

United States District Court
District of Massachusetts

)
Viken Detection Corporation,)
)
)
Plaintiff,)
)
)
v.) **Civil Action No.**
) **19-10614-NMG**
Videray Technologies Inc. and)
Paul E. Bradshaw,)
)
Defendants.)

MEMORANDUM & ORDER

GORTON, J.

Viken Detection Corporation ("Viken" or "plaintiff") brings this suit against Paul Bradshaw ("Bradshaw") and Videray Technologies Inc. ("Videray") (collectively "defendants"), alleging that Bradshaw misappropriated Viken's confidential information when he left Viken to form Videray to compete directly with Viken. Viken asserts that defendants' conduct constitutes 1) a violation of the Defend Trade Secrets Act ("the DTSA"), 18 U.S.C. § 1836(b)(1); 2) a violation of the Computer Fraud and Abuse Act ("the CFAA"), 18 U.S.C. § 1030; 3) misappropriation of trade secrets, M.G.L. c. 93, §§ 42 and 42A; 4) breach of contract; 5) breach of the duty of loyalty; and 6) tortious interference with contracts.

Pending before the Court is the motion of defendants to dismiss all counts of plaintiff's complaint (Docket No. 26).

I. Background

A. The Parties

Viken, formerly known as "Heuresis Corporation", is a Delaware corporation with its principal place of business in Massachusetts. Viken produces and sells hand-held x-ray scanners used by law enforcement and security professionals to discover concealed explosives, narcotics and other contraband in a quick and cost-effective manner. Among Viken's main products is the HBI-120, which is a hand-held x-ray backscatter imaging device.

Videray is a Delaware corporation with its principal place of business in Massachusetts. Bradshaw is a resident of Massachusetts and the founder and president of Videray. Videray has developed the PX1 which, like the HBI-120, is a hand-held x-ray backscatter imaging device.

B. Bradshaw's Employment with Viken

Bradshaw began his employment with Viken in November, 2013, as its Director of Engineering. He also periodically acted as Viken's Information Technology Administrator ("ITA"). At some point during his employment, Bradshaw was assigned to a team tasked with developing the HBI-120.

As part of his role on that team and as Viken's Director of Engineering, Bradshaw had access to proprietary and confidential information regarding the design, performance, marketing and strategic plan for the HBI-120, as well as potential modifications, improvements and design changes to that device. That information, which was stored electronically, was subject to access restrictions and password protection. In his role as ITA, Bradshaw was charged with implementing and overseeing most or all of the electronic access controls used to protect the HBI-120 proprietary and confidential information.

Bradshaw stored proprietary and confidential information relating to the HBI-120 on his desktop computer, laptop computer and personal Dropbox account. His Dropbox account allegedly contained approximately 1,800 sensitive files in a folder named "Hbi120." Bradshaw also kept files related to the plans for other Viken products on his personal Dropbox.

Others on Viken's research and development team purportedly had access to the files on Bradshaw's personal Dropbox account, including the former CEO of Viken, Henry Grodzins ("Grodzins"). The current CEO of Viken, Jim Ryan, attests, however, that he is not aware that anyone at the company previously knew that Bradshaw stored sensitive Viken documents on his personal Dropbox account.

Viken requires all new employees to sign a nondisclosure agreement ("the NDA"). Bradshaw was compelled to sign the NDA as a condition of his employment. Pursuant to that contract, he agreed that he would

keep in strictest confidence and trust all Proprietary Information [as defined in the NDA], and . . . not use or disclose any Proprietary Information without the written consent of the Company, except as may be necessary in the ordinary course of performing my duties to the Company.

Bradshaw also agreed that he would not retain any Proprietary Information of Viken upon termination of his employment. He further agreed that during his employment and for a period of one year thereafter, he would not 1) recruit or solicit for employment any employee of Viken or any affiliate of the company (or a former employee within his or her one-year grace period) or 2) interfere with Viken's business relationships with other persons or companies by inducing or attempting to induce a person or company to refrain from or discontinue doing business with Viken.

C. The Alleged Misconduct

In June, 2017, Katie McCabe ("McCabe"), a former employee of Viken, informed the company that while Bradshaw was still working at Viken, he told her that he planned to leave Viken and start a new company that would produce and sell a competing product. She also alleged that, while still employed by Viken,

Bradshaw met with a potential investor to solicit funds for his new company. He also purportedly solicited co-workers to leave with him by accessing confidential salary and equity information from Viken's protected server.

McCabe also alleged that Bradshaw failed to share customer feedback with Viken as to potential product improvements, while telling his co-workers that his new product would include those improvements. She told Viken managers that Bradshaw asked other employees to help him collect confidential Viken customer information for use at his new company. Finally, Bradshaw purportedly told McCabe that, in reference to a computer on which he kept proprietary and confidential information about the HBI-120, "I have everything I need". Bradshaw vigorously denies those allegations but at least one other Viken employee reiterates McCabe's assertions.

