IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

iC-1 SOLUTIONS, LLC, *et al.*, Plaintiffs, v. RAPTORS EDGE SOLUTIONS LLC, *et al.*, Defendants.	Case No. 1:25-cv-00079

PLAINTIFFS' MEMORANDUM IN SUPPORT OF THEIR MOTION FOR PRELIMINARY INJUNCTION

Attison L. Barnes, III (VA Bar No. 30458)
Savanna L. Shuntich (VA Bar No. 89568)
Michelle B. Karavas (*pro hac vice forthcoming*)
Wiley Rein LLP
2050 M Street NW
Washington, DC 20036
Tel: (202) 719-7000
Fax: (202) 719-7049
abarnes@wiley.law
sshuntich@wiley.law
mkaravas@wiley.law

Counsel for Plaintiffs iC-1 Solutions, LLC and TLG Worldwide, LLC

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTRODUCTION

Plaintiffs iC-1 Solutions, LLC ("iC-1") and TLG Worldwide, LLC ("TLG") (collectively, "Plaintiffs"), by counsel, submit this Memorandum in Support of Their Motion for a Preliminary Injunction. For the reasons detailed below, Plaintiffs are entitled to a preliminary injunction against Defendants Bryce Wilkins ("Wilkins"), Andrew Fernandes ("Fernandes"), Raptors Edge Solutions LLC ("Raptors Edge"), and Defendants Does 1–10 (collectively, "Defendants").

PRELIMINARY STATEMENT OF EMERGENCY

Absent preliminary injunctive relief, Plaintiffs face imminent and continuing irreparable harm, including interference with and loss of customers and prospective customers, damage to reputation, and loss of their intellectual property and trade secrets. Defendants Wilkins and Fernandes are former iC-1 employees and, based on newly obtained evidence, Wilkins and Fernandes, in concert with Defendants Raptors Edge and Does 1–10, are at this time using Plaintiffs' confidential and proprietary information and trade secrets[1] (collectively, "Protected Information") to unlawfully compete with their former employer and TLG. *See* Decl. of Holton Yost ("Yost Decl."). *Id.* ¶ 18. Plaintiffs believe Wilkins and Fernandes acquired the source code and necessary configurations for Serpent, which Plaintiffs store on password-protected servers separate from other data (collectively, the "Serpent Servers"). *Id.* ¶¶ 4, 9. Wilkins and Fernandes are working in concert with Defendants Does 1–10 and formed and/or are using Raptors Edge to compete directly with Plaintiffs by offering a software product derivative of Plaintiff's Serpent.

[1] This includes, but is not limited to configurations and other data relating to Plaintiff's software platform ("Serpent" or the "Platform"), methods of operation, customer lists and data, customer communications, any source code and development of products and services, product and services information, marketing plans and strategies, cost and pricing materials, training materials, draft and final proposals, contracts, contract negotiations, financial information and projections, recruiting and staffing materials, personnel data, management information systems, utilization procedures and protocols, utilization review and quality assurance mechanisms and data, and any other communications and documents that Plaintiffs maintain as confidential.

Id. ¶¶ 18, 42, 48. At present, Defendants are brazenly pursuing Plaintiffs' clients, including attempting to usurp Plaintiffs' roles at customer training sessions and other events. *Id.* ¶¶ 39–46.

Plaintiffs also recently learned the extent to which Defendants are willing to go to carry out their scheme. Defendants devised and sought to implement a troubling scheme to disable iC-1's use of Serpent and thus tortiously interfere with iC-1's subcontract with Core One Solutions, LLC ("Core One") for an active government contract. *See* Yost Decl. ¶¶ 40–41. Incredibly, by their own words, Defendants were seeking to enlist Core One's participation in the scheme as they ***unlawfully sought to "trigger" a failure in Plaintiffs' deliverables to the government under a government contract***. *Id.* Defendants thus sought to sabotage devices to be delivered to the government for their own gain and to tortiously interfere with iC-1's relationship with Core One and reputation with the government customer. *Id*.

Plaintiffs have reason to believe that Defendants are engaging in further efforts to damage their businesses, including their systems or products, and have analyzed, including forensically analyzed, Wilkins and Fernandes's iC-1 issued devices.[2] *Id*. ¶ 28. Among other things, Plaintiffs learned in the last few days that Wilkins interfered with Plaintiffs' relationship with TLG's customer, the [redacted], by improperly soliciting work and secretly performing a training for [redacted] personnel in December 2024, the same training that he had been negotiating in October 2024, while still employed by iC-1. *Id*. ¶ 44. The [redacted] training sessions were a follow-on to work TLG performed for the [redacted] in December 2023 and July 2024 in [redacted]. *Id*. ¶ 45. Indeed, Wilkins, while he was still employed at iC-1, forecasted, in writing to Plaintiffs' management, that TLG would conduct the training in December 2024, after

[2] Due to BitLocker encryption, Plaintiffs were unable to collect any evidence from Fernandes's iC-1 issued computer. *Id.* ¶ 28.

which the customer contacted Wilkins for quotes from TLG. *Id*. Wilkins not only took the business and apparently performed the training in [redacted] in December 2024, but he also shamelessly used the same independent contractor that TLG contracted with for its training exercise for the [redacted] in June 2024. *Id*. Plaintiffs also obtained evidence in the last few days that Defendants are soliciting the [redacted], another TLG customer. *Id*. ¶ 46. Plaintiffs are concerned that Defendants will continue interfering with Plaintiffs' customers and using the stolen trade secrets, client data, training materials, and other voluminous files of Protected Information they removed from Plaintiffs around the time of their departures. *Id*. ¶ 47.

While Plaintiffs are still in the process of recovering data about Wilkins and Fernandes's activities, Plaintiffs have discovered that they are hindered in their ability to conduct effective analyses in part due to Wilkins's deliberate deletion of the files and user activity on his iC-1 issued laptop (the "iC-1 Laptop"). *Id*. ¶¶ 32–33. Based on the information received to date of a substantial theft of Protected Information and other concerning facts just obtained, Plaintiffs have no choice but to move for injunctive relief.

Also, Plaintiffs have learned that on Fernandes's last day of employment (August 30, 2024) and through September 19, 2024, he accessed large volumes of Protected Information in Serpent Servers. *Id*. ¶¶ 9, 24. Recently obtained logs from Serpent Servers (the "Logs") show Fernandes logged into Serpent Servers on August 30, September 2–6, September 9, September 11–13, and September 19, 2024. *Id*. Fernandes logged in with his username from his previously approved IP address. *Id.* Each of those days, he had 140–3,275 access events, totaling 12,606 access events. *Id*. Because the volume is so excessive and Logs show access events occurred seconds apart, it does not appear that Fernandes could have accessed the Protected Information manually. *Id*. ¶ 25. Rather, the large volume of Protected Information Fernandes accessed each day over the two-and-

a-half-week span evidences that he was using a software program to access the Protected Information. *Id*. Fernandes had no legitimate reason to access Serpent Servers or the Protected Information on Serpent Servers from August 30, through September 19, 2024, and could only be doing so to engage in the theft of Protected Information. *Id*. ¶¶ 24, 26.

