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

MICROSOFT CORPORATION,

Plaintiff,

v.

ARIAN YADEGARNIA, RICKY YUEN, and PHAT PHUNG TAN,

Defendants.

Civil Action No 1:24-cv-2323-MSN-WEF

REPORT AND RECOMMENDATION

This matter comes before the Court on Plaintiff Microsoft Corporation's ("Plaintiff" or "Microsoft") Motion for Default Judgment pursuant to Federal Rule of Civil Procedure 55. Dkt. No. 64. Plaintiff brought this action for injunctive and other relief against Defendants Arian Yadegarnia (Yadegarnia), Ricky Yuen (Yuen), and Phát Phùng Tấn (collectively "Defendants") pursuant to the Computer Fraud and Abuse Act ("CFAA") (18 U.S.C. § 1030); the Digital Millennium Copyright Act ("DMCA") (17 U.S.C. § 1201), the Lanham Act (15 U.S.C. § 1125(a), (c)); the Racketeer Influenced and Corrupt Organizations ("RICO") Act (18 U.S.C. § 1962(c)); and Virginia state law. In short, Plaintiff alleges that Defendants unlawfully accessed and misused Microsoft's Azure OpenAI Service and generative artificial intelligence ("AI") technology to create images depicting misogyny, non-consensual intimate images of celebrities, and other sexually explicit content. Dkt. No. 41.

Pursuant to 28 U.S.C. § 636(b)(1)(C), the undersigned United States Magistrate Judge has reviewed the record and the pleadings, and for the reasons that follow, recommends that

the Court **GRANT** Plaintiff's Motion for Default Judgment against each of the three Defendants and convert the preliminary injunction previously entered by the Court (Dkt. No. 38) into a permanent injunction as requested by Plaintiff (Dkt. Nos 64, 64-1).[1]

I. Standard of Review Under Federal Rule of Civil Procedure 55

Federal Rule of Civil Procedure 55 establishes a two-step process for obtaining a default judgment. First, the plaintiff must request that the Clerk of Court enter default when the defendant fails to "plead or otherwise defend." Fed. R. Civ. P. 55(a); *see also City of New York v. Mickalis Pawn Shop, LLC*, 645 F.3d 114, 128 (2d Cir. 2011). Such failure constitutes an admission of liability by the defendant. Once the Clerk of Court enters the defendant's default, the second step requires the plaintiff to apply to the court for a default judgment. This "converts the defendant's admission of liability into a final judgment that terminates the litigation and awards the plaintiff any relief to which the court decides it is entitled…." *Mickalis Pawn Shop, LLC*, 645 F.3d at 128; *see also Home Port Rentals, Inc. v. Ruben*, 957 F.2d 126, 133 (4th Cir. 1992). However, a default judgment is not automatically granted as a matter of right. Rather, "[a] court confronted with a motion for default judgment is required to exercise sound judicial discretion in determining whether the judgment should be entered…." *JTH Tax, Inc. v. Grabert*, 8 F. Supp. 3d 731, 736 (E.D. Va. 2014).

II. Procedural Background

On December 19, 2024, Plaintiff filed a Complaint against ten DOE Defendants alleging that they orchestrated a malicious scheme to misuse Microsoft systems and technology for improper and illegal purposes, including the unlawful generation of images depicting misogyny,

[1] The relevant filings before the Court include Plaintiff's Complaint ("Compl.") (Dkt. No. 1); Plaintiff's First Amended Complaint ("FAC") (Dkt. No. 41); Motion for Default Judgment and Brief in Support ("Mem. Supp.") (Dkt. No. 64); and all attachments and exhibits submitted with those filings.

non-consensual intimate images of celebrities, and other sexually explicit content, using Microsoft's Azure OpenAI Service. Dkt. No. 1. After obtaining discovery and further investigative information, Microsoft identified certain individuals previously sued as DOE defendants and filed a First Amended Complaint ("FAC") on February 28, 2025 against named Defendants Yadegarnia, Yuen, and Phát Phùng Tấn. Dkt. No. 41. The First Amended Complaint alleged the following five counts: a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA"), *id.* at ¶¶ 97-103; two violations of the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(1) and (a)(2) ("DMCA"), *id*. at ¶¶ 104-112, 113-118; false designation of origin under the Lanham Act, 15 U.S.C. § 1125(a), *id*. at ¶¶ 119-126; violations of the Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1964(c), *id.* at ¶¶ 127-146; common law trespass to chattels, *id.* at ¶¶ 147-152; and tortious interference, *id.* at ¶¶ 153-159.

In the First Amended Complaint, Plaintiff sought (1) a judgment in its favor; (2) a declaration that Defendants' conduct was willful and that they acted with fraud, malice, and oppression; (3) a preliminary and permanent injunction enjoining Defendants from engaging in harmful activity set forth in the First Amended Complaint and isolating and securing the infrastructure, including the domain and the software operating from and through the infrastructure, outside of the control of Defendants or their representatives or agents; (4) an award of actual damages proven at trial; (5) and disgorgement of Defendants' profits. FAC at 41.[2]

On the same day the Complaint was filed, Plaintiff sought an Application for an Emergency Ex Parte Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction (Dkt. No. 4) (the "Application"). Also on December 19, 2024, Plaintiff filed a Motion for Expedited Discovery to permit discovery narrowly tailored to identifying the DOE Defendants (Dkt. No. 11).

[2] Plaintiff now seeks only a permanent injunction and is foregoing all other potential relief. Dkt. No. 64.

Plaintiff then filed a Motion for Alternative Service to permit service against Does 1-10 via emails to Defendants' known email addresses (Dkt. No. 12). The undersigned held a hearing on both motions on December 20, 2024 (Dkt. No. 23) and granted both motions that same day (Dkt. Nos. 24, 25).

December 19, 2024, Plaintiff filed a Motion for Protective Order Temporarily Sealing Documents until execution of the Application (Dkt. No. 13), which the Court granted on December 20, 2024 (Dkt. No. 22). Also on December 20, 2024, the District Judge held a hearing on Plaintiff's Application (Dkt. No. 20) and entered an Order temporarily restraining Defendants, including persons in active concert or participation with Defendants, from (1) accessing without authorization the computers or software comprising Microsoft's Azure OpenAI Service, (2) sending malicious code to configure, deploy or operate the Azure Abuse Enterprise, (3) generating and sending harmful images bearing false indicia of sponsorship or approval by Microsoft; and (4) stealing information, money, or property from Plaintiff or Plaintiff's customers (Dkt. No. 21). The Order further directed that the website operators and domain registry of the profiles and domain names at issue redirect the domain names to secure servers through the Domain Name System ("DNS") and preserve all evidence that may be used to identify the Defendants using the domains, among other actions. *Id.* at 4. The Order set a hearing on the request for a preliminary injunction for January 10, 2025 and required Plaintiff to serve Defendants by any means authorized by law.

The Order set a bond in the amount of $25,000.00, which Plaintiff deposited with the Court on December 27, 2024 (Dkt. No. 28). On January 8, 2025, Plaintiff filed a Motion to Unseal Case and Notice of Service certifying that the Application had been executed and that the civil action may be immediately unsealed (Dkt. No. 33), which the Court granted on January 10, 2025 (Dkt. No. 35). On January 10, 2025, the Court held a hearing on Plaintiff's request for a preliminary

injunction (Dkt. No. 32), which the Court granted (Dkt. No. 38).

