

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION**

MICROSOFT CORPORATION,

Plaintiff,

v.

ARIAN YADEGARNIA, RICKY YUEN, and
PHAT PHUNG TAN.

Defendants.

Case No. 1:24-cv-2323

MICROSOFT'S MOTION FOR DEFAULT JUDGMENT

TABLE OF CONTENTS

	Page No.
I. INTRODUCTION.....	1
II. LEGAL STANDARD.....	2
III. STATEMENT OF FACTS.....	3
A. Factual Overview.....	3
B. Procedural History.....	9
IV. ARGUMENT.....	11
A. The Court has Jurisdiction.....	11
B. All Relevant Default Factors Favor of Default Judgment.....	15
C. A Permanent Injunction is Appropriate.....	18
V. CONCLUSION	

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Amazon.com, Inc. v. WDC Holdings LLC</i> , Civil Action No. 1:20-cv-484, 2020 U.S. Dist. LEXIS 134555 (E.D. Va. July 28, 2020)	21
<i>Batts v. Snap Inc.</i> , No. 2:23-cv-03565-DCN, 2024 U.S. Dist. LEXIS 139286 (D.S.C. July 6, 2024)	13
<i>Bay Tobacco, LLC v. Bell Quality Tobacco Prod.</i> , LLC, 261 F. Supp. 2d 483 (E.D. Va. 2003)	20
<i>Bright Imperial Ltd. v. RT MediaSolutions, S.R.O.</i> , Civil Action No. 1:11-cv-935-LO-TRJ, 2012 U.S. Dist. LEXIS 70000 (E.D. Va. May 18, 2012)	13, 14
<i>BSN Med., Inc. v. Art Witkowski</i> , 2008 U.S. Dist. LEXIS 95338 (W.D.N.C. Nov. 21, 2008)	20
<i>Cadence Bank, N.A. v. Draam</i> , No. 2:24cv305, 2025 U.S. Dist. LEXIS 111291 (E.D. Va. Jan. 10, 2025)	16, 18
<i>Chapman v. Saber Healthcare Grp., L.L.C.</i> , No. 2:20CV106, 2021 WL 12324338 (E.D. Va. Nov. 1, 2021)	2, 15
<i>Conyers v. Guyton</i> , No. 2:23cv689, 2024 U.S. Dist. LEXIS 248982 (E.D. Va. Aug. 26, 2024)	16
<i>DIRECTV, Inc. v. Rawlins</i> , 523 F.3d 318 (4 th Cir. 2008)	2
<i>Dmarcian, Inc. v. Dmarcian Eur. BV</i> , 60 F.4 th 119 (4 th Cir. 2022)	12
<i>El Pollo Rico, LLC v. Wings & Pollo, LLC</i> , No. PWG 21-cv-2346, 2022 U.S. Dist. LEXIS 132472 (D. Md. July 25, 2022)	2
<i>Field v. GMAC LLC</i> , 660 F. Supp. 2d 679 (E.D. Va. 2008)	19
<i>Garden & Gun, LLC v. Twodalgals, LLC</i> , 2008 U.S. Dist. LEXIS 79982 (W.D.N.C. 2008)	19

George v. Brown,
Civil Action No. 3:24CV318 (RCY), 2025 U.S. Dist. LEXIS 259131 (E.D. Va. Dec. 15, 2025)17

Gunn v. Minton,
568 U.S. 257 (2013).....11

Int’l Labor Mgmt. Corp. v. Perez,
2014 U.S. Dist. LEXIS 57803 (M.D.N.C. Apr. 25, 2014).....20

Mayrant v. Norfolk Redevelopment & Hous. Auth.,
No. 2:24cv715, 2025 U.S. Dist. LEXIS 192852 (E.D. Va. Sep. 23, 2025)16, 18

Meineke Car Care Ctrs., Inc. v. Bica,
2011 U.S. Dist. LEXIS 118171 (W.D.N.C. Oct. 12, 2011).....21

Metro. Reg’l Info. Sys. V. Am. Home Realty Network, Inc.,
722 F.3d 591 (4th Cir. 2013)18

Microsoft Corp. v. Doe,
2014 U.S. Dist. LEXIS 48398 (E.D. Va. Jan. 6, 2014)20, 21

Microsoft Corp. v. Doe,
No. 1:17-cv-01224-TSE-MSN, 2018 U.S. Dist. LEXIS 202016 (E.D. Va. Oct. 31, 2018)2, 17

Microsoft Corp. v. Does,
Civil Action No. 1:16cv993, 2017 U.S. Dist. LEXIS 145448 (E.D. Va. Aug. 1, 2017)2, 17, 19

Microsoft Corp. v. Does,
Civil Action No. 1:22cv607, 2024 U.S. Dist. LEXIS 76088 (E.D. Va. Jan. 10, 2024)19

Noble Sec., Inc. v. MIZ Eng’g, Ltd.,
611 F. Supp. 2d 513 (E.D. Va. 2009)15

Pesch v. First City Bank of Dallas,
637 F. Supp. 1539 (N.D. Tex. 1986)20

Philips Med. Sys. Nederland B.V. v. TEC Holdings, Inc.,
No. 3:20-cv-21-MOC-DSC, 2023 U.S. Dist. LEXIS 7319 (W.D.N.C. Jan. 17, 2023)19

Sec. & Exch. Comm’n v. Ramaraj,
No. 1:24-CV-1282-CMH-LRV, 2025 WL 1905571 (E.D. Va. Apr. 22, 2025)11

Sierra Software, LLC v. Malih,
 No. 2:17cv607, 2019 U.S. Dist. LEXIS 250703 (E.D. Va. Feb. 15, 2019)16

SRL v. Lingxian Guangzhou Technol-Ogy Co., Ltd.,
 No. 2:21cv337, 2021 U.S. Dist. LEXIS 263977 (E.D. Va. Oct. 21, 2021)16