The early results of the forensic analysis on the iC-1 Laptop are equally concerning. Wilkins's final day of employment with iC-1 was October 15, 2024. *Id*. ¶ 27. On his last day of employment, Wilkins deleted large volumes of files and browser cookies from the iC-1 Laptop, likely in an effort to conceal his nefarious activities. *Id*. ¶¶ 32–34, 35. Wilkins left only fourteen files on the iC-1 Laptop, all in the Downloads folder. *Id*. ¶ 33.

In addition, since Plaintiffs learned of the sabotage plot, they have uncovered evidence that Defendant Wilkins is planning to market a software product derived from Serpent to Core One and Core One's customer, the [redacted] ("[redacted]"). *Id*. ¶ 42. A Core One employee recently informed Holton Yost ("Yost"), the Chief Executive Officer ("CEO") of The Swift Group Holdings, LLC ("Swift"), that Wilkins had approached Core One about showcasing a new product that competes with Serpent to [redacted] and Core One at a [redacted] exercise in [redacted] this month. *Id*. ¶¶ 1, 42. With less than a month between Wilkins' departure from iC-1 and his announcement of the new product, Defendants could have only created the new product if it was derivative of Serpent which is only possible through theft of the Protected Information, specifically the Serpent source code and related integral Serpent configurations stored on the Serpent Servers. *Id*.

Furthermore, there is evidence Defendants are now pursuing Plaintiffs' other clients. *Id*. ¶¶ 39–46. Yost recently received an email from the [redacted] ("[redacted]") about re-conducting training TLG had previously provided to [redacted] in the past. *Id*. ¶ 43. The [redacted]

representative wrote, "[t]he purpose of this email is to understand the services that can be offered by Swift for a similar exercise in June 2025, noting there have been some recent structural changes to your organization." *Id.* No one on behalf of Plaintiffs or any other Swift subsidiary (collectively, "Swift Entities") had communicated with [redacted] about "structural changes." *Id.* ¶¶ 2, 43. It appears that Defendants also contacted [redacted] offering competing services and representing Plaintiffs as failed companies. *Id.* For all these reasons uncovered recently, Plaintiffs remain concerned that Defendants have used and continue using the Protected Information to (1) create a competitor to Serpent derived from Serpent, (2) to sell and market the competitive product derived from Serpent to entities, including Plaintiffs' current and prospective customers, and (3) continue interfering with the Swift Entities' businesses. *Id.* ¶¶ 18, 47.

Injunctive relief should be granted against Defendants because Plaintiffs can demonstrate the following: (1) that they will prevail on the merits of their claims; (2) that they face imminent threat of commercial harm through loss of customers, prospective customers, and the value of their intellectual property; (3) that their interests outweigh Defendants' interests; and (4) that the injunction will serve the public interest.

STATEMENT OF FACTS

I. Plaintiffs Develop Their Trade Secret Serpent

Plaintiffs are wholly-owned subsidiaries of Swift that provide information technology capabilities, third-party logistics, and nontraditional operations for the intelligence community. Yost Decl. ¶ 2. Plaintiffs leverage their strong ties to the intelligence community to win government contracts and subcontracts from the Department of Defense to develop cutting-edge software used in intelligence operations and to train military personnel on non-traditional military operations. *Id.* ¶ 3. Plaintiffs' customers also include other entities in the intelligence community and private companies that have need of their specialized products. *Id.* ¶ 2.

In or around the fall of 2021, Plaintiffs began developing Serpent, a Ubiquitous Technical Surveillance ("UTS") software platform that analyzes cellphone activity and inactivity to assess digital patterns and anomalies. *Id*. ¶ 4.

Among the iC-1 employees tasked to develop Serpent were Defendants Wilkins and Fernandes. *Id*. Wilkins joined iC-1 in 2021 as the Director of Non-Traditional Training Programs and was responsible for sales and developing requirements for the user interface of Serpent by working with the coding team to refine the Platform's capabilities. *Id*. ¶ 5. Defendant Fernandes joined iC-1 originally in 2018 and became the Director and Lead Architect and Developer for Serpent. *Id*. ¶ 6. In that role, Defendant Fernandes had access to all the source coding for the Platform. *Id*. During the onboarding process Defendant Fernandes signed an Employment Agreement with iC-1 with non-solicitation, non-competition, and confidentiality restrictions, among other requirements. *Id*. ¶ 7.

After Plaintiffs expended roughly $2,000,000.00 to design, create, and market the Platform, Serpent was completed in or around the end of 2022. *Id*. ¶ 8. Plaintiffs regard Serpent as their trade secret and make reasonable efforts to ensure that it remains confidential, including through: (1) storing and executing the Serpent source code and integral configurations on servers separate from other data; (2) password protecting those servers; (3) restricting access to employees with a "need to know" the information; (4) instituting strong confidentiality policies and agreements to stop employees from intentionally or unintentionally sharing the information; (5) including language in their purchase orders with customers guaranteeing that Plaintiffs retain ownership of Serpent and other intellectual property; (6) locking equipment in a controlled access storage room; and (7) monitoring facilities with video surveillance. *Id*. ¶ 9–11.

Serpent proved successful, and the contracts for training and services on Serpent have generated business for Plaintiffs to date, with Plaintiffs' clients including the [redacted], [redacted], and other intelligence community entities. *Id.* ¶ 12. One such contract is with Core One. *Id.* ¶ 13. In or about May 2019, Core One was awarded an Indefinite Delivery/Indefinite Quantity Training Contract ("[redacted] Contract") with the [redacted] ("[redacted]"). *Id.* Core One engaged iC-1 as a subcontractor through a succession of purchase orders to train [redacted] personnel on using Serpent loaded onto iC-1-issued cell phones ("Training Phones"). *Id.* In the field, Training Phones gather and transmit data to Serpent Servers. *Id.* The [redacted] Contract is set to be awarded in the spring of 2025 for a five-year term and proposals to the solicitation are due mid-February 2025. *Id.* ¶ 14.

During Wilkins's employment, iC-1 tasked him with gaining customers for Serpent. *Id.* ¶ 15. Wilkins interfaced with iC-1's customers on a regular basis, including Core One, and served as the primary point of contact for customers. *Id.* Later, when TLG entered into contracts with customers for training on Serpent, Wilkins served as TLG's point of contact for those customers and interfaced with them on a daily basis. *Id.* ¶ 16.