On February 27, 2025, Plaintiff filed a Motion for Leave to File Amended Complaint (Dkt. No. 39), which was granted that same day (Dkt. No. 40). Plaintiff filed the First Amended Complaint on February 28, 2025 (Dkt. No. 41). On March 13, 2025 the undersigned issued an Order directing Plaintiff to explain to the Court (1) how it intended to serve the summonses and FAC on Defendants; and (2) why such methods would be proper under Federal Rule of Civil Procedure 4 (Dkt. No. 43). On March 21, 2025, Plaintiff filed a Motion for Alternative Service of the FAC, including to Defendant Yadegarnia via her known email address and Defendant Tấn via the Hague Convention (Dkt. No. 44), which was granted on March 25, 2025 (Dkt. No. 45). On May 28, 2025, Plaintiff filed a Proof of Service to Defendant Yadegarnia via her known email address.

On September 17, 2025, Plaintiff filed a Rule 41(a)(1)(A)(i) dismissal of certain other Defendants originally named in this action, leaving only the Defaulting Defendants remaining (Dkt. No. 53). On October 1, 2025, after unsuccessful attempts to effect Hague Convention service on Defendants Yuen, and Tấn (Dkt. No. 55), Plaintiff moved for leave to effect alternative service on Defendants Yuen and Tấn (Dkt. No. 56), which the Court granted on October 3, 2025 (Dkt. No. 58). Thereafter, Plaintiff served Defendants Yuen and Tấn using known email addresses and filed a Certificate of Service on October 9, 2025 (Dkt. No. 59).

On November 25, 2025, Plaintiff moved for an entry of default judgment against Defendants Yadegarnia, Yuen, and Tấn (Dkt. No. 60), supported by a declaration of Robert L. Uriarte stating that Plaintiff properly served process on Defendants; however, Defendants failed to answer or otherwise respond to the Complaint (Dkt. No. 60-1). The Clerk of Court entered default against Defendants on December 1, 2025 (Dkt. No. 61). On February 17, 2026, Plaintiff

filed a Motion for a Default Judgment (Dkt. No. 64). The hearing on Plaintiff's Motion was held on March 6, 2026 at which counsel for Plaintiff appeared and Defendants failed to appear (Dkt. No. 68). A review of the record confirms that Defendants have never appeared in this case in any manner. The Court then took the Motion for a Default Judgment under advisement to issue this Report and Recommendation.

III. Service of Process

Before a court can render default judgment, it must be satisfied that the defaulting party has been properly served. Under Federal Rule of Civil Procedure 4, courts may order service of process on individuals in a foreign country by "means not prohibited by international agreement." *JFXD TRX Acq LLC v. Trx.Com*, Civil Action No. 1:23-cv-217 (CMH/LRV), 2023 U.S. Dist. LEXIS 238064, at *1-2 (E.D. Va. Apr. 3, 2023). Federal Rule of Civil Procedure 4(f) gives effect to the Hague Service Convention and generally requires a plaintiff to first attempt service by formal means on an individual located in a Hague Convention jurisdiction. *See, e.g., Banilla Games, Inc. v. Guangzhou Crazy Software Tech. Co., Ltd.*, Civil Action No. 3:23-CV-183 (RCY), 2023 U.S. Dist. LEXIS 202083, at *5 (E.D. Va. Nov. 9, 2023); *BP Prods. N. Am. v. Dagra*, 236 F.R.D. 270, 272 (E.D. Va. 2006).

In cases where Hague Convention service cannot be achieved through the exercise of reasonable diligence, court-ordered alternative service in a foreign country is acceptable under Rule 4(f)(3) "so long as diligent attempts have been made to locate the defendant and serve process by traditional means." *Id.*; *see also DAG Ammo Corp. v. KM Trade d.o.o.*, No. 3:21cv332 (DJN), 2021 U.S. Dist. LEXIS 257187, at *3 (E.D. Va. June 4, 2021) (email service authorized where plaintiff first "reasonably attempted to effectuate service" under Hague Convention).

To "fulfill due process requirements under Rule 4(f)(3), the Court must approve a method of service that is 'reasonably calculated' to give notice to defendant." *JFXD TRX Acq LLC v. Trx.Com*, Civil Action No. 1:23-cv-217 (CMH/LRV), 2023 U.S. Dist. LEXIS 238064, at *1-2 (E.D. Va. Apr. 3, 2023) (quoting *Mullane v. Cent. Hanover Bank & Trust Co.*, 339 U.S. 306, 314 (1950)). Where a plaintiff's reasonable effort to formally serve a defendant at a physical address has failed, courts commonly find that "service of process by electronic mail is authorized by and warranted under Rule 4(f)(3)." *Williams v. Advert. Sex L.L.C.*, 231 F.R.D. 483, 488 (N.D.W. Va. 2005); *see also Overstock.com, Inc. v. Visocky*, 1:17-CV-1331-LMB-TCB, 2018 WL 5075511, at *4 (E.D. Va. Aug. 23, 2018), *report and recommendation adopted*, 2018 WL 5046673 (E.D. Va. Oct. 17, 2018) (service via email on foreign defendant is "reasonably calculated" to provide notice).

Here, the record reflects that Plaintiff undertook substantial efforts to identify and serve Defendants. Plaintiff first moved for expedited discovery to identify the Doe Defendants (Dkt. No. 23) and for leave to effectuate alternative service on Doe Defendants via email to their known email addresses and emails to the abuse contacts for third-party internet service providers ("ISPs") whose services Defendants used to carry out the unlawful conduct alleged in the FAC (Dkt. No. 25). Following execution of the TRO on January 7, 2025 and sending out notice emails, Plaintiff also published and made available to Defendants a website hosting all case documents, https://www.noticeofpleadings.net/fizzdog/index.html.

With respect to Defendant Yadegarnia, Plaintiff moved for alternative service after determining that it could not identify a physical address for him but possessed multiple known email addresses associated with Yadegarnia (Dkt. No. 44). On March 25, 2026, the Court granted the motion and authorized service via Yadegarnia's known email addresses (Dkt. No.

45). Plaintiff thereafter filed a Certificate of Service confirming service of the summons and First Amended Complaint via those email addresses (Dkt. No. 51).

As to Defendants Yuen and Tấn, Plaintiff initially attempted to pursue Hague Convention service based on a belief that they resided in Hague Convention jurisdictions. However, despite investigative efforts, including the use of third-party investigators, Plaintiff was unable to identify valid physical addresses for either Yuen and Tấn. However, Plaintiff did identify active email addresses associated with each Defendant and moved for alternative service (Dkt. No. 56). The Court granted that motion and authorized service on Yuen or Tấn via their known email addresses. Plaintiff subsequently filed a Certificate of Service confirming that the summons, First Amended Complaint, TRO, and Preliminary Injunction were served on those Defendants via email (Dkt. No. 59).

Accordingly, the record establishes that Defendants were timely and properly served in compliance with the Federal Rules of Civil Procedure and the Court's orders authorizing alternative service.