Stihl Inc. v. Kinetic Ceramics, LLC,
 No. 2:22cv111, 2023 U.S. Dist. LEXIS 237366 (E.D. Va. Feb. 9, 2023)15, 16, 17

Synopsys, Inc. v. AzurEngine Techs., Inc.,
 401 F. Supp. 3d 1068 (S.D. Cal. 2019).....20

Synopsys, Inc. v. Sunlune Corp.,
 No. 24-cv-00220-BLF, 2024 U.S. Dist. LEXIS 208388 (N.D. Cal. Nov. 15, 2024)19

Synopsys, Inc. v. Sunlune Corp.,
 No. 24-cv-00220-BLF, 2025 U.S. Dist. LEXIS 97297 (N.D. Cal. May 21, 2025)16, 18, 19

Toolhex, Inc. v. Trainor,
 No. 3:08-CV-236, 2009 U.S. Dist. LEXIS 64186 (E.D. Va. July 24, 2009).....17, 19

UMG Recordings, Inc. v. Kurbanov,
 963 F.3d 344 (4th Cir. 2020)13

Umg Recordings v. Kurbanov,
 Civil Action No. 1:18-cv-957, 2021 U.S. Dist. LEXIS 250844 (E.D. Va. Dec. 16, 2021)20

US Airways, Inc. v. US Airline Pilots Ass’n,
 813 F. Supp. 2d 710 (W.D.N.C. 2011)20

Wells Fargo Commer. Distribution Fin., LLC v. Shore Saw & Mower, Inc.,
 No. 2:23-cv-100, 2023 U.S. Dist. LEXIS 140218 (E.D. Va. Aug. 10, 2023)17

Whittingham v. Bluevine Capital, Inc.,
 No. 3:17-cv-720-JAG, 2018 U.S. Dist. LEXIS 212252 (E.D. Va. Dec. 17, 2018)2, 17, 19

Statutes

18 U.S.C. § 1962.....9

28 U.S.C. § 1367.....11

Computer Fraud and Abuse Act, the Digital Millennium Copyright Act.....1

DMCA, the Lanham Act, and the RICO Act. 28 U.S.C. § 133111, 19, 20

Lanham Act.....1, 19, 20

RICO8, 19, 21

Other Authorities

Fed. R. Civ. P. 4(k)(2).....14

Fed. R. Civ. P. 8(b)(6).....2

Fed. R. Civ. P. 41(A)(1)(a)(i)10

Fed. R. Civ. P. 55(a)2

Fed. R. Civ. P. 55(b)1, 2

I. INTRODUCTION

This case arises from a scheme to break into Microsoft’s systems and abuse AI tools for the purpose of generating harmful images. In December 2024, Microsoft sued ten DOE Defendants for violations of the Computer Fraud and Abuse Act, the Digital Millennium Copyright Act, the Lanham Act, the Racketeer Influenced and Corrupt Organizations Act, and for trespass to chattels and tortious interference under Virginia state law. After obtaining discovery and further investigative information, Microsoft identified certain individuals previously sued as DOE defendants and filed a First Amended Complaint (“FAC”) against *inter alia* named Defendants Arian Yadegarnia (Yadegarnia), Ricky Yuen (Yuen), and Phát Phùng Tấn (collectively “Defaulting Defendants”). Dkt. 41. Pursuant to the Court’s order authorizing alternative service on Defaulting Defendants (Dkt. 46 and 58), Microsoft served each of Messrs. Yadegarnia, Yuen, and Tấn by emailing the summons, complaint, and other pleadings to their known email accounts and the abuse contacts for the infrastructure associated with them. See Dkt. 45 (authorizing service on Defendants’ known email address and ISP abuse contacts for Defendants’ infrastructure).

Despite being properly served and receiving actual notice of this case, none of the Defaulting Defendants ever filed an Answer to the FAC or otherwise made any appearance in this action. Dkt. 61 (Clerk’s Default). Microsoft respectfully requests entry of default judgment against Defendants pursuant to Rule 55(b). The evidence Microsoft gathered through discovery and its investigative efforts establishes that the allegations in Microsoft’s Complaint are true. Given the record and the equities presented, Microsoft respectfully submits that the default judgment should include permanent injunctive relief preventing Defendants from regaining control over the subject infrastructure.

II. LEGAL STANDARD

Where a defendant fails “to plead or otherwise defend” the claims against it, “the clerk must enter the party’s default.” Fed. R. Civ. P. 55(a). Upon entry of default, the complaint’s well-pleaded allegations relating to the defendant’s liability are taken as true, with the exception of the allegations relating to the amount of damages. *See* Fed. R. Civ. P. 8(b)(6); *see also* *DIRECTV, Inc. v. Rawlins*, 523 F.3d 318, 322 n.2 (4th Cir. 2008) (“Due to [the defendant’s] default, we accept [the plaintiff’s] allegations against him as true.”) (citation omitted).

Following a default, a plaintiff may seek entry of judgment. Fed. R. Civ. P. 55(b). Whether to enter a default judgment is within the district court’s discretion, and the court may consider a variety of factors, including:

the amount of money potentially involved; whether material issues of fact or issues of substantial public importance are at issue; whether the default is largely technical; whether plaintiff has been substantially prejudiced by the delay involved; ... whether the grounds for default are clearly established or are in doubt...[;] how harsh an effect a default judgment might have; or whether the default was caused by a good-faith mistake or by excusable or inexcusable neglect on the part of the defendant.

Chapman v. Saber Healthcare Grp., L.L.C., No. 2:20CV106, 2021 WL 12324338, at *1 (E.D. Va. Nov. 1, 2021) (citations omitted).