Fernandes demanded higher compensation based on Serpent's success. *Id.* ¶ 17. When Yost gave Fernandes and Wilkins the right to earn shares in Swift in the summer of 2024, Fernandes complained to Yost that his shares were not vesting fast enough. *Id.*

II. Wilkins and Fernandes Depart iC-1 and Establish Raptors Edge

Based on recently acquired information, Plaintiffs now believe that Wilkins and Fernandes got greedy and stole Serpent and other Protected Information from Plaintiffs. Yost Decl. ¶ 18. Plaintiffs further believe Wilkins and Fernandes, working in concert with others, have used and continue using the Protected Information to (1) create a competitor to Serpent derived from Serpent and (2) sell and market the competitive product derived from Serpent to entities—including

Plaintiffs' current and prospective customers—through Raptors Edge. *Id.*

Fernandes was the first to depart from iC-1. *Id.* ¶ 19. His final day of work with iC-1 was August 30, 2024, and Plaintiffs have discovered that the days prior were marked by a flurry of activity. *Id.* Three days before Fernandes left iC-1's employ, Wilkins provided Fernandes access to a folder called "Clients" stored on Plaintiffs' secure file storage platform, SharePoint. *Id.* ¶ 20. The "Clients" folder contains a sub-folder for all Plaintiffs' clients, each of which stores all of the records for that client, including trainings performed and financial information for each contract. *Id.* ¶ 21. It is the essential information needed for Plaintiffs to run their businesses. *Id.* Upon information and belief, Fernandes had no valid business reason to need access to this Protected Information three days before his departure from iC-1 unless he planned to use the information to directly compete with Plaintiffs. *Id.*

Plaintiffs have also learned that two days before Fernandes departed iC-1, Raptors Edge was formed in Delaware. *Id.* ¶ 22. Two weeks later, former TLG employee "Jay Wright" executed Raptors Edge's Application for a Certificate of Registration in Virginia. *Id.* Then, Raptors Edge registered with the Department of Defense's Commercial and Government Entity Program ("CAGE"). *Id* ¶ 23. The registration identified "John Wright" (John is Jay Wright's legal first name) as the point of contact but used Wilkins's cell phone number, revealing Wilkins's role with the company. *Id.*

Prior to his departure, Fernandes offered to assist Plaintiffs on an as needed basis after he left iC-1 in the event issues arose with Serpent. *Id.* ¶ 24. His services were not needed because Serpent ran smoothly. *Id.* Still, between August 30, 2024 (his final day with iC-1) and September 19, 2024, Fernandes proceeded to access thousands of files of Protected Information in Serpent Servers. *Id.* Plaintiffs believe that Fernandes accessed thousands of files of Protected Information

to steal the Protected Information underlying Serpent so that he could recreate Serpent at Raptors Edge. *Id.* ¶ 26.

On October 15, 2024, Wilkins abruptly submitted his resignation from iC-1 to Yost. *Id.* ¶ 27. Much like with Fernandes's departure, Plaintiffs have discovered that the days leading up to Wilkins's departure involved much activity to facilitate unlawful competition with iC-1. *Id.* Upon analysis of his devices, Wilkins appears to have saved Protected Information, including most of the training and financial files essential to Plaintiffs' businesses and Plaintiffs' client lists, to thumb drives. *Id.* ¶ 29. Wilkins did not have any business need to copy Protected Information onto these external drives to perform his duties for Plaintiffs. *Id.* Notably, the drives are not in Plaintiffs' possession, custody, or control. *Id.*

Further, in the days leading up to his resignation, Wilkins told iC-1's IT department that he wanted to restrict employee access to Plaintiffs' files on SharePoint. *Id.* ¶ 30. Wilkins instructed IT to open a new SharePoint site and delete all the files from the existing site, claiming that he would download all the files to his desktop and re-upload them to the new SharePoint site, where fewer employees would have access. *Id.* Wilkins never re-uploaded the majority of the files to the new SharePoint site. *Id.* The files Wilkins failed to upload were most of the financial and training files essential to Plaintiffs' businesses. *Id.* Presumably, Wilkins was attempting to destroy Plaintiffs' training businesses. *Id.*

Wilkins also viewed numerous Serpent-specific materials, including a PowerPoint presentation detailing financials for Plaintiffs' training projects and Serpent. *Id.* ¶ 36. Wilkins had no business need for Plaintiffs' businesses to view these files that afternoon. *Id.* Wilkins seems to have viewed these files to obtain the final information Raptors Edge needed to compete with Plaintiffs. *Id.*

Also during Wilkins's last afternoon of work, Plaintiffs recently discovered Wilkins created a training invoice for him and "Andrew" to provide a [redacted] training with Serpent in [redacted] the following week. *Id.* ¶ 31. In doing so, Wilkins looked up the mileage from Defendant Fernandes's home address to a [redacted] hotel. *Id.* Wilkins's invoice was for his own services and those of Fernandes, even though neither had authorization to conduct the training as a former and soon to be former iC-1 employee. *Id.*

That same final afternoon, in a likely effort to conceal his unlawful activities from Plaintiffs, Wilkins deleted all but fourteen files from the iC-1 Laptop, deleted his browser cookies from the iC-1 Laptop, and unsuccessfully tried recycling the cookies on the iC-1 Laptop. *Id.* ¶ ¶ 32–34.

After the above activity, Wilkins sent an email to Yost resigning from his position, in which he denied any knowledge of the circumstances of Fernandes's resignation or future professional plans and explained that he was resigning to tend to family matters and take some time off. *Id.* ¶ 37. This assertion could not have been further from the truth. *Id.*

III. Defendants Conspire to Sabotage Plaintiffs' Use of Serpent and Solicit Plaintiffs' Clients

Since Wilkins and Fernandes left their positions with iC-1, they have conspired with Defendants Raptors Edge and Does 1–10 and taken numerous actions to unlawfully compete with Plaintiffs for Defendants' own benefit. Yost Decl. ¶ 38.

Plaintiffs recently learned that shortly after departing iC-1, Wilkins contacted iC-1's customer representative, and Core One's CEO, Patrick Moniz ("Moniz"), via the Signal messaging platform about the possibility of replacing iC-1 as a subcontractor for a follow-on Serpent training effort. *Id.* ¶ 39. The October 21, 2024 Signal message Wilkins sent to Moniz contained the following communication:

> Once [redacted] [the then-current Serpent training exercise] is over, roughly 50 [redacted] [P]hones will need to be re-provisioned . . . Before [Core One] returns the [Training] [P]hones to the unit . . . **Andrew and I need access to them for a few hours to set various triggers to have them start failing. Simple supply chain attack** and this is assuming Swift can even re-provision them . . . which is doubtful.

Id. ¶ 40 (Emphasis added).