IV. Jurisdiction

Before entering default judgment in this matter, the Court must have (1) subject-matter jurisdiction over the claims asserted and (2) personal jurisdiction over the Defendants.

First, the undersigned finds that this Court has proper subject-matter jurisdiction under 28 U.S.C. § 1331, which vests the United States district courts with exclusive original jurisdiction over cases involving federal claims. Plaintiff's claims under the DMCA, the Lanham Act, and the RICO Act each arise under federal law. *See Gunn v. Minton*, 568 U.S. 257 (2013) ("[A] case arises under federal law when federal law creates the cause of action asserted."). In addition, where the district court has original jurisdiction over an action, it also

has "supplemental jurisdiction over all other claims that are so related to claims in the action within such original jurisdiction that they form part of the same case or controversy . . . ." 28 U.S.C. § 1367. All claims in this case arise from the same scheme to infiltrate Microsoft's systems and misuse those systems to create harmful content. Accordingly, the Court may properly exercise supplemental jurisdiction over Plaintiff's state law claims. *See, e.g.*, FAC ¶¶ 1; 23 (jurisdictional allegations); ¶¶ 79-96 (core factual allegations); ¶¶ 97-159 (federal and state claims incorporating the same factual allegations).

Second, the undersigned finds that this Court has personal jurisdiction over Defendants. Federal due process permits personal jurisdiction where a defendant has "certain minimum contacts with [the forum state] such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice.'" *Int'l Shoe Co. v. Washington,* 326 U.S. 310, 316 (1945) (quoting *Milliken v. Meyer*, 311 U.S. 457, 463 (1940)). The Fourth Circuit has directed district courts to consider the following three factors in determining whether a court's exercise of personal jurisdiction comports with the Constitution's due process requirements: "(1) the extent to which the defendant purposefully availed itself of the privilege of conducting activities in the State; (2) whether the plaintiffs' claims arise out of those activities directed at the State; and (3) whether the exercise of personal jurisdiction would be constitutionally reasonable." *Dmarcian, Inc. v. Dmarcian Eur. BV*, 60 F.4th 119, 133 (4th Cir. 2022) (citing *UMG Recordings, Inc. v. Kurbanov*, 963 F.3d 344, 352 (4th Cir. 2020)).

The purposeful-availment prong "is not susceptible to a mechanical application" and requires a court to consider "a list of various nonexclusive factors" including whether the defendant reached into the State to solicit or initiate business; the defendant deliberately engaged in significant or long-term business activities in the State; and the nature, quality, and

extent of the parties' communications about the business being transacted. *Dmarcian, Inc*., 60 F.4th at 133.

First, the purposeful-availment factor weighs in favor of exercising personal jurisdiction. Although Defendants are not located in Virginia, they have deliberately availed themselves of this forum by operating online infrastructure tied to servers located in this District. Specifically, to carry out their scheme, Defendants utilized domains with top-level configurations that depend on computers located in Reston, Virginia, and an AWS IP address that geolocates to a physical server within the Commonwealth. FAC ¶ 24; Mem. Supp. at 19. The undersigned takes judicial notice of the fact that Reston, Virginia falls within the Eastern District of Virginia. In addition, the two principal domains used by Defendants ("rentry.org/de3u" and "aitism.net") are administered by Virginia-based entities and rely, in part, on DNS servers located in Virginia. FAC ¶ 24.

Moreover, the default repository for the infringing images bearing Plaintiff's trademarks was an AWS server with an IP address geolocated to Virginia. FAC ¶¶ 80, 94–96. Defendants acted with knowledge that their conduct would be effectuated through Virginia-based computer systems and would cause harm to Plaintiff, its customers, and others within Virginia and the United States. FAC ¶ 25. Accordingly, Defendants' contacts with this forum reflect deliberate actions and an intent to carry out their business from within the state, which is sufficient to satisfy the purposeful-availment prong.

Second, Plaintiff's claims clearly arise out of activities directed at Virginia. Courts in this district have found that where affected computers are located within the district, and when a defendant's intentional acts cause those computers to affect the harms complained of, jurisdiction is appropriate. *See Bright Imperial Ltd. v. RT MediaSolutions S.R.L*., 2012 U.S.

Dist. LEXIS 70000, at *23 (E.D. Va. May 18, 2012). Here, Plaintiff's claims all arise from Defendants' use of the de3u software and the oai reverse proxy to gain unauthorized access to Microsoft's systems and generate harmful images for delivery to and through computers in Virginia. Mem. Supp. at 13.

Lastly, exercising personal jurisdiction in this district is constitutionally reasonable. Because Defendants' conduct was directly connected to the infrastructure located in Virginia, it is not necessary that Defendants be physically present in the forum for jurisdiction to comport with "traditional notions of fair play and substantial justice." *Bright Imperial Ltd.*, 2012 U.S. Dist. LEXIS 70000, at *39–40. To the contrary, it would undermine "traditional notions of fair play and substantial justice" to permit Defendants to avoid accountability merely because aspects of their conduct occurred abroad. As courts have recognized, the evolving nature of internet-based technologies enables foreign actors to cause direct and substantial effects within the United States, and such actors should not be permitted to evade the reach of the court's authority on that basis alone. *Id.*

V. Venue

Before entering default judgment against Defendants, the Court must be satisfied that venue is proper in this judicial district. Here, venue is proper pursuant to 28 U.S.C. § 1391(b) because, as discussed above, a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this judicial district, as well as a substantial part of the property that is the subject of Plaintiff's claims is situated in this district, and a substantial part of the harm caused by defendants has occurred in this judicial district. FAC ¶¶ 24-25, 80, 94–96. Venue is also proper under 28 U.S.C. § 1391(c) because Defendants are subject to personal jurisdiction in this judicial district.

VI. Defendants' Liability

On a motion for default judgment, the defendant in default is deemed to have admitted the complaint's non-conclusory "well-pleaded allegations of fact" and the Court must evaluate whether the complaint "states a claim upon which relief can be granted" by applying the standards used in motions to dismiss under Federal Rule of Civil Procedure 12(b)(6). *See GlobalSantaFe Corp. v. Globalsantafe.com*, 250 F. Supp. 2d 610, 613 n.3 (E.D. Va. 2003); *Grabert*, 8 F. Supp. 3d at 736, 739 (citing *Ryan v. Homecomings Fin. Network*, 253 F.3d 778, 780 (4th Cir. 2001)); *see* also *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (complaint must contain sufficient factual matter to state a claim to relief that is plausible on its face); *Burbach Broad Co. of Delaware v. Elkins Radio Corp*., 278 F.3d 401, 406 (4th Cir. 2002) (court will "assume the facts alleged in the complaint are true and draw all reasonable factual inferences in [the plaintiff's] favor"). "Where a complaint offers only 'labels and conclusions' or 'naked assertion[s] devoid of further factual enhancement,' the allegations therein are not well-pleaded and, consistent with the Court's discretion to grant default judgment, relief should be denied." *Vasquez-Padilla v. Medco Properties, LLC*, Civ. No. PX-16-3740, 2017 WL 4747063, at *2 (D. Md. Oct. 20, 2017) (collecting cases) (citations omitted).