A default judgment may include permanent injunctive relief. *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 default judgment with permanent injunctive relief); *El Pollo Rico, LLC v. Wings & Pollo, LLC*, No. PWG 21-cv-2346, 2022 U.S. Dist. LEXIS 132472, at *8 (D. Md. July 25, 2022) (same); *Whittingham v. Bluevine Capital, Inc.*, No. 3:17-cv-720-JAG, 2018 U.S. Dist. LEXIS 212252, at *4 (E.D. Va. Dec. 17, 2018) (same); *Microsoft Corp. v. Doe*, No. 1:17-cv-01224-TSE-MSN, 2018 U.S. Dist. LEXIS 202016, at *19 (E.D. Va. Oct. 31, 2018) (“Because

plaintiff sought a default judgment and permanent injunction in its Complaint, plaintiff is entitled to the relief requested in its motion for default judgment and for a permanent injunction.”).

III. STATEMENT OF FACTS

A. Factual Overview

This case arises from Defendants’ misuse of computers in Virginia, Microsoft’s systems, and generative technology for improper and illegal purposes, including the unlawful generation of images depicting misogyny, non-consensual intimate images of celebrities, and other sexually explicit content. FAC ¶¶1-2, 24, 79. Through this action, Microsoft disrupted a sophisticated international scheme involving tools specifically designed to bypass the safety guardrails of generative AI services provided by Microsoft and others. *Id.*; Dkt. 4-2, Declaration of Jason Lyons re TRO Application (“Lyons TRO Decl.”) ¶¶ 33-51. Among other things, this action resulted in the take down of domains and proxy services used to break into Microsoft’s systems and distribute harmful content. Dkt. 34-1, Declaration of Jason Lyons re Preliminary Injunction (“Lyons PI Decl.”) ¶¶2-3 (discussing redirection of domain and Defendants deletion of malicious infrastructure and tool sets). This case also resulted in foreign and domestic law enforcement action. *See, e.g.*, Dkt. 53 (Dismissal as to certain defendants to avoid interference).

Microsoft. Plaintiff Microsoft Corp. is a Washington corporation and is a leading provider of technology products and services, including computer software, Internet services, websites, and email services. FAC ¶ 3. Microsoft has long been a leader in the field of Artificial Intelligence (“AI”), which generally refers to software that imitates human behaviors and capabilities. FAC ¶ 30. Commencing in 2019, Microsoft began a partnership with the AI company OpenAI through a multiyear investment designed to ensure that AI’s benefits are broadly shared with the world. FAC ¶ 31. OpenAI has used Microsoft infrastructure to train its

models, which are now deployed in Azure to power generative AI products like GitHub Copilot, DALL·E and ChatGPT. FAC ¶ 31.

In addition to its technological leadership, Microsoft has also long been at the forefront of setting ethical standards for use of AI. FAC ¶ 32. Microsoft helps customers put responsible AI principles into action by providing educational resources and technical capabilities. FAC ¶ 32. For example, the Microsoft Generative AI Services Code of Conduct (“Code of Conduct”) defines the requirements that all customers of Microsoft Generative AI Services must adhere to in good faith. The Code of Conduct requires customers to ensure that all of their applications built with Microsoft Generative AI Services and Azure AI Content Safety implement controls like human oversight, technical limits on inputs, and various transparency measures. FAC ¶ 53. The Code of Conduct also imposes Content Requirements that prohibit the use of Microsoft Generative AI Services for processing, generating, classifying, or filtering content in ways that can inflict harm. FAC ¶ 55. Microsoft prohibits content that describes, features, or promotes sexual exploitation or abuse, whether or not prohibited by law. Microsoft further prohibits the creation of erotic, pornographic, or otherwise sexually explicit content. FAC ¶ 56. The Code of Conduct, contractual restrictions, and other guidelines for responsible use enhance safety of the Azure OpenAI Service. FAC ¶¶ 55-60.

In addition to the contractual restrictions and the guardrails imposed by the Code of Conduct, the Transparency Note, and Microsoft’s AI principles, Microsoft has also developed technical measures controlling access to and enhancing the safety of the Azure OpenAI Service. FAC ¶ 60. Microsoft technical measures for protecting the safety of the Azure OpenAI Service include Microsoft’s content filtering and abuse detection technologies. Within the Azure OpenAI Service, the OpenAI models are integrated with Microsoft-developed content filtering and abuse

detection models. For example, Azure OpenAI Service includes a content filtering system that works alongside core models, including DALL·E image generation models. This system works by running both the prompt and output through an ensemble of classification models designed to detect and prevent the output of harmful content. The content filtering system detects and takes action on specific categories of potentially harmful content in both input prompts and output completions. The text content filtering models for the hate, sexual, violence, and self-harm categories have been specifically trained and tested on the following languages: English, German, Japanese, Spanish, French, Italian, Portuguese, and Chinese. However, the service can work in many other languages. FAC ¶ 61. In addition to the content filtering system, Azure OpenAI Service performs Abuse Monitoring to detect content and/or behaviors that suggest use of the service in a manner that might violate applicable product terms. Azure OpenAI Service detects and mitigates instances of recurring content and/or behaviors that suggest use of the service in a manner that may violate the Code of Conduct or other applicable product terms. FAC ¶ 66.

Defendants’ Enterprise. Unfortunately, Microsoft’s status as a leader in AI also makes Microsoft a prime target for bad actors. One type of malicious conduct that Microsoft has had to combat concerns malicious use of Microsoft’s Azure OpenAI Service and DALL·E image generation technology to create harmful content. FAC ¶ 33. Here, Defendants devised ways to obtain unlawful access to Microsoft’s systems, circumvent safety mitigations built into OpenAI’s tools and Microsoft’s systems, and generate harmful content using Microsoft systems. FAC ¶ 36. Using stolen API keys and technical circumvention measures, the Defendants in this case gained unauthorized access to the computers and software that provide Microsoft’s Azure-based implementation of OpenAI’s generative AI models (“Azure OpenAI Service”) and used that

unauthorized access to circumvent Microsoft’s safety measures preventing generation and dissemination of harmful content. Defendants used Microsoft’s Azure OpenAI Service to generate thousands of harmful images. FAC ¶ 37.