In May or June, 2017, Viken terminated Bradshaw's employment, at least partly as a result of McCabe's allegations. Within a few days after his termination, however, then-CEO Grodzins offered Bradshaw his job back because he believed that McCabe either lied or exaggerated about Bradshaw's conduct. Bradshaw declined the offer of re-instatement.

Viken alleges that within two months after he left the company, Bradshaw formed Videray. Videray has developed the PX1

which apparently has the same external design, ergonomics and operating characteristics as Viken's HBI-120. Viken alleges that the PX1 1) is the same size and shape, 2) uses approximately the same x-ray energy, 3) uses approximately the same power and 4) likely achieves the same x-ray shielding requirements for user safety as the HBI-120. It allegedly does so by using

a combination of Viken trade secrets involving characteristics of the X-ray anode, X-ray shielding material (alloy), and source-detector geometry.

Viken asserts that the PX1 includes certain design modifications that were taken from confidential Viken documents and which Videray advertises as product advantages on its website. Those modifications include 1) increased power by upgrading to "140 [keV]", 2) "[i]mage analysis and processing . . . object recognition capability" and 3) use of a touch screen interface with additional buttons to control the device. Viken purportedly protected those design modifications as trade secrets for possible future use and Bradshaw had access to that information during his employment with Viken. Plaintiff contends that the files maintained on Bradshaw's personal Dropbox account were proprietary and confidential information of Viken and that Bradshaw misappropriated and used that information after he left Viken.

D. Procedural History

Plaintiff filed its complaint in the instant action in March, 2019. Shortly thereafter, it filed a motion for a temporary restraining order and preliminary injunction. Defendant moved to dismiss plaintiff's complaint in its entirety in May, 2019.

This Court considered plaintiff's motion for injunctive relief at a hearing in June, 2019. The Court ultimately denied plaintiff's motion on the ground that plaintiff failed to demonstrate a reasonable likelihood of success on the merits.

II. Defendants' Amended Motion to Dismiss

A. Legal Standard

To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to "state a claim to relief that is plausible on its face." Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007). In considering the merits of a motion to dismiss, the Court may only look to the facts alleged in the pleadings, documents attached as exhibits or incorporated by reference in the complaint and matters of which judicial notice can be taken. Nollet v. Justices of Trial Court of Mass., 83 F. Supp. 2d 204, 208 (D. Mass. 2000), aff'd, 228 F.3d 1127 (1st Cir. 2000).

Furthermore, the Court must accept all factual allegations in the complaint as true and draw all reasonable inferences in the plaintiff's favor. Langadinos v. Am. Airlines, Inc., 199 F.3d 68, 69 (1st Cir. 2000). If the facts in the complaint are sufficient to state a cause of action, a motion to dismiss the complaint must be denied. See Nollet, 83 F. Supp. 2d at 208.

Although a court must accept as true all the factual allegations in a complaint, that doctrine is not applicable to legal conclusions. Ashcroft v. Iqbal, 556 U.S. 662 (2009). Threadbare recitals of legal elements which are supported by mere conclusory statements do not suffice to state a cause of action. Id. Accordingly, a complaint does not state a claim of relief where the well-pled facts fail to warrant an inference of any more than the mere possibility of misconduct. Id. at 1950.

B. Application

1. Count II: Violation of the CFAA

To establish a claim under the CFAA, a plaintiff must prove that the defendant "knowingly and with intent to defraud" accessed a protected computer without valid authorization or in excess of authorization to further the intended fraud and obtain something of value, with certain exceptions not relevant here.

18 U.S.C. § 1030(a)(4).

The phrase "without authorization" is not defined in the statute, but this Court has previously recognized that the First Circuit Court of Appeals has advocated for a broad interpretation of that phrase to include an employee who accesses his employer's computer, without the employer's knowledge, to acquire, or after acquiring, an interest adverse to his employer. Guest-Tek Interactive Entm't, Inc. v. Pullen, 665 F. Supp. 2d 42, 45 (D. Mass. 2009) (citing EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582-84 (1st Cir. 2001)). The phrase to "exceed authorized access" is defined as to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.

18 U.S.C. § 1030(e)(6).

Defendant urges the Court to narrow its interpretation of the CFAA, arguing that plaintiff's claim must be dismissed because there is no violation of the CFAA when an employee misappropriates information that he had authorization to access.

See Wec Carolina Energy Solutions, LLC v. Miller, 687 F.3d 199 (4th Cir. 2012). Viken responds that when Bradshaw accessed its sensitive and confidential information, he was acting not as an authorized employee, but as an unauthorized competitor. See International Airport Centers, LLC, 440 F.3d at 419-20.