Plaintiffs believe that the "Andrew" referenced in Wilkins's Signal message is Andrew Fernandes, and that Fernandes and Wilkins intended to sabotage the Training Phones to undermine iC-1's reputation with [redacted], thereby positioning Raptors Edge to successfully win any subcontract stemming from the recompete of the [redacted] Contract in the summer of 2025. *Id*. ¶ 41.

Recently, a Core One employee notified Yost that Defendants plan to showcase a competitor to Serpent to [redacted] and Core One at an upcoming [redacted] training exercise in [redacted] in January of 2025. *Id*. ¶ 42. The only way Defendants could have realistically created a competitor to Serpent in such an abbreviated timeline is if it was derivative of Serpent which is only possible through theft of the Protected Information, specifically the Serpent source code and its related integral Serpent configurations stored on the Serpent Servers. *Id*. Indeed, Fernandes previously disclosed to his iC-1 colleagues during his employment that it would take anyone at least a year to catch up since Serpent was so far ahead of the competition. *Id*.

As stated above, there is substantial evidence that Defendants are soliciting other clients of Plaintiffs, including the [redacted], [redacted], and [redacted] and that Wilkins has performed a training for the [redacted] that TLG was originally to perform. *Id*. ¶¶ 39–46.

Absent preliminary injunctive relief, Defendants will continue to take further measures to cause irreparable harm to Plaintiffs and to unlawfully undermine the Swift Entities' businesses. Given the amount of Protected Information in Defendants' possession, allowing Defendants to continue their activities will irreparably harm Plaintiffs.

LEGAL STANDARD

I. Standard for Injunctive Relief

The Court may grant a preliminary injunction when a party demonstrates "[1] that [it] is likely to succeed on the merits, [2] that [it] is likely to suffer irreparable harm in the absence of preliminary relief, [3] that the balance of equities tips in [its] favor, and [4] that an injunction is in the public interest." *Centro Tepeyac v. Montgomery Cnty.*, 722 F.3d 184, 188 (4th Cir. 2013) (en banc) (quoting *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008)); *see also Newsom ex rel. Newsom v. Albemarle Cnty. Sch. Bd.*, 354 F.3d 249, 254 (4th Cir. 2003) (vacating denial of preliminary injunction). Where multiple causes of action are alleged at once the plaintiff must only show likelihood of success on one claim to justify injunctive relief. *See Audio-Video Grp., LLC v. Green*, No. 14-169 (JCC/TCB), 2014 WL 793535 at *2 (E.D. Va. Feb. 26, 2014); *see also Nabisco Brands, Inc. v. Conusa Corp*, 892 F.2d 74 (4th Cir. 1989) (a showing of entitlement to preliminary injunctive relief with respect to any claim obviates the necessity to consider any other).

Additionally, injunctive relief is specifically authorized by statute under the Defend Trade Secrets Act, 18 U.S.C. § 1836 ("In a civil action brought under this subsection with respect to the misappropriation of a trade secret, a court may grant an injunction to prevent any actual or threatened misappropriation [of trade secrets] . . . on such terms as the court deems reasonable . . . ."); Virginia Statutory Business Conspiracy, Va. Code § 18.2-500 ("Whenever a person shall duly file a civil action . . . praying that such party defendant be restrained and enjoined from continuing the acts complained of, such court shall have jurisdiction . . . to issue injunctions pendente lite and permanent injunctions . . . ."); and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g) ("Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain . . . injunctive relief or other equitable relief."). Finally, Fernandes's Employment Agreement authorizes injunctive relief for breaches or

threatened breaches of the Employment Agreement's non-compete restrictions.

ARGUMENT

Plaintiffs' Motion for a Preliminary Injunction should be granted because (1) Plaintiffs can demonstrate that they are substantially likely to succeed on the merits of their claims, (2) Plaintiffs will suffer irreparable harm if not granted a preliminary injunction, (3) the balance of equities weigh in Plaintiffs' favor, and (4) an injunction is in the public interest.

I. Plaintiffs Are Substantially Likely to Succeed on the Merits

The law only requires that one of Plaintiffs' claims be substantially likely to succeed on the merits for the first factor in the preliminary injunction analysis to weigh in Plaintiffs' favor. *See Audio-Video Grp., LLC*, No. 1:14-cv-169-JCC-TCB, 2014 WL 793535 at *2. Nevertheless, Plaintiffs iC-1 and TLG are substantially likely to prevail on the following multiple counts of the Complaint: (1) violation of the Defend Trade Secrets Act; (2) violation of the Computer Fraud and Abuse Act; (3) breach of the duty of loyalty; (4) breach of Defendant Fernandes's Employment Agreement; (5) violation of the Virginia Business Conspiracy statute; and (6) tortious interference with contract and business expectancy. Each is discussed separately, below.

A. Substantial Likelihood of Success on Plaintiffs' Defend Trade Secrets Act Claims

Plaintiffs can show a substantial likelihood of success on their Defend Trade Secrets Act ("DTSA") claim due to Defendants' misappropriation of Plaintiffs' trade secret Serpent. A DTSA claim has three elements, requiring that the plaintiff demonstrate "(1) the existence of a trade secret, (2) the trade secret's misappropriation, and (3) that the trade secret implicates interstate or foreign commerce." *dmarcian, Inc. v. dmarcian Eur. BV*, 60 F.4th 119, 141 (4th Cir. 2023) (citing *Oakwood Labs. LLC v. Thanoo*, 999 F.3d 892, 905 (3d Cir. 2021)).

To meet the first element of a DTSA claim, the information the plaintiff seeks to protect

must meet the statutory definition of a "trade secret." The DTSA defines a trade secret as "all forms and types of financial, business, scientific, technical, economic, or engineering information, including . . . program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes . . . [where] . . . the owner thereof has taken reasonable measures to keep such information secret." 18 U.S.C. § 1839(3). Demonstrating the existence of a trade secret also requires a showing that "the information derives independent economic value . . . from [it] not being generally known to, and not being readily ascertainable through proper means." *Id.*

To meet the second element of a DTSA claim, the plaintiff must demonstrate one or more of several types of misappropriation defined under the law. For example, it is misappropriation when a person acquires a trade secret knowing or having reason to know "that the trade secret was acquired by improper means." *Id*. § 1839(5). Improper means "includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means." *Id*. § 1839(6).

Misappropriation also takes place when an individual discloses or uses a trade secret that was acquired by improper means without consent, or when "at the time of disclosure or use, [the person] knew or had reason to know that" (1) the information came from someone who acquired the trade secret through improper means; (2) the information was "acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret"; or (3) the information came from a person who owed a duty to the plaintiff "to maintain the secrecy of the trade secret or limit the use of the trade secret." *Id*. § 1839(5).

