available to [the] defendants for their use in servicing clients on behalf of [the plaintiff] only.
>
> The record is clear that [the] defendants also knew that [the plaintiff] had an interest in protecting that information. [One of the defendants] signed an agreement that so stated, and both . . . declined to sign a later agreement that sought to afford further protection to the information. [One defendant] acknowledged that he would not have given such information to a competitor if requested, and he would not have permitted a[n] employee [of plaintiff] to do so. Also, [the defendants] both were aware that [a] co-employee . . . had been fired because of his attempt to privately solicit Lamorte's customers.
>
> [Id. at 301-02.]

Here, viewing the evidence in the light most favorable to plaintiff, there remains a genuine issue of material fact as to whether the information gathered by defendant was legally protected. There is sufficient evidence for a rational factfinder to conclude that the 1750 duplicate contact entries between the parties' Act Databases were trade secrets owned by plaintiff, which were surreptitiously taken and used by defendant. While it is plausible that the names of the

companies, their key contact employees' names, email addresses, and phone numbers could be collected from the industry's directories and LinkedIn, as defendant contends, we disagree that this vast collection of information should be considered, as a matter of law, "readily ascertainable," N.J.S.A. 56:15-2, or easily duplicated, Ingersoll-Rand Co., 110 N.J. at 637. Evidence in the record also suggests that the Act Database contains plaintiff's history with the listed contacts, such as "sales activities, pipeline, [and] opportunities."

Plaintiff made efforts to protect the information at issue from defendant: it took his company computer back the day after his termination; it sought to collect all paper documents from his home; and in the severance agreement, it secured defendant's agreement to "return to [plaintiff] any and all [of plaintiff's] equipment and property of any kind whatsoever that [defendant] may have in [his] possession." Lastly, defendant agreed to "keep confidential," "not divulge," and "not use any confidential, proprietary, and/or trade secret information of STERIS to [his] own or another's benefit." The record reflects genuine issues of material fact as to whether defendant breached these parts of the agreement.

The record also contains evidence that defendant actively sought to attain proprietary information owned by plaintiff upon his termination, and took steps

to cover his tracks in the process. The night of his termination, defendant allegedly bought two printers and stayed up all night with his son and daughter, printing documents from his company-issued laptop. The forensic computer analyst's report supports this allegation, indicating that a USB drive was inserted into that computer for the first time on November 5, 2015, at 9:38 p.m., and remained connected until 2:38 a.m. the next morning. The record also reveals that defendant threw away the computer he used for several relevant months, and then purged his new computers' histories when he installed new operating systems in them.

Considering "the relationship of the parties . . . and the intended use of the information," Lamorte, 167 N.J. at 299 (citing Platinum Mgmt., 285 N.J. Super. at 295), plaintiff terminated defendant, who agreed to not use plaintiff's proprietary or trade secrets information. Defendant also agreed to return any such property to plaintiff. The record contains evidence, sufficient to survive summary judgment, that defendant used this information with the intent to take business from plaintiff by reaching out to plaintiff's key contacts within these client companies, and offered the same products for lower prices and faster service than what plaintiff was providing to them. Since defendant did not actively work with these clients while employed by plaintiff, a rational

factfinder could conclude that he used plaintiff's proprietary or trade secret information in these solicitations. Moreover, while the record includes one client taken from plaintiff in Baxter, and three of plaintiff's clients solicited by defendant in "BPL in UK," "Central Biomedia," and "Hospira/Pfizer," more clients might have been discovered had the trial court granted plaintiff's motion to compel discovery on this matter.

Viewed in a light most favorable to plaintiff, the evidence in the record raises genuine issues of material fact as to whether defendant misappropriated legally protected information or trade secrets owned by plaintiff, whether this was in breach of the severance agreement, and whether defendant's conduct constituted unfair competition. We therefore reverse the order granting the summary judgment dismissal of plaintiff's complaint and remand the case for trial.

Reversed and remanded. We do not retain jurisdiction.