Defaulting Defendants Yadegrania, Yuen, and Tân, referred to in the FAC as “Infrastructure Provider Defendants” FAC ¶ 10, operated a hacking-as-a-service scheme (“Azure Abuse Enterprise” or “Enterprise”) specifically designed to abuse Microsoft’s Azure infrastructure and software. FAC ¶¶ 80, 128. In brief, Defaulting Defendants provided and trafficked the infrastructure and services that end-users needed to create the harmful content described in the FAC. FAC ¶ 10. The key components of this infrastructure included a software tool named “de3u” and a custom-built “oia reverse proxy” service to generate and communicate HTTP requests that included Azure OpenAI Service API calls configured with stolen API Keys, deployment ID, endpoint address and other information configured by the de3u software and oia reverse proxy. FAC ¶¶ 81-82. 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. These features, combined with unlawful programmatic API access to the Azure OpenAI service via the oia-reverse-proxy service, enabled Defendants to reverse engineer means of circumventing Microsoft’s content and abuse measures. FAC ¶ 88. Through their infrastructure, Defaulting Defendants and/or their end users gained unauthorized access to and use of Microsoft computers running Azure OpenAI services software necessary for processing, routing, filtering, executing, and communicating responses to Azure OpenAI Service API calls.

Id. Images created by Defendants include a C2PA Content Credentials symbol (“CR Icon”) inserted by the Azure OpenAI service.¹ 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 could not have achieved the level of access they achieved without configuring their HTTP requests in a manner designed to circumvent Microsoft’s technological measures for limiting access to and use of the computers and software that comprise the Azure OpenAI Service. FAC ¶¶ 81-82. The actions alleged in the FAC were actions that each Defaulting Defendant authorized, controlled, directed, or had the ability to authorize, control or direct, and/or were actions each Defendant assisted, participated in, or otherwise encouraged, and are actions for which each Defendant benefited from and is liable. FAC ¶ 22. Each Defaulting Defendant aided and abetted the actions of other Defendants and had knowledge of those actions, provided assistance, and benefited from those actions, in whole or in part. Each Defaulting Defendant was the agent of each of the other, and in doing the things alleged in the FAC, was acting within the course and scope of such agency and with the permission and consent of other Defendants. FAC ¶ 22.

Though investigation and discovery, Microsoft learned that the person identified in Microsoft’s original complaint as Defendant DOE 1 is a natural person named Arian Yadegarnia aka “Fiz.” FAC ¶ 4. Defaulting Defendant Yadegarnia appears to reside in the Islamic Republic of Iran. At all times relevant, Yadegarnia had access to and control over instrumentalities used in connection with the violations of law described in the FAC, including at least the website located

¹ Microsoft is a founding member of the Coalition for Content Provenance and Authenticity (“C2PA”). C2PA addresses the prevalence of misleading information online through the development of technical standards for certifying the source and history (or provenance) of media content. It publishes open source standard that allows for insertion of a digital watermark

at “reentry.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.

Defaulting Defendant Ricky Yuen aka “CG-Dot” is a natural person with access to instrumentalities used in connection with violations of law described in the FAC, including an implementation of the oai-reverse-proxy designed to leverage Google’s Cloud Platform (“GCP”) service and what appear to be stolen Google API keys and other customer credentials. FAC ¶ 7. Yuen appears to reside in the Hong Kong Special Administrative Region of the People’s Republic of China.

Defaulting Defendant Phát Phùng Tấn aka “Asakuri” is a natural person with access to and control over instrumentalities used in connection with the violations of law described in this 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. Tấn appears to reside in the Socialist Republic of Vietnam. FAC ¶ 9.

Defaulting Defendants are each members of the Enterprise, which is an ongoing association-in-fact enterprise for purposes of the RICO Act. FAC ¶ 128. The Enterprise’s members function as a continuing unit for the common purpose of achieving the objectives of the Enterprise, 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. FAC ¶ 129. Defaulting Defendants each provided funding, devices, infrastructure, resources, and logistical support needed to conduct the Enterprise. FAC ¶ 134. Defaulting Defendants also sold the Enterprise’s technological capabilities to other malicious actors and provided those other actors with detailed instructions on how to use the Azure Abuse

Enterprise's custom tools to generate harmful content. FAC ¶ 135. The Enterprise has engaged in activities that affect interstate commerce through a pattern of racketeering activity in violation of 18 U.S.C. § 1962. FAC ¶ 137.

Defendants conspired to operate the Azure Abuse Enterprise through a pattern of racketeering activity in furtherance of the common purpose of the Enterprise sometime prior to July 2024. FAC ¶ 138. Thereafter, each Defendant took wrongful acts in furtherance of their unlawful agreement by supplying resources to the Azure Abuse Enterprise. Defendants continuously and effectively carried out the purpose of the Azure Abuse Enterprise from at least July to September 2024, causing harm to the business and property of Microsoft and others. Defendants use of the stolen Azure customer credentials referenced herein to gain fraudulent access to Microsoft's systems would have continued beyond September 2024 but for Microsoft's actions to invalidate and replace those customers' credentials. Defendants represent a continuing threat to Microsoft and others and would likely resume their attacks on the Azure OpenAI Service upon coming into possession of additional stolen customer credentials. FAC ¶ 138.