1. *Plaintiff's Well-Pleaded Allegations of Fact*

The undersigned finds the following facts to have been properly pleaded and therefore deemed admitted.

As noted above, this case arises from Defendants' use of Microsoft's Azure OpenAI Service and generative artificial intelligence ("AI") technology for improper and unlawful purposes, including the creation of images depicting misogyny, non-consensual intimate images of celebrities, and other sexually explicit content. FAC ¶¶ 1–2, 24, 79.

A. The Parties

Defendant Yadegarnia is a natural person with access to and control over instrumentalities used in connection with the violations of law described in the First Amended Complaint, including the website located at "rentry.org/de3u," the source code repositories located at "github.com/notfiz/de3u," and stolen Azure API keys and other Microsoft customer authentication information. FAC ¶ 4. To Plaintiff's knowledge, Defendant Yadegarnia resides in the Islamic Republic of Iran. *Id.*

Defendant Yuen is a natural person with access to instrumentalities used in connection with violations of law alleged in the First Amended Complaint, including proxy domains and stolen customer credentials. FAC ¶ 7. To Plaintiff's knowledge, Yuen resides in the Hong Kong Special Administrative Region of the People's Republic of China. *Id.* Yuen's oai-reverse-proxy code is maintained in a GitHub repository located at the URL: https://github.com/cg-dot/oai-reverse-proxy. *Id.*

Defendant Tấn is a natural person with access to and control over instrumentalities used in connection with the violations of law alleged in the First Amended Complaint, including proxy domains, stolen customer credentials, and an implementation of the oai-reverse-proxy designed to leverage Microsoft's Azure OpenAI Service and several other companies' generative AI services. FAC ¶ 9. To Plaintiff's knowledge, Tấn resides in the Socialist Republic of Vietnam. *Id.*

Plaintiff Microsoft Corporation is a Washington corporation and a provider of technology products and services, including software, internet services, websites, and email platforms. FAC ¶ 3.

B. Microsoft's AI Services and Safeguards

Microsoft offers certain AI products, which generally refers to software designed to replicate human intellectual capabilities. FAC ¶ 30. Beginning in 2019, Microsoft entered into a multiyear partnership with OpenAI to advance the development and deployment of AI technologies. FAC ¶ 31. OpenAI's models are trained on Microsoft infrastructure and deployed through Azure to power various products, including GitHub Copilot, DALL·E, and ChatGPT. *Id.*

Of particular relevance here, DALL·E is an AI system that can create realistic images from a description in natural language. FAC ¶ 34. DALL·E has several built-in safety controls in place. For example, OpenAI has "limited the ability for DALL·E to generate violent, hate, or adult images by removing the most explicit content from DALL-E training data." FAC ¶ 35. OpenAI also has a content policy that does not allow users to "generate violent, adult, or political content, among other categories" and prevents users from generating images if the safety controls "identify text prompts and image uploads that may violate" company policy. *Id.*

In addition, Microsoft's Azure-based integration of DALL·E adds further layers of safety and security. FAC ¶ 36. First, the Microsoft Azure OpenAI Service is made available to customers pursuant to the terms governing their subscriptions to Microsoft Azure Services, including the Product Terms for Microsoft Azure Services. FAC ¶ 48. To access Azure services, a user must first create an Azure account and user profile and agree to the Microsoft Customer Agreement. FAC ¶ 48. That agreement prohibits users, among other things, from: (i) "reverse engineer[ing], decompil[ing], or disassembl[ing] any Product or Services Deliverable, or attempt[ing] to do so (except where applicable law permits despite this

limitation)"; (ii) "install[ing] or us[ing] non-Microsoft software or technology in any way that would subject Microsoft's intellectual property or technology to any other license terms"; and (iii) "work[ing] around any technical limitations in a Product or Services Deliverable or restrictions in Product documentation." FAC ¶ 48.

Second, Microsoft has established detailed standards governing responsible AI use. FAC ¶ 32. Its Generative AI Services Code of Conduct imposes requirements on customers to implement safeguards such as human oversight, input limitations, and transparency measures. FAC ¶ 53. The Code of Conduct also prohibits content that "describes, features, or promotes sexual exploitation or abuse, whether or not prohibited by law." FAC ¶ 56. Microsoft further prohibits "the creation of erotic, pornographic, or otherwise sexually explicit content." *Id.* This includes "sexually suggestive content, depictions of sexual activity, and fetish content. Microsoft prohibits content that attacks, denigrates, intimidates, degrades, targets, or excludes individuals or groups on the basis of traits such as actual or perceived race, ethnicity, national origin, gender, gender identity, sexual orientation, religious affiliation, age, disability status, caste, or any other characteristic that is associated with systemic prejudice or marginalization." *Id.* The Code of Conduct prohibits content that targets "individual(s) or group(s) with threats, intimidation, insults, degrading or demeaning language or images, promotion of physical harm, or other abusive behavior such as stalking." *Id*.

Third, Microsoft has implemented technical safeguards, including content filtering and abuse-detection systems integrated into Azure OpenAI services. FAC ¶ 60. These systems analyze both prompts and outputs to detect harmful content across categories such as hate, sexual content, violence, and self-harm. FAC ¶ 61. In addition, Azure OpenAI services employ abuse-monitoring mechanisms to identify patterns suggesting misuse of the software or

violations of applicable terms. FAC ¶ 66. These technical safeguards, together with contractual restrictions outlined above and related policies, are designed to ensure safe use of the Azure OpenAI Service. FAC ¶¶ 55–60.

In addition, the Microsoft® Mark is famous, distinctive, and widely recognized by the general consuming public of the United States as a designation of the source of goods or services that are the subject of this lawsuit. FAC ¶ 123.

C. Defendants' Scheme

Despite Microsoft's multiple layers of safety controls, Defendants "illegally procured authentication information from legitimate Microsoft customers with malicious intent, trafficked and used that stolen customer authentication information to bypass Microsoft authentication gates and gain unauthorized access to Microsoft software and computer systems, and then exploited their unauthorized access to Microsoft's software and computers to create harmful content in violation of Microsoft's policies and through circumvention of Microsoft's technical protective measures." FAC ¶¶ 19, 36, 37.

Specifically, Defendants are members of an ongoing association-in-fact enterprise operating a "hacking-as-a-service" scheme designed to abuse Microsoft's Azure infrastructure and software and provide the infrastructure necessary for end-users to generate harmful content that would otherwise be prohibited. FAC ¶ 10, 80, 128. Each Defendant individually provided funding, devices, infrastructure, resources, and logistical support necessary to carry out the enterprise's activities. FAC ¶ 134. Each Defendant further marketed and sold the enterprise's technological capabilities to other malicious actors and provided detailed instructions for using the enterprise's custom tools to circumvent Microsoft's safety controls and generate harmful content. FAC ¶ 135.

Defendants, through this "hacking-as-a-service" enterprise, developed, deployed, marketed, and sold two related software tools and associated Internet infrastructure, which were used to unlawfully generate thousands of harmful images, including various images depicting misogyny, non-consensual intimate images of celebrities, and other sexually explicit content, through the Azure OpenAI Service. FAC ¶ 37.