Element 1 – Serpent is a Trade Secret

Serpent meets the definition of a trade secret as a program or code where "the owner . . . has taken reasonable measures to keep such information secret," and that the owner "derives

independent economic value . . . from [it] not being generally known to, and not being readily ascertainable through proper means." 18 U.S.C. § 1839(3).

Plaintiffs made diligent efforts to maintain the secrecy of Serpent by: (1) storing and executing the source code and integral configurations on servers separate from other data; (2) password protecting those servers; (3) restricting access to employees with a "need to know" the information; (4) instituting strong confidentiality policies and agreements to stop employees from intentionally or unintentionally sharing the information; (5) including language in their purchase orders with customers guaranteeing that Plaintiffs retained ownership of Serpent and other intellectual property; (6) locking equipment in a controlled access storage room; and (7) monitoring facilities with video surveillance.

Plaintiffs have derived economic value from Serpent not "being generally known" to its competitors. Serpent is a unique product in the intelligence space and Plaintiffs anticipate that Serpent will continue to be a success on existing and new contracts for clients and future clients. Were Defendants permitted to introduce a competing product into the market derived from Plaintiffs' trade secrets, it would irreparably harm Plaintiffs and the Platform.

Element 2 – Defendants Misappropriated Serpent

Plaintiffs can demonstrate that Fernandes and Wilkins, working in concert with Raptors Edge and Defendants Does 1–10, misappropriated Serpent in multiple ways. First, Fernandes acquired Serpent through improper means and used the trade secret to create a competitive product derived from Serpent for Raptors Edge, which Defendants are now marketing to Plaintiffs' customers. 18 U.S.C. § 1839(5)(A) (Explaining that misappropriation includes "acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means"); *id*. § 1839(5)(B) (Misappropriation includes "disclosure or use of

a trade secret of another without express or implied consent by a person who—(i) used improper means to acquire knowledge of the trade secret.").

Fernandes's means were improper because upon information and belief he stole Serpent's source code and the associated configurations necessary to run the application. Even if Fernandes previously had access to Serpent while working for Plaintiffs, that does not extend to using the trade secret for other purposes, particularly to compete with Plaintiffs. *See, e.g.*, *dmarcian, Inc.*, 60 F.4th at 141 (Defendant's license to use plaintiff's source code in Europe and Africa did not extend to competing with Plaintiff in the United States.).

Fernandes's actions additionally constituted misappropriation of Serpent because at the time he disclosed and used Serpent he was under a duty to iC-1 pursuant to his Employment Agreement and the common law duty of loyalty "to maintain the secrecy of the trade secret or limit the use of the trade secret." 18 U.S.C. § 1839(5)(B)(ii)(III). Additionally, he "acquired [Serpent] under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret." *Id*. § 1839(5)(B)(ii)(II).

Moreover, Wilkins, on his own behalf and of behalf of Raptors Edge, misappropriated Serpent when he downloaded Protected Information related to Serpent to thumb drives and shared the "Clients" folder with Fernandes through improper means. Wilkins used improper means to acquire the information because he deceived Plaintiffs into believing that he was a loyal employee of iC-1 using his access to Plaintiffs' systems for Plaintiffs' benefit. Instead, Wilkins used his access to acquire Protected Information in order to establish a direct competitor to Plaintiffs. Moreover, Wilkins misappropriated Serpent because he was under the common law duty of loyalty as an iC-1 employee "to maintain the secrecy of the trade secret or limit the use of the trade secret." *Id*. § 1839(5)(B)(ii)(III). Additionally, he "acquired [Serpent] under circumstances giving rise to

a duty to maintain the secrecy of the trade secret or limit the use of the trade secret." *Id.* § 1839(5)(B)(ii)(II).

Element 3 – Serpent Implicates Interstate Commerce

Plaintiffs can establish element three of a DTSA claim "that the trade secret implicates interstate or foreign commerce." *dmarcian, Inc.*, 60 F.4th at 141. Plaintiffs conduct trainings on Serpent around the United States. Thus, Plaintiffs have demonstrated that their Defend Trade Secrets Act claim is substantially likely to succeed on the merits.

B. Substantial Likelihood of Success of Plaintiffs' Computer Fraud and Abuse Act Claims

Plaintiffs have a substantial likelihood of success on the merits of their Computer Fraud and Abuse Act claims against all Defendants. The Computer Fraud and Abuse Act ("CFAA") is a federal criminal statute that makes various types of hacking and other digital malfeasance unlawful. The Fourth Circuit has explained that though the CFAA is "primarily a criminal statute designed to combat hacking . . . Nevertheless, it permits a private party 'who suffers damage or loss by reason of a violation of [the statute]' to bring a civil action 'to obtain compensatory damages and injunctive relief or other equitable relief.'" *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 201 (4th Cir. 2012) (quoting 18 U.S.C. § 1030(g) (internal citations omitted)).

The CFAA defines a computer as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device . . . ." 18 U.S.C. § 1030(e)(1). Protected computers are those, *inter alia*, which are "used in or affecting interstate or foreign commerce or communication." *Id.*

§ 1030(e)(2)(B). The Serpent Servers and the Training Phones both satisfy the definition of protected computers under the CFAA.

The following three violations of the CFAA are relevant for purposes of this motion:

First, it is a violation of the CFAA when an individual "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . ." *Id.* § 1030(a)(2)(C).

Second, it is a violation of the CFAA when an individual "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period . . . ." *Id.* § 1030(a)(4).

Third, it is a violation of the CFAA when an individual does any of the following:

> (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
>
> (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
>
> (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

Id. § 1030 (a)(5).

Courts in this jurisdiction have interpreted the "without authorization clause of the CFAA . . . to defend computers against outside hackers—those who access a computer without any permission at all," and the "exceeds authorized access clause . . . to defend computers against inside hackers—those who access a computer with permission, but then exceed the parameters of authorized access by entering an area of the computer to which that authorization does not extend."

Carfax, Inc. v. Accu-Trade, LLC, No. 21-361, 2022 WL 657976, at *11 (E.D. Va. Mar. 4, 2022) (internal citations and quotations omitted). The CFAA obligates plaintiffs to demonstrate $5,000 or more in loss or damages. *See Maplebear Inc. v. Does*, No. 1:21-CV-00474AJTIDD, 2022 WL 1837935, at *4 (E.D. Va. Apr. 6, 2022), report and recommendation adopted sub nom. *Maplebear Inc. v. Does 1-2*, No. 1-21-CV-00474AJTIDD, 2022 WL 2900625 (E.D. Va. May 26, 2022) (citing *Sprint Nextel Corp. v. Simple Cell, Inc.*, No. 13-617, 2013 WL 3776933, at *7 (D. Md. July 17, 2013)). Loss is defined in the CFAA 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 interruption of service." 18 U.S.C. § 1030(e)(11). "This broadly worded provision plainly contemplates consequential damages of . . . costs incurred as part of the response to a CFAA violation, including the investigation of an offense." *A.V. v. Iparadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009) (citations omitted). Moreover, Plaintiffs are permitted to "[a]ggregate multiple intrusions or violations for the purpose of satisfying the $5,000 threshold." *Maplebear*, 2022 WL 1837935, at *4 (citing *Sprint Nextel Corp.*, 2013 WL 3776933, at *7).