B. Procedural History

Microsoft filed this action under seal on December 19, 2024 and moved that same day for temporary emergency relief designed to disable the network infrastructure Defendants were using to carry out their scheme. *See* Dkt. 1-13. On December 20, 2024, the Court granted a temporary restraining order against Defendants. Dkt. 21. Also on December 20, 2024, the Court granted Microsoft's motion for expedited discovery (Dkt. 24) and motion for alternative service (Dkt. 25). After effecting the Court's TRO and disabling the core infrastructure provided by the Infrastructure Provider Defendants, Microsoft filed a Notice of Service of Process and Motion to Unseal the case on January 8, 2025. Dkt. 33. On January 10, 2025, the Court held a preliminary

injunction proceeding at which no Defendant appeared. Dkt. 32, 36. On January 10, 2025, the Court entered a preliminary injunction and unsealed this action. Dkt. 35, 38.

Microsoft moved to amend its complaint on February 27, 2025 to add new information and identify individual defendants uncovered during the course of discovery and Microsoft's continued investigation. Dkt. 39 (Motion); Dkt. 39-2 (Declaration of Maurice Mason, "Mason Decl." hereafter) ¶ 7. As noted in Microsoft's Motion to Amend the complaint and supporting declaration of Mr. Mason, after Microsoft serve the complaint and TRO on Defendants, Microsoft investigators observed communications among certain Defendants discussing this case. Dkt. 39-2, Mason Decl. ¶13. Some of those communications included messages doxxing Microsoft's attorneys in this case. Mason Decl. ¶ 15. In addition, Microsoft attorneys received direct communications from person believed to be affiliated with Defendants. Mason Decl. ¶ 18. Defendants also attempted to delete evidence and otherwise obfuscate their identities in response to learning of this case. Mason Decl.¶ 19.

The Court granted Microsoft's motion to amend the complaint on February 27, 2025. Dkt. 40. Microsoft docketed the FAC on February 28, 2025. Dkt. 41. On March 25, 2025, the Court granted Microsoft leave to effect alternative service on Defendant Yadegrania by electronic means and issued summons as to the FAC. Dkt. 45, 46. Microsoft docketed a Certificate of Service on Defendant Yadegarnia on May 28, 2025. Dkt. 51.

On September 17, 2025, Microsoft filed a Rule 41(A)(1)(a)(i) dismissal of Defendants Alan Krysiak and DOES 4-10 in order to avoid interfering with certain criminal investigations, leaving only the Defaulting Defendants remaining in this action. Dkt. 53. On October 1, 2025, after unsuccessful attempts to effect Hauge Convention service on Defendants Yuen, and Tân (*see* Dkt. 55), Microsoft moved for leave to effect alternative service on Messrs. Yuen and Tân

(Dkt. 56), which the Court granted on October 3, 2025. Dkt. 58. Thereafter, Microsoft served Defendants Yuen and Tân using known email addresses and filed a Certificate of Service on October 9, 2025. Dkt. 59.

On November 25, 2025, Microsoft filed a Request for Entry of Default as to Defendants Yadegarnia, Yuen, and Tân. Dkt. 59. The clerk entered Defendants Default on December 1, 2025. Dkt. 61.

IV. ARGUMENT

A. The Court has Jurisdiction

Before entering a default judgement, a district court must ensure it has subject matter and personal jurisdiction. *Sec. & Exch. Comm'n v. Ramaraj*, No. 1:24-CV-1282-CMH-LRV, 2025 WL 1905571, at *4 (E.D. Va. Apr. 22, 2025). Here, the Court has subject matter jurisdiction because the United States district courts are vested with exclusive original jurisdiction over cases involving federal claims like Microsoft's claims under the DMCA, the Lanham Act, and the RICO Act. 28 U.S.C. § 1331; *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 Defendants violations of federal statutes and Virginia common law as part of a scheme to break into Microsoft's systems and misuse those systems to create harmful content. *See, e.g.*, Dkt. 41, FAC ¶¶ 1; 23 (jurisdictional allegations); ¶¶ 79-96 (core factual allegations); ¶¶ 97-159 (federal and state claims incorporating the same factual allegations).

The Court also has personal jurisdiction over Defaulting Defendants, especially because

some of the core infrastructure at issue in this case is in Virginia. FAC ¶¶ 24 (discussing domains and Virginia IP address), 80, 94-96 (discussing AWS Virginia IP address). The Fourth Circuit has synthesized the due process requirements for specific personal jurisdiction into a three-prong test that considers: “(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)).

Purposeful Availment. 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. v. Dmarcian Eur. BV*, 60 F.4th 119, 133 (4th Cir. 2022). Here, all applicable purposeful availment factors weigh in favor of jurisdiction. Although Defendants do not maintain physical offices or human agents within the State, Defendants have effectively set up shop in this Judicial District by choosing websites with top level domains that depend on computers located in Reston, Virginia and a physical AWS IP Address that geolocates to a physical server located in this State. FAC ¶¶ 24; Lyons TRO Decl. ¶ 56. The two key domains, “reentry.org/de3u” and “aitism.net,” are administered by Virginia companies and rely on DNS servers located *inter alia* in Virginia. FAC ¶ 24 (discussing domains and Virginia IP address). Moreover, the default location for storing the harmful images bearing Microsoft’s trademarks was an AWS server with an IP address geolocated in Virginia. FAC ¶¶ 80, 94-96. Defendants

have acted at all times relevant with knowledge that their acts would cause harm through computers located in Virginia thereby injuring Plaintiff, its customers, and others in Virginia and the United States. FAC ¶ 25.