First, Defendants created a client-side software tool referred to by Defendants as "de3u," which Defendants make publicly available via the "rentry.org/de3u" domain. FAC ¶ 82. The de3u software is designed to try to prevent the Azure OpenAI Service from revising the original text prompt used to generate images, which can happen for example when a text prompt contains words that trigger Microsoft's content filtering. FAC ¶ 88. In addition, the de3u software is designed to detect and report whether the Azure OpenAI Service rejected a text prompt because it is considered as violating Microsoft's content policy. FAC ¶ 88.

Second, Defendants created software for running a reverse proxy service, referred to as the "oai reverse proxy," designed specifically for processing and routing communications from the de3u software to Microsoft's systems. FAC ¶ 82. The oai reverse proxy service consists of software running on a reverse proxy server that transmits communications from de3u user computers to the Azure OpenAI Service.[3] In addition to performing the traditional function of any reverse proxy, such as forwarding requests, the oai reverse proxy tool "processes and alters communications traffic between de3u client computers and the target Azure OpenAI Service." FAC ¶ 91. Defendants configured the proxy to route traffic to designated Azure OpenAI Service endpoints. *Id*. For example, when a de3u user submits a request to generate an image,

[3] In general, a reverse proxy server is a server that sits in front of web servers and forwards client (e.g., web browser) requests to those web servers. A reverse proxy ensures that no client ever communicates directly with that origin server. FAC ¶ 90.

the de3u software routes that request to the oai reverse proxy. The proxy then parses the request and forwards it to the appropriate Azure OpenAI Service endpoint. FAC ¶ 92.

The de3u software and oai reverse proxy enabled Defendants to gain unauthorized access to and use of Microsoft computers running Azure OpenAI services and reverse engineer methods to circumvent Microsoft's content and abuse control measures. FAC ¶ 88. The harmful images created by Defendants and/or end-users using Defendants' malicious tools include a C2PA Content Credentials symbol ("CR Icon") inserted by the Azure OpenAI service. This CR Icon identifies the Azure OpenAI Service as the technology used to generate the image via a metadata field that contains the Microsoft® registered trademark. FAC ¶ 95.

Defendants' "hacking-as-a-service" enterprise caused substantial harm to Plaintiff. First, Microsoft's internal personnel and outside counsel spent months investigating and remediating Defendants' conduct, resulting in significant costs. FAC ¶ 100. Second, the inclusion of the Microsoft® registered trademark in harmful images caused "injury to Microsoft's business goodwill and diminished the value of Microsoft's and its customers' possessory interest in their computers and software." FAC ¶ 150. Finally, Defendants fraudulently obtained valuable services from Microsoft. FAC ¶ 101.

2. Federal Rule of Civil Procedure 12(b)(6) Analysis

Now, as explained above, the undersigned must evaluate whether the Complaint states a "claim upon which relief can be granted" by applying the standards used in motions to dismiss under Federal Rule of Civil Procedure 12(b)(6).

Having examined the record, the undersigned Magistrate Judge finds that the well-pleaded allegations of fact in the First Amended Complaint (Dkt. No. 41), supported by Plaintiff's Motions for Default Judgment (Dkt. No. 64) and Briefs In Support of Plaintiff's

Motion for Default Judgment (*id.*), establish that Defendants violated the CFAA, the DMCA, the Lanham Act, RICO, and committed trespass to chattels and tortious interference.

A. Computer Fraud and Abuse Act Claim Under 18 U.S.C. § 1030

The CFAA penalizes a party that: (1) intentionally accesses a protected computer without authorization and, as a result of such conduct, causes damage and loss, 18 U.S.C. § 1030(a)(5)(C); (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer, 18 U.S.C. § 1030(a)(2)(C); or (3) 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, 18 U.S.C. § 1030(a)(5)(A). A "protected computer" is a computer "used in interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B); *see also SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593, 608 (E.D. Va. 2005). The phrase "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled to obtain or alter." 18 U.S.C. § 1030(e)(6); *see also SecureInfo Corp.*, 387 F. Supp. 2d at 608. Congress did not define "unauthorized access" by statute. *SecureInfo Corp.*, 387 F. Supp. 2d at 608. Lastly, to pursue a claim under the CFAA, a plaintiff must demonstrate loss or damage in excess of $5,000. 18 U.S.C. § 1030(c)(4)(A)(i)(I).

The First Amended Complaint sufficiently states a claim under the CFAA by establishing that Defendants knowingly and intentionally accessed protected computers without authorization and knowingly caused the transmission of information, code, and commands that resulted in damage to the protected computers, the software, and Plaintiff. Specifically, the record reflects that Defendants "illegally procured authentication information

from legitimate Microsoft customers with malicious intent, trafficked and used that stolen customer authentication information to bypass Microsoft authentication gates and gain unauthorized access to Microsoft software and computer systems, and then exploited their unauthorized access to Microsoft's software and computers to create harmful content in violation of Microsoft's policies and through circumvention of Microsoft's technical protective measures." FAC ¶ 19. To respond to Defendants' cyber attacks, Plaintiff's "internal personnel and outside counsel … spent months investigating and working to remediate Defendants' conduct, which has imposed costs well over the CFAA's $5,000 threshold." *Id.* ¶ 101. In addition, the value of the services Defendants fraudulently obtained from Plaintiff exceeds $5,000. *Id.*

This type of attack, and resulting monetary damage, is precisely what the CFAA is designed to prevent. *See, e.g.*, *Global Policy Partners, LLC v. Yessin,* 686 F. Supp. 2d 631, 635-37 (E.D. Va. 2009) (accessing an email account using credentials that did not belong to defendant was actionable under the CFAA); *Physicians Interactive v. Lathian Systems, Inc*., 2003 U.S. Dist. LEXIS 122472, at *18-19 (E.D. Va. Dec. 5, 2003) (attacking websites and computer file servers to obtain proprietary information was actionable under the CFAA). Indeed, courts have observed that the CFAA was targeted at "computer hackers (e.g., electronic trespassers)." *State Analysis Inc. v. Am. Fin. Services Assoc*., 621 F. Supp. 2d 309, 315 (E.D. Va. 2009) (internal citations omitted). Moreover, this Court has consistently held that analogous activity causing damage in excess of $5,000 is actionable under the CFAA. *See, e.g*., *Microsoft Corp. v. Does 1-2,* No. 1:17-CV-01224-TSE-MSN, 2018 WL 6186826, at *1 (E.D. Va. Oct. 31, 2018), *report and recommendation adopted, Microsoft Corp. v. Does,* No. 1:17-CV-1224, 2018 WL 6183279 (E.D. Va. Nov. 27, 2018); *Microsoft Corp. v. Doe*, 2015

U.S. Dist. LEXIS 109729, at *1-4 (E.D. Va. Aug. 17, 2015); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 46951, at *1-2 (E.D. Va. Apr. 2, 2014). Accordingly, the undersigned finds that Defendants have violated the CFAA.