In denying plaintiff's motion for a preliminary injunction, this Court found that plaintiff had not demonstrated a reasonable likelihood of success on its CFAA claim because members of Viken's research and development team apparently had access to the files on Bradshaw's personal Dropbox account and former-CEO Grodzins attested that he was aware of and had no issue with Bradshaw's use of his personal Dropbox account for that purpose.

That conclusion does not, however, support an inference that Viken has failed to state a claim upon which relief can be granted. Indeed, Viken alleges that regardless of what level of authorization Bradshaw was granted as its employee, when he accessed its protected information for the purpose of competing with Viken, a quintessential adverse interest, he was acting either without or in excess of his authorization. Considering such allegations as true for the purpose of the motion at issue, plaintiff has stated a claim for relief pursuant to the CFAA under First Circuit law.

2. Counts I and III: Violation of the DTSA and Misappropriation of Trade Secrets

A plaintiff can establish misappropriation of trade secrets pursuant to M.G.L. c. 93, § 42 by proving that the defendant acquired them through improper means (including by theft, bribery, misrepresentation or breach of contract but not by

reverse engineering) or by disclosing or using trade secrets obtained through improper means without that person's consent. M.G.L. c. 93, § 42. A plaintiff may also bring a claim under the DTSA for misappropriation of trade secrets if the trade secret is related to a product or service used in or intended to be used in interstate or foreign commerce. 18 U.S.C. § 1836(b)(1). The standard for misappropriation under the DTSA is substantially similar to that under Massachusetts law. Compare 18 U.S.C. § 1839(5)-(6), with M.G.L. c. 93, § 42(1)-(2).

To prevail on a claim of misappropriation of trade secrets, a plaintiff must establish that 1) the information at issue constitutes a trade secret, 2) the plaintiff took reasonable measures to secure the confidentiality of the information and 3) the defendant obtained the trade secret through improper means. Optos, Inc. v. Topcon Medical Systems, Inc., 777 F. Supp. 2d 217, 238 (D. Mass. 2011).

A trade secret is any confidential information used in the plaintiff's business that "gives [the owner] an advantage over competitors who do not know or use it". Id. (quoting J.T. Healy & Son, Inc. v. James A. Murphy & Son, Inc., 260 N.E.2d 723, 729 (Mass. 1970)). Matters of public knowledge or information generally known in an industry cannot be a trade secret. J.T.

Healy, 260 N.E.2d at 729; see also Ruckelhaus v. Monsanto Co., 467 U.S. 986, 1002 (1984).

Viken's complaint identifies the following information as comprising its trade secret:

HBI-120 Confidential and Trade Secret Information includes the design files, operating characteristics, and physical optimization constraints for the device; it also includes the strategic plan for the HBI-120 and for potential modifications, improvements and design changes [including] characteristics of the x-ray anode, x-ray shielding material (alloy), and source detector geometry.

Defendants respond that such information is not a trade secret because it is readily ascertainable from publicly accessible features of Viken's HBI-120. Indeed, at the preliminary injunction stage, the Court recognized that sworn affidavits of experts in the field stated that the following features are generally known in the industry and thus likely do not amount to trade secrets: 1) size, 2) shape, 3) energy, 4) power and 5) weight of a handheld x-ray backscatter device and the use of 6) an x-ray tube, 7) a scanning method, 8) a shielding element and 9) software to translate the radiation pulses into images.

Nevertheless, plaintiff has plausibly alleged the existence of a trade secret. In addition to the listed physical characteristics of the HBI-120, plaintiff identifies certain information undisclosed to the public,

such as information regarding the iterative development process, alternative or incorrect solutions and developmental "dead ends". Viken further contends that its unique alloy composition cannot be determined precisely without the use of specialized advanced laboratory techniques and, even then, is difficult to determine with accuracy. Plaintiff also alleges that defendants misappropriated certain of its strategic product plans and potential product modifications.

Such undisclosed information, according to Viken, provided Bradshaw with an unfair advantage in developing a competing complex product, which defendants did in an "unusually concentrated timeline". Viken has, therefore, sufficiently stated a claim that its developed information constituted a trade secret.

With respect to the second element of trade secret misappropriation, plaintiff has sufficiently alleged that it took reasonable measures to protect its trade secrets, including restricting access to select employees and requiring employees to sign non-disclosure agreements.

As to the final element of trade secret misappropriation, Bradshaw contends that he did not obtain Viken's confidential and sensitive information by improper

means. To the contrary, and as described with respect to plaintiff's CFAA claim, the Complaint alleges that, in accessing Viken's sensitive information to further an interest adverse to it, Bradshaw either acted as an unauthorized competitor or exceeded his authorization as an employee.

Accordingly, plaintiff has alleged that defendants misappropriated its trade secrets under Massachusetts law and the DTSA.