This case involves an interactive website that depends on physical computers located in Virginia in order to receive commands and serve content to end users. When Defendants' malicious Reverse Proxy Service received harmful images in response to Defendants' use of the de3u software, those images were returned to a computer at the AWS IP address that is physically located in Virginia. Defendants established "continued interaction with their website" infrastructure in Virginia and manifested an intent to carry out their virtual business from within the state. *Id.*; Lyons TRO Decl. ¶ 56. These facts support jurisdiction. *See, e.g., Bright Imperial Ltd. v. RT MediaSolutions, S.R.O.*, Civil Action No. 1:11-cv-935-LO-TRJ, 2012 U.S. Dist. LEXIS 70000, at *23 (E.D. Va. May 18, 2012); *see also Batts v. Snap Inc.*, No. 2:23-cv-03565-DCN, 2024 U.S. Dist. LEXIS 139286, at *18 (D.S.C. July 6, 2024) ("viewed in the context of other jurisdictionally relevant facts...Kurbanov, through his websites, had purposefully availed himself of the privilege of conducting business in Virginia.") (discussing *UMG Recordings, Inc. v. Kurbanov*, 963 F.3d 344 (4th Cir. 2020)).

Activities Directed at the State. Plaintiffs' claims all arise from Defendants' use of the de3u software, Reverse Proxy Service, and AWS IP address to gain unauthorized access to Microsoft's systems and generate images for delivery to and through computers in Virginia. Where affected computers are located within the district, and when Defendants' intentional acts cause those computers to effect the harms complained of, jurisdiction is appropriate. *See, e.g., Bright Imperial*, 2012 U.S. Dist. LEXIS 70000, at *23; *Batts*, 2024 U.S. Dist. LEXIS 139286, at *18 (citation omitted).

Constitutional Reasonableness. Exercising jurisdiction in Virginia easily satisfies the standard of constitutional reasonableness. “Because [Defendants’] actions were so directly connected to” the reentry.org domain, the AWS IP address, and oai reverse proxy service, all of which are effectively Virginia-based infrastructure, “it is not necessary that [Defendants] step foot in Virginia...so as not to offend the traditional notions of fair play and substantial justice inherent in our Constitution’s Due Process Clause.” *Bright Imperial*, 2012 U.S. Dist. LEXIS 70000, at *39-40 (E.D. Va. May 18, 2012). “Quite the contrary, it would offend substantial justice to permit” Defendants “to avoid accountability here simply because [they] conducted [their] affairs abroad” in part. *Id.* “It is the ever evolving nature of technology that makes it possible for a foreign defendant to so directly impact the United States...and it would be illogical to permit...individual[s] allegedly responsible for each of the injurious decisions [at issue] to escape the grasps of this Court’s judicial authority.” *Id.*

National Contacts. “When a defendant’s contacts with a single state are insufficient to establish personal jurisdiction within that state, but the defendant’s contacts with the United States as a whole are sufficient to establish jurisdiction, any state within the United States may exercise jurisdiction over the defendant under Rule 4(k)(2).” *Id.* at *23-24. “This Rule permits jurisdiction when (i) a claim arises under federal law, (ii) the defendant is not subject to jurisdiction in any state court, and (iii) exercising jurisdiction does not offend the constitution or laws of the United States.” *See* Fed. R. Civ. P. 4(k)(2). Rule 4(k)(2) is easily satisfied here. If Defendants are not subject to jurisdiction in Virginia specifically, they are surely subject to jurisdiction in the United States due to their multiple ongoing contacts with the United States as a whole. FAC ¶ 26 (cataloguing U.S. business activities); Lyons TRO Decl. ¶ 57 (same). Defendants configured their software and systems to use physical machines, technology, and

services provided in and from the United States by Microsoft; configured their software and systems to use physical machines, technology, and services provided in and from the United States by Amazon Web Services (“AWS”), a U.S. company; configured their software and systems to victimize U.S. companies like Microsoft, OpenAI, AWS, Cloudflare, PIR, and Verisign; and configured their software and systems to create and distribute harmful images within the U.S. *Id.* These sustained and purposeful acts within, towards, and concerning the United States make it constitutionally reasonable for Defendants to be hauled into court here. “Since such nationwide contacts would satisfy any general personal jurisdiction test, unless inconvenience rises to a level of constitutional concern...minimum contacts with the United States” supports “subjecting [Defendants] to personal jurisdiction” and does not offend the rights protected by the Due Process Clause of the Fifth Amendment. *Noble Sec., Inc. v. MIZ Eng’g, Ltd.*, 611 F. Supp. 2d 513, 553 (E.D. Va. 2009).

B. All Relevant Default Factors Favor Default Judgment

The factors a court may consider in deciding a default motion include: “the amount of money potentially involved; whether material issues of fact or issues of substantial public importance are at issue; whether the default is largely technical; whether plaintiff has been substantially prejudiced by the delay involved; whether the grounds for default are clearly established or are in doubt; how harsh an effect a default judgment might have; or whether the default was caused by a good-faith mistake or by excusable or inexcusable neglect on the part of the defendant.” *Chapman*, 2021 U.S. Dist. LEXIS 273959, at *4 (cleaned up). These factors weigh in favor of a default judgment here.

First, Microsoft is not seeking a default judgment as to damages. This factor weighs in favor of entering a default judgment. *See, e.g., Stihl Inc. v. Kinetic Ceramics, LLC*, No.

2:22cv111, 2023 U.S. Dist. LEXIS 237366, at *16 (E.D. Va. Feb. 9, 2023) (“\$20,000 is not so significant that it would shock the conscience if it were entered by default judgment”). Second, there are no material issues of fact—the record contains multiple sworn declarations and a wealth of documentary evidence establishing that Defendants have in fact committed the alleged wrongful acts. *See, e.g.*, Dkt.4-1 through Dkt. 4-30; Dkt. 34-1; Dkt. 39-39 through Dkt. 39-22. *Stihl Inc. v. Kinetic Ceramics, LLC*, No. 2:22cv111, 2023 U.S. Dist. LEXIS 237366, at *16 (E.D. Va. Feb. 9, 2023). Nor can there be any serious dispute about whether the conduct Defendants engaged in is unlawful, or whether Microsoft should be able to vindicate its rights to protect its computer systems and intellectual property. *See, e.g.*, *SRL v. Lingxian Guangzhou Technol-Ogy Co., Ltd.*, No. 2:21cv337, 2021 U.S. Dist. LEXIS 263977, at *8 (E.D. Va. Oct. 21, 2021) (relief that “primarily affects the private interests of the business entities involved...is not of such substantial public importance that it cannot be decided on default.”).