B. The DMCA Claims Under 17 U.S.C. § 1201

The DMCA was enacted in 1998 to address the "perceived need of copyright owners for 'legal sanctions' to enforce various technological measures they had adopted to prevent the unauthorized reproduction of their works." *Murphy v. Millennium Radio Grp. LLC*, 650 F.3d 295, 300 (3d Cir. 2011). The DMCA "backed with legal sanctions the efforts of copyright owners to protect their works from piracy behind digital walls such as encryption codes or password protections." *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 435 (2d Cir. 2001). In adopting the DMCA, "Congress targeted not only those pirates who would circumvent these digital walls (the "anti-circumvention provisions," contained in 17 U.S.C. § 1201(a)(1)), but also anyone who would traffic in a technology primarily designed to circumvent a digital wall (the "anti-trafficking provisions," contained in 17 U.S.C. § 1201(a)(2), (b)(1))." *Id.*

Here, Plaintiff asserts two claims under two separate subsections of the DMCA. The first is subsection 1201(a)(1)(A), the anti-circumvention provision. This provision "prohibits a person from 'circumvent[ing] a technological measure that effectively controls access to a work protected under [Title 17, governing copyright].'" *Id.* (quoting 17 U.S.C. § 1201(a)). The second subsection is 1201(a)(2), which provides:

> "No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—
>
> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title. *Id.* § 1201(a)(2).
>
> To "circumvent a technological measure" is defined, in pertinent part, as "to descramble a scrambled work ... or otherwise to ... bypass ... a technological measure, without the authority of the copyright owner." *Id.* § 1201(a)(3)(A).

The First Amended Complaint sufficiently states claims under subsections 1201(a)(1) and 1201(a)(2) by establishing that Defendants (1) used sophisticated technical means to circumvent the normal operation of Microsoft's content-filtering systems, thereby gaining unauthorized access to portions of Microsoft's Azure software that would otherwise have been denied; and (2) manufactured, imported, offered to the public, provided, and otherwise trafficked in technologies and services primarily designed or produced for the purpose of circumventing technological measures that effectively control access to Microsoft's Azure software, which is protected under the Copyright Act.

Specifically, the record reflects the following relevant facts: (1) "Microsoft's Azure APIs, the software the Azure APIs interact with, and the software that implements Microsoft's abuse and content filtering policies are creative works of authorship subject to protection under the Copyright Act" (FAC ¶ 106); (2) the "Azure middleware responsible for processing, routing, filtering, executing, and communicating Azure communications is subject to copyright protection" (FAC ¶ 106); (3) the "Azure OpenAI Service Software that implements Microsoft's abuse and content filtering policies comprises a collection of creative models authored by Microsoft" (FAC ¶ 106); (4) "Microsoft controls access to and use of its copyright protected Azure software . . . through use of authentication information that includes API Keys, customer deployment IDs, endpoint information, and token information" (FAC ¶ 106); (5)

"Microsoft's API key management system requires application, with Microsoft's authority, of authenticating information to gain access to Microsoft's Azure software" (FAC ¶ 107); (6) "using HTTP requests containing stolen and dynamically manipulated API Key, deployment ID, end point, and token information" Defendants "sent to the Azure OpenAI Service computer commands that mimicked authentic Azure OpenAI Service API calls" (FAC ¶ 108); and (7) these "maliciously configured HTTP requests allowed Defendants to circumvent Microsoft's technical measures for controlling access to its Azure software" (*id.*).

These facts, deemed admitted as to Defendants, are sufficient to establish that Defendants violated 17 U.S.C. §§ 1201(a)(1) and 1201(a)(2).

C. Lanham Act Claim

Plaintiff asserts a single count of false designation of origin under 15 U.S.C. § 1125(a) of the Lanham Act. Section 1125(a) of the Lanham Act prohibits "the use of a trademark, any false designation of origin, false designation of fact or misleading representation of fact which is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person." *Microsoft Corp. v. Does 1-2,* No. 1:17-CV-01224-TSE-MSN, 2018 WL 6186826, at *8 (E.D. Va. Oct. 31, 2018), *report and recommendation adopted, Microsoft Corp. v. Does,* No. 1:17CV1224, 2018 WL 6183279 (E.D. Va. Nov. 27, 2018) (citing 15 U.S.C. § 1125(a)(1)(A)). In order to prevail in an action for trade mark infringement under 15 U.S.C. § 1125(a), a plaintiff must establish the following three elements: "(1) the alleged violator must employ a false designation; (2) the false designation must deceive as to origin, ownership or sponsorship; and (3) the plaintiff must believe that 'he or she is or is likely to be damaged by such [an] act.'" *Id.* (citing *Am.*

Online v. IMS, 24 F. Supp. 2d 548, 551 (E.D. Va. 1998)).

Here, Plaintiff has established that Defendants "generated and/or distributed unauthorized and harmful images containing the famous Microsoft® mark in metadata identifying Microsoft as the source of such images." FAC ¶ 120. Such conduct, involving embedding a protected mark in distributed content to suggest source or origin, is analogous to conduct this Court has found actionable under Section 1125(a) of the Lanham Act. *See Am. Online*, 24 F. Supp. 2d at 551-52 (holding that spam email with purported "from" addresses including plaintiffs' trademarks constituted false designation of origin).

The record further establishes that Defendants' conduct is likely to cause confusion, mistake, or deception as to the affiliation, connection, or association between Defendants and Microsoft, or as to Microsoft's sponsorship or approval of Defendants' activities. FAC ¶¶ 121–22. In addition, the Microsoft® Mark is famous, distinctive, and widely recognized by the general consuming public of the United States as a designation of the source of goods or services that are the subject of this lawsuit. FAC ¶ 123. This Court has recognized that similar misuse of Microsoft's marks caused confusion and mistake as to Microsoft's affiliation with the misconduct. *Microsoft Corp. v. Does 1–2*, No. 1:17-cv-01224, 2018 WL 6186826, at *8 (E.D. Va. Oct. 31, 2018), report and recommendation adopted, 2018 WL 6183279 (E.D. Va. Nov. 27, 2018) (finding that, through spear phishing techniques, defendants "misleadingly and falsely caused the famous and distinctive Microsoft, Windows, and Internet Explorer trademarks to be associated with malicious conduct performed on plaintiff's and its customers' computers and operating systems.")

Plaintiff also alleged significant harm resulting from Defendants' violation of Section 1125(a), including injury to its reputation, brand, and goodwill, the dilution by tarnishment of

its famous mark, and significant financial expenses necessary to respond to Defendants' actions. FAC ¶ 124.

Accordingly, the First Amended Complaint sufficiently states a claim for false designation of origin under 15 U.S.C. § 1125(a) of the Lanham Act.

D. RICO Claim under 18 U.S.C. § 1964(c)

"Violations of RICO can be prosecuted criminally or brought as civil claims, including as private actions by any person injured in his business or property by reason of such violations." *Field v. GMAC LLC*, 660 F. Supp. 2d 679, 686 (E.D. Va. 2008) (citing 18 U.S.C. §§ 1962–1964). "Specifically, a private RICO plaintiff must allege '(1) conduct (2) of an enterprise (3) through a pattern (4) of racketeering activity.'" *Id.* (citing *Sedima, S.P.R.L. v. Imrex Co*., Inc., 473 U.S. 479, 496 (1985)). "'Plaintiff must additionally show that (5) he was injured in his business or property (6) by reason of the RICO violations.'" *Id.* (citing *D'Addario v. Geller*, 264 F.Supp.2d 367, 396 (E.D. Va. 2003)).