3. Counts IV & V: Breach of Contract

Under Massachusetts law, to prove a breach of contract the plaintiff must demonstrate that: 1) "there was an agreement between the parties"; 2) "the agreement was supported by consideration"; 3) "the plaintiff was ready, willing, and able to perform his or her part of the contract"; 4) "the defendant committed a breach of the contract"; and 5) "the plaintiff suffered harm as a result". Bulwer v. Mount Auburn Hosp., 46 N.E.3d 24, 39 (Mass. 2016).

A valid contract in the form of the NDA clearly existed. The only dispute is whether Bradshaw breached the terms of that agreement. Viken submits that Bradshaw breached the NDA by, among other things, 1) failing to "keep in strictest confidence and trust" the proprietary and confidential information of

Viken; 2) retaining Viken's proprietary and confidential information upon termination of employment; and 3) recruiting or soliciting Viken employees to join a competitor.

Specifically, Viken avers that Bradshaw utilized proprietary and confidential information to "jumpstart the development" of the PX1. Viken also submits that certain combinations of design elements Bradshaw utilized to accelerate the development of Videray's competing product amounts to an improper use of proprietary and confidential information. Viken maintains that Bradshaw retained such information upon termination and that, while still employed by Viken, utilized proprietary and confidential employee records to entice other Viken employees to join Videray after its formation.

At the preliminary injunction stage, this Court noted that plaintiff's circumstantial evidence tending to show Bradshaw used protected information to compete with Viken during and after his employment was insufficient to warrant the "extraordinary remedy" of a preliminary injunction. Such allegations are sufficient, however, to survive a motion to dismiss.

4. Count VI: Breach of Duty of Loyalty

An employee who occupies a position of confidence and trust owes a "duty of loyalty" to his employer and must protect the

interests of his employer. Chelsea Industries, Inc. v. Gaffney, 449 N.E.2d 320, 326 (Mass. 1983). An employee is bound to act solely for his employer's benefit in all matters taken within the scope of his employment. Id. As a result, an employee may not actively compete with his employer during the tenure of his employment. Id.

Bradshaw submits that he merely prepared to compete with Viken by making certain logistical arrangements during his employment and, therefore, did not breach his duty of loyalty.

Plaintiff's complaint alleges that Bradshaw's conduct amounts to more than simply making logistical arrangements to prepare to compete. Indeed, Viken complains that Bradshaw actively competed by, among other things, 1) meeting with a potential investor to solicit funds; 2) soliciting a co-worker to join his new company; 3) collecting Viken customer contacts; 4) accessing confidential salary and equity information of Viken employees to entice co-workers to join his new company; 5) failing to share customer feedback related to product improvements and intending to utilize such information to improve his competing product; and 6) asking co-workers to help him collect confidential customer information.

Such allegations support a claim that Bradshaw actively competed with Viken during his employment and, therefore, breached his duty of loyalty.

5. Count VII: Tortious Interference with Contracts

A claim for tortious interference of contract requires the plaintiff to prove that 1) he had a contract with a third party, 2) the defendant induced the third party to break that contract, and 3) the plaintiff was harmed by the defendant's actions.

United Truck Leasing Corp. v. Geltman, 551 N.E.2d 20, 21 (Mass. 1990).

Viken claims Videray knowingly induced Bradshaw into breaching his contractual obligations to Viken. Defendants contend that plaintiff has failed to state a claim for tortious interference because Bradshaw, as owner and principal of Videray, is synonymous with his company. In other words, Bradshaw is so "closely identified" with Videray that he should not be considered a third party for purposes of a claim of tortious contractual interference. See Schinkel v. Maxi-Holding, Inc., 565 N.E.2d 1219, 1225 (Mass. App. Ct. 1991).

Whether an individual is synonymous with a corporation of which he is owner and principal is a question ill-suited for resolution at the motion to dismiss stage. Id. Such an inquiry requires fact-intensive investigation regarding whether an

individual "might be so closely identified with the corporation itself, and with its policies" that he cannot be considered a third party. Id.

Furthermore, as emphasized by plaintiff, the only citation proffered by defendants in support of their motion to dismiss plaintiff's claim of tortious interference holds that a principal, in some circumstances, may not be treated as a third party in relation to "corporate contracts." Schinkel, 565 N.E.2d at 1225-26. Here, plaintiff conversely alleges that the corporation tortiously interfered with a contract of its principal.

Accordingly, defendants' have not met their burden of demonstrating that plaintiff has failed to state a claim of tortious interference with contractual relations.

ORDER

For the forgoing reasons, the amended motion of defendants to dismiss all counts against them (Docket No. 26) is **DENIED**.

So ordered.

/s/ Nathaniel M. Gorton
Nathaniel M. Gorton
United States District Judge

Dated January 7, 2020