Third, the default is not “largely technical.” Although the entry of default was filed on December 1, 2024, Defaulting Defendants “have still not made an appearance on the docket.” *Cadence Bank, N.A. v. Draam*, No. 2:24cv305, 2025 U.S. Dist. LEXIS 111291, at *17-18 (E.D. Va. Jan. 10, 2025); *accord Mayrant v. Norfolk Redevelopment & Hous. Auth.*, No. 2:24cv715, 2025 U.S. Dist. LEXIS 192852, at *28 (E.D. Va. Sep. 23, 2025).

Fourth, Microsoft has been substantially prejudiced by Defendants’ refusal to participate in this action. *Conyers v. Guyton*, No. 2:23cv689, 2024 U.S. Dist. LEXIS 248982, at *20 (E.D. Va. Aug. 26, 2024) (“Plaintiff has been prejudiced by Defendants’ delay”); *Sierra Software, LLC v. Malih*, No. 2:17cv607, 2019 U.S. Dist. LEXIS 250703, at *4 (E.D. Va. Feb. 15, 2019) (“Due to Defendants’ failure to appear, Plaintiff is prejudiced because it cannot calculate actual damages with precision and has accrued additional litigation costs.”); *Synopsys, Inc. v. Sunlune*

Corp., No. 24-cv-00220-BLF, 2025 U.S. Dist. LEXIS 97297, at *18 (N.D. Cal. May 21, 2025) (defaulting defendant’s spoliation of evidence weighed in favor of maintaining default judgment). “Default judgment is appropriate when the adversary process has been halted because of an essentially unresponsive party.” *George v. Brown*, Civil Action No. 3:24CV318 (RCY), 2025 U.S. Dist. LEXIS 259131, at *6 (E.D. Va. Dec. 15, 2025)(citation omitted).

Fifth, “the grounds for default here are clearly established by the factual and procedural history,” including the evidentiary record and the Court’s multiple orders granting preliminary injunctive relief. *See Wells Fargo Commer. Distribution Fin., LLC v. Shore Saw & Mower, Inc.*, No. 2:23-cv-100, 2023 U.S. Dist. LEXIS 140218, at *10 (E.D. Va. Aug. 10, 2023); *see also* Dkt. 21 (TRO); Dkt. 38 (Preliminary Injunction). Microsoft’s well-pleaded claims and supporting evidence have supported multiple requests for preliminary relief, and “Defendant has not contested any of the facts alleged in the complaint, which are taken as admitted after the entry of default.” *Stihl*, 2023 U.S. Dist. LEXIS 237366, at *16. There is substantial evidence in the record proving the merits of Microsoft’s claims. *See, e.g.*, Dkt.4-1 to Dkt. 4-30; Dkt. 34-1; Dkt. 39.

Sixth, the default requested is not “harsh” in the context of this case. All the default judgment will do is maintain the *status quo* prohibitions on Defendants’ continued unlawful activity. *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 in case involving similar facts and procedural history); *Microsoft Corp. v. Doe*, No. 1:17-cv-01224-TSE-MSN, 2018 U.S. Dist. LEXIS 202016, at *19 (E.D. Va. Oct. 31, 2018) (same); *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).

Seventh, it is clear that the default was not caused by a good-faith mistake or by excusable neglect on the part of the Defaulting Defendants. *Compare Synopsys*, 2025 U.S. Dist. LEXIS 97297, at *18 (no good faith or excusable neglect where party intentionally failed to respond to complaint and engaged in evidence spoliation). Defaulting Defendants obtained actual notice of this action and some even took measures to cover their tracks in response to receiving notice. Mason Decl. ¶ 19. Although the entry of default was filed on December 1, 2025, Defaulting Defendants “have still not made an appearance on the docket”—“[g]iven the amount of time that has elapsed, and absent any communication from Defendants suggesting otherwise...Defendants’ default is not due to good faith mistake or neglect.” *Cadence*, 2025 U.S. Dist. LEXIS 111291, at *17-18. The time between the Clerk’s entry of default in December and Microsoft’s instant motion has been more than enough time to warrant a finding that Defendant’s default is not the result of good-faith mistake or excusable neglect. *See, e.g., Cadence*, 2025 U.S. Dist. LEXIS 111291, at *17-18 (two months between Clerk’s default and motion for default judgement); *accord Mayrant v. Norfolk Redevelopment & Hous. Auth.*, No. 2:24cv715, 2025 U.S. Dist. LEXIS 192852, at *28 (E.D. Va. Sep. 23, 2025) (less than one month between entry of default and motion for default judgment).

C. A Permanent Injunction is Appropriate

“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 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.*, 2017 U.S. Dist. LEXIS 145448, at *17 (E.D. Va. Aug. 1, 2017) (granting motion for default and imposing permanent injunction); *Toolchex*, 2009 U.S. Dist. LEXIS 64186, at *18 (same); *Whittingham*, 2018 U.S. Dist. LEXIS 212252, at *4 (same); *Synopsys*, 2025 U.S. Dist. LEXIS 97297, at *18; *Synopsys, Inc. v. Sunlune Corp.*, No. 24-cv-00220-BLF, 2024 U.S. Dist. LEXIS 208388, at *17 (N.D. Cal. Nov. 15, 2024) (same).