"In order adequately to allege elements (3) and (4), plaintiff must allege two or more predicate acts of racketeering and, more importantly, 'allege a continuing pattern and a relationship among the defendant's activities showing they had the same or similar purposes.'" *Id.* (citing *Anderson v. Found. for Advancement, Educ. & Employment of Am. Indians*, 155 F.3d 500, 505 (4th Cir. 1998)). "'RICO treatment is reserved for conduct 'whose scope and persistence pose a special threat to social well-being.'" *Id.* (citing *GE Inv. Private Placement Partners II v. Parker*, 247 F.3d 543, 550 (4th Cir. 2001)).

"Where RICO claims are based on predicate acts of fraud, the heightened pleading standard set forth in Rule 9(b) of the Federal Rule of Civil Procedure applies." *Id.* (citing *Menasco, Inc. v. Wasserman*, 886 F.2d 681, 684 (4th Cir.1989)). Specifically, Plaintiff "must

state with particularity the circumstances constituting fraud or mistake" though "[m]alice, intent, knowledge, and other conditions of a person's mind" may be alleged generally. *See Field*, 660 F. Supp. 2d at 686.

"In order [to] adequately allege elements (5) and (6), the Fourth Circuit has indicated that U.S. Supreme Court precedent 'instructs us to employ a traditional causation analysis in determining whether a RICO plaintiff has been injured 'by reason of' a section 1962 violation." *Id.* (citing *Busby v. Crown Supply, Inc*., 896 F.2d 833, 839–40 (4th Cir.1990)).

Here, Plaintiff has established that Defendants violated the RICO Act by engaging in a pattern of wire fraud (in violation of 18 U.S.C. § 1343) and access device fraud (in violation of 18 U.S.C. § 1029) in furtherance of their criminal enterprise targeting Plaintiff. Specifically, Defendants orchestrated an "ongoing association-in-fact enterprise" that provides "hacking-as-a-service software and infrastructure." FAC ¶ 128. Defendants have conducted the affairs of the enterprise through a "coordinated and continuous pattern of illegal activity" for the "common purpose of achieving the objectives of the [e]nterprise, including the common objectives of wire fraud and access device fraud designed to enable unauthorized and fraudulent access to generative AI services provided by Microsoft and others." *Id.* ¶¶ 129-30.

In order to support a claim based on wire fraud, Plaintiff must establish that Defendants (1) devised or intended to devise a scheme or artifice to defraud, or (2) for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, (3) transmitted or caused to be transmitted by means of wire, radio, or television communication (4) in interstate or foreign commerce, (5) any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

In support of its wire fraud claim, Plaintiff established that "at some point prior to July

2024, Defendants devised a scheme to obtain money or property from Microsoft's paying customers and others, and to defraud Microsoft and other generative AI service providers, by stealing authentication information from Microsoft customers and misusing that authentication information to gain fraudulent access [to] the Azure OpenAI Service." FAC ¶ 139. The record further reflects that "Defendants understood and intended that their misuse of stolen customer authentication information would deplete the account balances of the paying customers whose credentials they stole," and that they acted "at least in part to avoid paying the costs of obtaining a license[] to services like the Azure OpenAI Service and to avoid the cost of purchasing the tokens required to use such services at scale." FAC ¶ 139. The FAC clearly and specifically alleges that Defendants unlawfully accessed and misused Microsoft's systems and technology and in so doing defrauded Plaintiff out of both money and property.

The record also reflects that Defendants utilized interstate wires in furtherance of their scheme. Specifically, "[f]rom July 26, 2024, to at least September 17, 2024, Defendants transmitted and/or caused to be transmitted by means of wire communication in interstate and foreign commerce writings, signals, and pictures for the purpose of executing their scheme to defraud" (FAC ¶ 140), including that "on numerous occasions between July 26, 2024, and August 18, 2024, Defendants transmitted . . . stolen API Key and token information in order to defraud Microsoft and others regarding Defendants' identities and authorization to access Microsoft's and others' systems and to deprive paying customers of tokens they had paid for." FAC ¶ 140. Lastly, the record reflects that Defendants' conduct was "willful" and has "caused harm to Microsoft's business and property." FAC ¶ 144-45.

These factual allegations, deemed admitted as to Defendants, satisfy Rule 9(b) and the elements of 18 U.S.C. § 1343 by establishing the willfulness of the alleged conduct, resulting

harm, the precise nature of the fraudulent scheme, the approximate timeframe, and the specific means by which Defendants executed the scheme.

In order to support a claim based on counterfeit access device fraud, Plaintiff must establish that Defendants (1) knowingly and with intent to defraud, (2) produced, used, or trafficked, (3) in one or more counterfeit access devices. The term "access device" means any card, plate code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds. 18 U.S.C. § 1029(e)(1). The term "counterfeit access device" means any access device that is "counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device." 18 U.S.C. § 1029(e)(2).

In order to support a claim based on unauthorized access device fraud, Plaintiff must establish that Defendants (1) knowingly and with intent to defraud (2) trafficked in or used (3) one or more unauthorized access devices (4) during any one-year period, and (5) by such conduct obtained anything of value aggregating $1,000 or more during that period. The term "unauthorized access device" means any access device that is lost, stolen, expired, revoked, cancelled, or obtained with intent to defraud. 18 U.S.C. § 1029(e)(3).

In support of its access device fraud claims, the record reflects that "[f]rom July 26, 2024, to at least August 18, 2024, Defendants knowingly and with the intent to defraud produced, used, and trafficked in counterfeit access devices including the oai reverse proxy server and de3u computers" (FAC ¶ 141), and that during the same period Defendants

"knowingly and with intent to defraud trafficked in and used unauthorized access devices, and by such conduct obtained a thing of value aggregating $1,000 or more" (FAC ¶ 142).

Taken together, these facts, deemed admitted as to Defendants, are sufficient to establish the requisite predicate acts of wire fraud and access device fraud under the RICO statute. Accordingly, the First Amended Complaint sufficiently states a claim under 18 U.S.C. § 1964(c).

E. Trespass to Chattels Claim

Under Virginia law, trespass to chattels occurs when "personal property of another is used without authorization, but the conversion is not complete." *Dpr Inc. v. Dinsmore*, 82 Va. Cir. 451, 458 (Va. Cir. Ct. 2011). Here, the First Amended Complaint establishes that "in abusing the Azure OpenAI Service" Defendants gained "unauthorized access to the computers of Microsoft." FAC ¶ 148.

This conduct is an illegal trespass. *See, e.g.*, *Physicians Interactive v. Lathiam Sys.*, 2003 U.S. Dist. LEXIS 22868, at *26-28 (E.D. Va. Dec. 5, 2003) (holding that a cyber attack, which used a software robot to hack into plaintiff's computer system and obtain proprietary information, serves as a prima facie basis for a claim for trespass to chattels); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 24-25 (E.D. Va. Jan. 6, 2014) ("The unauthorized intrusion into an individual's computer system . . . supports actions under [trespass to chattel claim]"); *Does 1-2*, No. 1:17-CV-01224-TSE-MSN, 2018 WL 6186826, at *8 (finding that defendants' unauthorized access to plaintiff's and its customers' computers and plaintiff's operating system and defendant's unauthorized downloading of software and control over such computers was an illegal trespass). Accordingly, the undersigned finds that Defendants are liable for trespass to chattels.