As detailed below, Defendants have violated the CFAA in multiple ways. Fernandes violated the CFAA when he exceeded his authorized access to the Serpent Servers and obtained Protected Information related to Serpent. *See* 18 U.S.C. § 1030 (a)(2)(C) (It is unlawful when an individual "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."). Additionally, Fernandes violated the CFAA by exceeding his authorized access to the protected computer containing the Serpent Servers and thereby "furthered the intended fraud and obtain[ed]" something of value in

the form of the Protected Information underlying Serpent. 18 U.S.C. § 1030(a)(4). Fernandes's acts were fraudulent because he had represented to iC-1 that he wanted to retain access to the Serpent Servers to assist rather than to abscond with Protected Information.

Both violations require a showing that Fernandes exceeded authorized access to a protected computer. As set forth above, Fernandes accessed the Serpent Servers for roughly a two-and-a-half-week period after he was no longer an employee of iC-1. Upon information and belief, as a former employee, Fernandes exceeded his authorized access to the Serpent Servers when he viewed and downloaded large quantities of files after August 30, 2024. Thus, Fernandes exceeded "the parameters of [his] authorized access by entering an area of the computer to which that authorization d[id] not extend." *Carfax, Inc.*, 2022 WL 657976, at *11. Wilkins and Raptors Edge are liable under the CFAA for conspiring with Fernandes and Defendants Does 1–10 to commit these violations. *See* 18 U.S.C. § 1030(b) (making it unlawful to conspire to commit an offense under the CFAA).

Finally, both Fernandes and Wilkins violated the CFAA in conspiracy with each other and Defendants Does 1–10 and on Raptors Edge's behalf when they attempted to sabotage the Training Phones to cause the phones to malfunction during a [redacted] military exercise. In doing so Defendants violated 18 U.S.C. § 1030 (a)(5) which makes it unlawful to knowingly, intentionally, and without authorization cause the transmission of a program, information, code, or command to cause damage and loss to a Protected Computer. *See also* 18 U.S.C. § 1030(b) (making it unlawful to attempt to commit an offense under the CFAA).

Plaintiffs have incurred in excess of $5,000 in losses due to Defendants' violations through "costs incurred as part of the response to a CFAA violation" which includes *inter alia*, money spent on computer forensics in the "the investigation of an offense" and time spent by employees

determining the extent of Defendants' malfeasance, along with the value of the Protected Information. *Iparadigms, LLC*, 562 F.3d at 646.

Thus, Plaintiffs have demonstrated that their CFAA claims are substantially likely to succeed on the merits.

C. Substantial Likelihood of Success on Plaintiff iC-1's Breach of the Duty of Loyalty Claims

Plaintiff iC-1 can establish a substantial likelihood of success on its Virginia common law breach of the duty of loyalty claim against Wilkins and Fernandes. Both Wilkins and Fernandes breached their duty of loyalty to iC-1 by competing with iC-1 while active employees of iC-1 and continuing to compete with iC-1 after termination of their employment by leveraging information obtained as iC-1 employees. Wilkins and Fernandes are violating their duty of loyalty to iC-1 to this day and will continue doing so unless otherwise enjoined from their unlawful activity.

In Virginia, "an employee, including an employee-at-will, owes a fiduciary duty of loyalty to his employer during his employment." *Williams v. Dominion Tech. Partners, LLC*, 265 Va. 280 (2003). "Principally, an employee must not have 'misappropriated trade secrets, misused confidential information, [or] solicited an employer's clients or other employees prior to termination of employment.'" *Id.* at 291 (quoting *Feddeman & Co. v. Langan Assoc.*, 260 Va. 35, 42 (2000)). Importantly, "'termination does not automatically free a[n] . . . employee from his or her fiduciary obligations' if the action was 'founded on information gained during the relationship.'" *Tech Sys., Inc. v. Pyles*, 630 F. App'x 184, 187 (4th Cir. 2015) (internal quotation marks omitted) (quoting *Today Homes, Inc. v. Williams*, 272 Va. 462, 474 (2006)).

While employees of iC-1, Fernandes and Wilkins had a fiduciary duty of loyalty to the company which obligated them not to compete with their employer. Despite that duty, Wilkins and Fernandes repeatedly took actions adverse to iC-1's interest. These include but are not limited

to: (1) forming a direct competitor of iC-1 two days before Fernandes's last day with the company and over a month and a half before Wilkins's last day of October 15th; (2) Wilkins's misappropriation of iC-1's Protected Information in the lead up to his October 15th departure date; (3) Wilkins's creation of an invoice to conduct a training for [redacted] in [redacted] and attempt to perform the training without iC-1's authorization or involvement; (4) Wilkins's sharing of Plaintiffs' "Clients" file with Fernandes with the intent of using the Protected Information to solicit and poach iC-1's clients for Raptors Edge; and (5) Wilkins's subsequent deletion of all files from SharePoint necessary for Plaintiffs to run their businesses.

Now that Wilkins and Fernandes have left employment with iC-1, they continue to violate their duty of loyalty to iC-1 by taking actions "founded on information gained during the relationship." *Tech Sys., Inc.*, 630 F. App'x at 187 (quoting *Today Homes, Inc.*, 272 Va. at 474). Thus, it was a violation of the fiduciary duty of loyalty that Wilkins and Fernandes owed to iC-1 as former employees when they: (1) attempted to sabotage the Training Phones and undermine iC-1's relationship with Core One; (2) created a product derivative of Serpent using iC-1's Protected Information that was designed to compete with Serpent; and (3) by currently marketing the Serpent derived product directly to Core One and potentially other iC-1 customers.

Thus, Plaintiffs have demonstrated that their breach of the duty of loyalty claim is substantially likely to succeed on the merits.

D. Substantial Likelihood of Success on Plaintiff iC-1's Breach of Contract Claims against Fernandes

Plaintiff iC-1 has a substantial likelihood of success of prevailing on its breach of contract claim against Defendant Fernandes based on his flagrant violations of his Employment Agreement. In Virginia, "[t]he elements of a breach of contract action are (1) a legally enforceable obligation of a defendant to a plaintiff; (2) the defendant's violation or breach of that obligation; and (3)

injury or damage to the plaintiff caused by the breach of obligation." *Young-Allen v. Bank of Am., N.A.*, 298 Va. 462, 469 (2020) (quoting *Ramos v. Wells Fargo Bank, NA*, 289 Va. 321, 323 (2015)).