The Court previously determined that Microsoft 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. 21 (TRO); Dkt. 38 (Preliminary Injunction). The only material development since the Court's Preliminary Injunction order is that the facts alleged in the FAC have now all been deemed admitted. Accordingly, preliminary injunctive relief remains appropriate. Defendants have violated the CFAA by using stolen credentials to bypass authentication gates, which is an archetypical example of unauthorized access to computer systems. *See e.g., Microsoft Corp. v. Does*, Civil Action No. 1:22cv607 (LMB/WEF), 2024 U.S. Dist. LEXIS 76088, at *26-27 (E.D. Va. Jan. 10, 2024) (collecting cases). Defendants' also violated the DMCA through use of a reverse proxy tool configured with a library of stolen keys and credentials. *Philips Med. Sys. Nederland B.V. v. TEC Holdings, Inc.*, No. 3:20-cv-21-MOC-DSC, 2023 U.S. Dist. LEXIS 7319, at *34-35 (W.D.N.C. Jan. 17, 2023). Defendants also violated the Lanham Act by distributing harmful images containing Microsoft's "Azure" trademark. *See Garden & Gun, LLC v. Twodalgalis, LLC*, 2008 U.S. Dist. LEXIS 79982 (W.D.N.C. 2008). And because Defendants engaged in a pattern of wire fraud and access device fraud in furtherance of conducting the RedVDS enterprise, Defendants also violated the RICO Act. *See, e.g., Field v. GMAC LLC*, 660 F. Supp. 2d 679, 686 (E.D. Va. 2008). Defendants

conduct was also tortious under Virginia law. *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]”); *Bay Tobacco, LLC v. Bell Quality Tobacco Prod., LLC*, 261 F. Supp. 2d 483, 500 (E.D. Va. 2003) (tortious interference).

All of the foregoing conduct causes irreparable harm and warrants injunctive relief. *Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (injunction to dismantle botnet command and control servers); *Umg Recordings v. Kurbanov*, Civil Action No. 1:18-cv-957 (CMH/TCB), 2021 U.S. Dist. LEXIS 250844, at *32 (E.D. Va. Dec. 16, 2021) (“Plaintiffs have lost the ability to control how their Works are distributed. Ultimately, this loss of control makes monetary damages inadequate as Defendant’s conduct will continue to harm Plaintiffs in the future absent an injunction.”); *Synopsys, Inc. v. AzurEngine Techs., Inc.*, 401 F. Supp. 3d 1068, 1074 (S.D. Cal. 2019) (similar, collecting cases). Consumer confusion and injury to business goodwill constitute irreparable harm. *See, e.g., Int’l Labor Mgmt. Corp. v. Perez*, 2014 U.S. Dist. LEXIS 57803, 35 (M.D.N.C. Apr. 25, 2014) (damage to “reputation and loss of goodwill constitutes irreparable harm for purposes of injunctive relief”).

The balance of equities and public interest also weigh in favor of a permanent injunction in light of the record evidence. *See, e.g., US Airways, Inc. v. US Airline Pilots Ass’n*, 813 F. Supp. 2d 710, 736 (W.D.N.C. 2011); *Pesch v. First City Bank of Dallas*, 637 F. Supp. 1539, 1543 (N.D. Tex. 1986) (balance of hardships clearly favors injunction where enjoined activity is illegal). The public has a strong interest in enforcing laws like the CFAA, DMCA, and Lanham Act. *See, e.g., BSN Med., Inc. v. Art Witkowski*, 2008 U.S. Dist. LEXIS 95338, 10 (W.D.N.C. Nov. 21, 2008) (“In a trademark case, the public interest is ‘most often a synonym for the right of the public not to be deceived or confused.’ . . .the infringer’s use damages the public

interest.”) (citation omitted); accord *Meineke Car Care Ctrs., Inc. v. Bica*, 2011 U.S. Dist. LEXIS 118171, 10 (W.D.N.C. Oct. 12, 2011) (similar); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 32 (E.D. Va. Jan. 6, 2014) (public interest weighed in favor of injunction to enforce CFAA). The public also has a strong interest in disrupting criminal enterprises operating in violation of the RICO Act. See, e.g., *Amazon.com, Inc. v. WDC Holdings LLC*, Civil Action No. 1:20-cv-484, 2020 U.S. Dist. LEXIS 134555, at *31 (E.D. Va. July 28, 2020) (granting injunction to enjoin RICO enterprise conduct).

V. CONCLUSION

For the foregoing reasons, Microsoft respectfully requests that its motion be granted in its entirety.

Dated: February 17, 2026

Respectfully submitted,

/s/ Sten Jensen

STEN JENSEN (VA Bar No. 38197)
sjensen@orrick.com
JOSHUA POND (VA Bar No. 68545)
jpond@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
2100 Pennsylvania Avenue NW
Washington, D.C. 20037
Telephone: + 202 339 8400
Facsimile: + 202 339 8500

ROBERT L. URIARTE (*Pro Hac Vice*)
ruriarte@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
355 S. Grand Ave.
Ste. 2700
Los Angeles, CA 90017
Telephone: + 1 213 629 2020
Facsimile: + 1 213 612 2499

JACOB M. HEATH (*Pro Hac Vice*)
jheath@orrick.com

ANA M. MENDEZ-VILLAMIL (*Pro Hac Vice*)
amendez-villamil@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
The Orrick Building
405 Howard Street
San Francisco, CA 94105
Telephone: + 1 415 773 5700
Facsimile: + 1 415 773 5759

Of Counsel:

RICHARD BOSCOVICH
rbosco@microsoft.com
MICROSOFT CORPORATION
Microsoft Redwest Building C
5600 148th Ave NE
Redmond, Washington 98052
Telephone: +1 425 704 0867
Facsimile: +1 425 706 7329
Attorneys for Plaintiff
MICROSOFT CORPORATION