F. Tortious Interference with Contractual Relations Claim

To prevail on a tortious interference claim under Virginia law, a party must prove "'(1) the existence of a valid contractual relationship…; (2) knowledge of the relationship…on the part of the interferor; (3) intentional interference inducing or causing a breach or termination of the relationship…; and (4) resultant damage to the party whose relationship…has been disrupted.'" *Does 1-2,* No. 1:17-CV-01224-TSE-MSN, 2018 WL 6186826, at *9. (quoting *Commerce Funding Corp. v. Worldwide Sec. Services Corp*., 249 F.3d 204, 214 (4th Cir. 2001)).

The First Amended Complaint pleads sufficient facts to support a finding of a tortious interference. Specifically, the record establishes that "Microsoft has valid contracts with the customers who have been victimized by Defendants" (FAC ¶ 155); that Defendants "had knowledge of Microsoft's customer contracts and intentionally set out to wrongfully use Microsoft's customers' contracts and funds for Defendants' own unlawful purposes" (FAC ¶ 155); that Defendants "have interfered with Microsoft's contracts with its customers by stealing customer account information and using that information to deplete customer account funds" (FAC ¶ 156); and that Defendants' conduct "has impeded the parties to Microsoft's customer contracts' abilities to perform their respective obligati Accordingly, the undersigned finds that Defendants committed a tortious interference with contractual relations.

VII. Analysis of Plaintiff's Requested Relief

Plaintiff is not requesting monetary relief but is only seeking injunctive relief to prevent Defendants from engaging in further unlawful and harmful activity. Dkt. No. 64-1. Specifically, Plaintiff seeks a permanent injunction enjoining Defendants and their

representatives, officers, agents, directors, affiliates, servants, employees, and all persons acting in concert or participation with them, including employees and independent contractors from "(1) accessing without authorization the computers or software comprising Microsoft's Azure OpenAI Service; (2) sending malicious code to configure, deploy or operate the Azure Abuse Enterprise; (3) generating and sending harmful images bearing false indicia of sponsorship or approval by Microsoft; and (4) stealing information, money, or property from Plaintiff or Plaintiff's customers." Dkt. No. 64-1. In addition, Plaintiff seeks a permanent injunction requiring the registered Internet domain "aitism.net," which was used by Defendants to carry out their scheme, to (1) "Prevent transfer or modification of the domain to the Defendants; (2) Maintain unchanged the WHOIS or similar contact and identifying information as of the time of receipt of this Order and maintain the domains with the current registrar; and (3) Continue to direct traffic to the domain to secure servers identified by Microsoft as may be necessary." *Id.*

Under the Federal Rules of Civil Procedure, a default judgment "must not differ in kind from, or exceed in amount, what is demanded in the pleadings." Fed. R. Civ. P. 54(c). Because Plaintiff sought a permanent injunction in its First Amended Complaint (Dkt. No. 41), Plaintiff is entitled to permanent injunctive relief on its Motion for Default Judgment.

"Parties seeking a preliminary injunction must demonstrate that (1) they are likely to succeed on the merits, (2) they are likely to suffer irreparable harm, (3) the balance of hardships tips in their favor, and (4) the injunction is in the public interest. *Metro. Reg'l Info. Sys. V. Am. Home Realty Network, Inc*., 722 F.3d 591, 595 (4th Cir. 2013). Courts in this District routinely grant permanent injunctive relief upon entry of default judgment in order to preserve relief granted in prior preliminary injunction orders. *See, e.g.*, Microsoft Corp. v. Does, Civil Action

No. 1:16cv993, 2017 U.S. Dist. LEXIS 145448, at *17 (E.D. Va. Aug. 1, 2017) (granting motion for default and imposing permanent injunction); *Does 1-2,* No. 1:17-CV-01224-TSE-MSN, 2018 WL 6186826, at *9 (recommending that the Court grant motion for default judgment and enter a permanent injunction against defendants); *Toolchex, Inc. v. Trainor*, No. 3:08-CV-236, 2009 U.S. Dist. LEXIS 64186, at *18 (E.D. Va. July 24, 2009) (imposing permanent injunction in default judgment); *Whittingham v. Bluevine Capital, Inc*., Civil Action No. 3:17-cv-720-JAG, 2018 U.S. Dist. LEXIS 212252, at *4 (E.D. Va. Dec. 17, 2018) (same).

As discussed above, the Court previously determined that Plaintiff was likely to prevail on its claims, that Defendants' conduct threatens irreparable harm, and that the equities and public interest both weigh in favor of injunctive relief. Dkt. No. 21 (TRO); Dkt. No. 38 (Preliminary Injunction). The Court's January 10, 2025 Preliminary Injunction Order granted the same injunctive relief that Plaintiff seeks in the instant Motion for Default Judgment. The only material change since the Preliminary Injunction Order is that the facts alleged in the First Amended Complaint have now been deemed admitted as to Defendants. Accordingly, the undersigned finds that the injunctive relief granted by this Court in the preliminary injunction remains appropriate and that Plaintiff's request for a permanent injunction addressing the same conduct should be entered.

VIII. Recommendation

For the foregoing reasons, the undersigned recommends:

1) **GRANTING** Plaintiff's Motion for Default Judgment (Dkt. No. 64); and

2) **ENTERING** a permanent injunction as requested in Plaintiff's Proposed Order (Dkt. No. 64-1), that enjoins Defendants and their representatives, officers, agents, directors, affiliates, servants, employees, and all persons acting in concert or participation with them,

including employees and independent contractors from (1) accessing without authorization the computers or software comprising Microsoft's Azure OpenAI Service; (2) sending malicious code to configure, deploy or operate the Defendants' scheme as set forth in the First Amended Complaint and referred to by Plaintiff as the Azure Abuse Enterprise; (3) generating and sending harmful images bearing false indicia of sponsorship or approval by Microsoft; and (4) stealing information, money, or property from Plaintiff or Plaintiff's customers. In addition, the undersigned recommends that the permanent injunction require that, with respect to the registered Internet domain "aitism.net," which was used by Defendants to carry out their scheme, the relevant Registry shall take the following actions (1) prevent transfer or modification of the domain to the Defendants; (2) maintain unchanged the WHOIS or similar contact and identifying information as of the time of receipt of this Order and maintain the domains with the current registrar; and (3) continue to direct traffic to the domain to secure servers identified by Microsoft as may be necessary.

IX. Notice

The parties are advised that objections to this Report and Recommendation, pursuant to 28 U.S.C. § 636 and Rule 72(b) of the Federal Rules of Civil Procedure, must be filed within fourteen (14) days of its service. Failure to object to this Report and Recommendation waives appellate review of any judgment based on it.

William E. Fitzpatrick
WILLIAM E. FITZPATRICK
UNITED STATES MAGISTRATE JUDGE

May 26, 2026

Alexandria, Virginia