On September 10, 2018, Fernandes executed an Employment Agreement with iC-1 at the outset of his employment that contained certain restrictions, including reasonable post-employment restrictions. Fernandes has violated the Employment Agreement in a myriad of ways, but for the purposes of this Motion we focus on Section 8 (non-competition) because it entitles iC-1 "to a preliminary restraining order and injunction preventing [Fernandes] from violating its provisions" if he breaches or threatens to breach the provision. Under Section 8 of the Employment Agreement, it states as follows:

> At the end of the Employment Period, by expiration or termination, [Fernandes] may not engage, own, manage, control, operate, be employed by, participate in, or be connected with the ownership, management, operation, or control of a business that participates in direct-competition, on the same programs of [iC-1] for a period of 1 year.

Defendant Fernandes left his position with iC-1 at the end of August 2024 and remains bound by the one-year non-competition restriction. Upon information and belief, Fernandes has created a competitor to Serpent. iC-1 believes that Fernandes, in conjunction with his co-conspirators, is now marketing that product to iC-1's clients, including Core One, to provide services interfering with the iC-1's customer relationship, trade secrets, and proprietary information. As such, Fernandes is directly competing with iC-1 "on the same programs" in violation of his Employment Agreement.

For the reasons stated above, iC-1 has a substantial likelihood of success on its breach of contract claim against Defendant Fernandes and Fernandes should be preliminarily enjoined against future breaches.

E. Substantial Likelihood of Success on Plaintiffs' Virginia Business Conspiracy Claims

Plaintiffs can establish a substantial likelihood of success on the merits of their statutory business conspiracy claim. To succeed on a statutory business conspiracy claim in Virginia "a plaintiff must establish: '(1) a combination of two or more persons for the purpose of willfully and maliciously injuring plaintiff in his business[;] and (2) resulting damage to plaintiff.'" *Dunlap v. Cottman Transmission Sys., LLC*, 287 Va. 207, 214 (2014) (quoting *Allen Realty Corp. v. Holbert*, 227 Va. 441, 449 (1984)). Demonstrating malice requires "proof that the defendants acted intentionally, purposefully, and without lawful justification, and that such actions injured the plaintiff's business." *N. Va. Real Est., Inc. v. Martins*, 283 Va. 86, 110 (2012) (quoting *Dominion Tech. Partners, LLC.*, 265 Va. at 290).

"Because there can be no conspiracy to do an act that the law allows" the Virginia Supreme Court has "held that 'an allegation of conspiracy, whether criminal or civil, must at least allege an unlawful act or an unlawful purpose' to survive" dismissal. *Cottman Transmission Sys., LLC*, 287 Va. at 215 (quoting *Hechler Chevrolet, Inc. v. Gen. Motors Corp.*, 230 Va. 396, 402 (1985)). Put differently, "without proof of the underlying tort, there can be no conspiracy to commit the tort." *Adnet, Inc. v. Soni*, 66 F.4th 510, 521 (4th Cir. 2023) (internal quotations omitted).

As discussed above and in the Complaint, Defendants acted with malice in concert with one another to steal Plaintiffs' Protected Information, establish a direct competitor to Plaintiffs, sabotage Serpent, and harm Plaintiffs through theft of their goodwill and customers. Defendants took numerous unlawful acts in furtherance of the conspiracy, including violating the DTSA, the CFAA, the Virginia Computer Crimes Act, the Virginia Uniform Trade Secrets Act, their fiduciary duties of loyalty, Fernandes's Employment Agreement, and engaging in tortious interference with contract and business expectancy. As a consequence of Defendants' business conspiracy,

Plaintiffs have suffered harm through the loss of their valuable Protected Information and goodwill with customers, and costs incurred in completing forensics analyses of their computer systems to ensure the Protected Information is secured and that their technology cannot be sabotaged by Defendants.

In consequence, Plaintiffs have a substantial likelihood of success on their statutory business conspiracy claim.

F. Substantial Likelihood of Success on Plaintiffs' Tortious Interference with Contract and Business Expectancies Claim

Under Virginia law:

> a claim for tortious interference with contractual relations includes the following elements: (1) the existence of a valid contractual relationship or business expectancy; (2) knowledge of the relationship or expectancy on the part of the interferor; (3) intentional interference inducing or causing a breach or termination of the relationship or expectancy; and (4) resultant damage to the party whose relationship or expectancy has been disrupted.

USI Ins. Servs., LLC v. Ellis, No. 21-797, 2023 WL 2244677, at *4–5 (E.D. Va. Feb. 27, 2023) (citing *Schaecher v. Bouffault*, 290 Va. 83, 106 (2015)).

Upon information and belief, Defendants have tortiously interfered with iC-1's Purchase Order 0000072 with Core One and other business expectancies of iC-1 and TLG through: (1) Wilkins and Fernandes's attempt to sabotage the Training Phones; (2) approaching TLG's customer [redacted] and representing TLG as a failed company unable to provide [redacted] with the same services it previously provided; (3) approaching Core One and [redacted] about showcasing a competitor to Serpent at a [redacted] training exercise this month to replace iC-1 in the short term and when the [redacted] Contract is rebid in the summer of 2025; (4) soliciting TLG's customer, the [redacted]; and (5) by improperly soliciting work from TLG's customer the [redacted] and secretly performing a training for [redacted] personnel in December 2024 that was originally to be performed by TLG.

Defendants were well aware of iC-1's contract (Purchase Order 0000072) with Core One to provide training to [redacted] and iC-1's ongoing relationship with Core One having performed work under Purchase Order 0000072 and earlier agreements. Wilkins and Fernandes are also aware that the [redacted] Contract will be re-bid. Finally, Wilkins is aware of TLG's ongoing relationship with [redacted] as TLG's prior point of contact for clients.

If Defendants are not enjoined from tortiously interfering with Plaintiffs' contracts and business expectancies, Plaintiffs will suffer irreparable harm including loss of customers and future contracts with Core One and untold other clients. Thus, Plaintiffs have demonstrated that their tortious interference claim is substantially likely to succeed on the merits.

II. Plaintiffs Will Suffer Irreparable Harm

Plaintiffs will suffer irreparable harm if Defendants are not enjoined from their unlawful actions. iC-1 and TLG have spent many years developing their Protected Information for the work at issue in this matter. iC-1 has developed a reputation with [redacted] through its Serpent platform and Plaintiffs have cultivated and established valuable relationships with other customers that are now in jeopardy due to Defendants' actions. Moreover, Defendants' actions have caused significant disruptions to Plaintiffs' operations. For Defendants to continue illegally usurping Plaintiffs' Protected Information and stealing its assets would cause immediate irreparable harm to iC-1 and TLG, particularly given the Defendants' ongoing efforts to solicit Plaintiffs' customers.

As this Court stated recently "the Fourth Circuit has repeatedly recognized that [t]he threat of a permanent loss of costumers and the potential loss of goodwill . . . support a finding of irreparable harm." *M Corp. v. Infinitive, Inc.*, No. 24-1823, 2024 WL 4696132, at *7 (E.D. Va. Nov. 6, 2024) (quoting *Variable Annuity Life Ins. Co. v. Corinth*, 535 F. Supp. 3d 488, 517 (E.D. Va. 2021)). And "courts in this District have held that 'the likelihood of irreparable harm in

customer solicitation cases . . . is obvious' because '[c]ustomers cannot be unsolicited.'" *Id.* (quoting *Fid. Glob. Brokerage Grp., Inc. v. Gray*, No. 10-1255, 2010 WL 4646039, at *3 (E.D. Va. Nov. 9, 2010)). On a final note, "[g]enerally, the 'disclosure of trade secrets establishes immediate irreparable harm because a trade secret, once lost is, of course, lost forever.'" *Hampton Rds. Connector Partners v. Land to Sand Site Servs., Inc.*, No. 23-174, 2023 WL 8539536, at *10 (E.D. Va. Oct. 17, 2023) (quoting *Peraton, Inc. v. Raytheon Co.*, No. 17-979, 2017 WL 11501665, at *4 (E.D. Va. Nov. 7, 2017)).

III. The Threatened Injury to Plaintiffs Outweighs any Harm to Defendant

In light of the troubling facts involved in this matter, Defendants can show no legitimate interest that weighs against entry of the requested injunction. As this Court has stated in another matter, "Defendants would not suffer cognizable hardship because an injunction would require them to cease from engaging in illegal activities." *Microsoft Corp. v. Does*, No. 21-822, 2022 WL 18359421, at *5 (E.D. Va. Dec. 27, 2022), report and recommendation adopted, 2023 WL 289701 (E.D. Va. Jan. 18, 2023). Additionally, the balance of equities "strongly favors" granting injunctive relief "to foreclose [a party] from benefitting from [its] misappropriation of [another's] trade secrets." *Cap. One Fin. Corp. v. Sykes*, No. 20-763, 2021 WL 2903241, *14 (E.D. Va. July 9, 2021) (quoting *API Tech. Servs., LLC v. Francis*, No. 13-142, 2013 WL 12131381, at *3 (E.D. Va. Dec. 4, 2013)).

The requested injunction is of no consequence to Defendants when compared to the harm that Plaintiffs will suffer absent injunctive relief. An injunction only restores the *status quo*—the overriding purpose of preliminary injunctive relief. Thus, the balance of harm weighs highly in favor of Plaintiffs because they have far more to lose if Defendants are allowed to continue with the unlawful conduct.

IV. An Injunction Will Serve the Public Interest

The public interest weighs heavily in favor of a preliminary injunction because the public has a substantial interest in upholding the law and the enforcement of contracts. *See, e.g.*, *SDSE Networks, Inc. v. Mathur*, No. 1:22-cv-01024, 2022 WL 18109791, at *2 (E.D. Va. Sept. 15, 2022) ("Public interest favors protecting confidential business information and enforcing valid contracts."); *Prysmian Cables & Sys. USA, LLC v. Szymanski*, 573 F. Supp. 3d 1021, 1045 (D.S.C. 2021) ("[P]ublic interest favors enforcing laws protecting trade secrets and preventing unfair competition in the marketplace."). In addition, courts generally find that the public interest is served when a company's right to proprietary information is protected. *See e.g.*, *Capital One Fin. Corp.*, 2021 WL 2903241, at *15 ("The public has an interest in allowing companies like [plaintiff] to protect confidential information, to obtain temporary injunctive relief to enjoin any further breach or disclosure, and ultimately to avoid irreparable harm and the destruction of incentives to develop proprietary information.").

V. A Bond is Not Necessary in this Case

While Federal Rule of Civil Procedure 65(c) provides that the court may issue a preliminary injunction order only if the movant provides security in an amount the court deems proper, a court "retains the discretion to set the [Rule 65(c)] bond amount as it sees fit or waive the security requirement." *CACI, Inc. - Fed. v. United States Navy*, 674 F. Supp. 3d 257, 281 (E.D. Va. 2023).

To the extent that the Court determines security is required pursuant to Rule 65, any such bond should be *de minimis*. As noted in Rule 65(c), the security is only "in an amount that the court considers proper to pay the costs and damages sustained by a party found to have been wrongfully enjoined or restrained." Fed. R. Civ. P. 65(c); *see Hoechst Diafoil Co. v. Nan Ya Plastics Corp.*, 174 F.3d 411, 421 n.3 (4th Cir. 1999) ("Where the district court determines that

the risk of harm is remote, or that the circumstances otherwise warrant it, the court may fix the amount of the bond accordingly. In some circumstances, a nominal bond may suffice.").

Here, Defendants will not and cannot be damaged from an order enjoining the use or disclosure of the Protected Information, the solicitation of Plaintiffs' customers and current and former employees, or interference with Plaintiffs' contractual relations and business expectancies. Plaintiffs respectfully request that the Court, in its discretion, waive any bond or security in this case.

CONCLUSION

For the reasons set forth above, all four factors weigh in favor of granting Plaintiffs injunctive relief. Plaintiffs respectfully request that this Court grant their Motion for Preliminary Injunction and such further relief as the Court deems proper.

January 16, 2025

IC-1 SOLUTIONS, LLC AND TLG WORLDWIDE, LLC
By counsel

By: */s/ Attison L. Barnes, III*
Attison L. Barnes, III (VA Bar No. 30458)
Savanna L. Shuntich (VA Bar No. 89568)
Michelle B. Karavas (*pro hac vice forthcoming*)
Wiley Rein LLP
2050 M Street NW
Washington, DC 20036
Tel: (202) 719-7000
Fax: (202) 719-7049
abarnes@wiley.law
sshuntich@wiley.law
mkaravas@wiley.law
Counsel for Plaintiffs iC-1 Solutions, LLC and TLG Worldwide, LLC

CERTIFICATE OF SERVICE

I hereby certify that on January 16, 2025, the foregoing was served on Defendants by overnight mailing and emailing a copy thereof to:

Raptors Edge Solutions LLC
c/o Corporation Service Company
100 Shockoe Slip
Floor 1
Richmond, VA 23219
jwright236@gmail.com

Bryce Wilkins
6304 Shannon Ct
Warrenton, VA 20187
bryceallenwilkins@gmail.com

and

Andrew Fernandes
4201 Roberts Rd.
Fairfax, VA 22032
afernan4e@gmail.com

/s/ Attison L. Barnes, III
Attison L. Barnes, III