UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

Microsoft Corporation, a Washington State Corporation and Health-ISAC, Inc., a Florida non-profit organization,
 	
            Plaintiffs,
 	
        v.
 	
Saad Fridi,
 	
and
 	
John Does 1-4, Controlling A Computer Network and Thereby Injuring Plaintiffs and Their Customers,
 	
            Defendants.
	Case No.
	
	FILED UNDER SEAL
	PURSUANT TO LOCAL RULE 5

PLAINTIFFS' MEMORANDUM OF LAW IN SUPPORT OF *EX PARTE* APPLICATION FOR TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Pursuant to Rule 65 of the Federal Rules of Civil Procedure, Plaintiff Microsoft Corporation ("Microsoft") and Health-ISAC, Inc. ("Health-ISAC") (collectively, "Plaintiffs"), respectfully submit this Memorandum of Law in Support of their Motion for an Emergency *Ex Parte* Temporary Restraining Order ("TRO") and a Preliminary Injunction against Saad Fridi and John Does 1-4, (collectively "Tycoon 2FA Defendants").

I.   INTRODUCTION

This action involves the relentless and persistent phishing attacks conducted and facilitated by a foreign cybercrime organization designated as "Tycoon 2FA Defendants" against Microsoft its customers, and the public. One of the most pernicious forms of cybercrime is known as "phishing." Phishing is the fraudulent practice of sending emails or other messages purporting to be from legitimate senders to induce recipients to reveal personal information, such as passwords

or other credentials. It is a form of social engineering and a scam where the recipient-victim is convinced to interact with the correspondence (referred to as the "lure").[1]

Tycoon 2FA Defendants manufacture and sell phishing kits that are designed to allow users of the kit to steal sensitive information, compromise business email and perpetrate ransomware and financial fraud. Tycoon 2FA Defendants advertise products that target Microsoft services, as well as those from other companies like Adobe, Google, and GoDaddy. This business model of selling phishing kits and services for use by other cybercriminals is referred to as "Phishing-as-a-Service" or "PhaaS." The Tycoon 2FA Defendants sell these PhaaS kits to downstream cybercriminals who use these do-it-yourself- kits and the accompanying technical infrastructure to perpetrate phishing attacks at high volume against American companies. The Tycoon 2FA Defendants operate, oversee, and administer a vast cybercriminal infrastructure comprised of hundreds of kit purchasers and hundreds of domains that operate together in connection with phishing attacks against Microsoft, its customers, Health-ISAC, its member organizations, and the public.

Each time a phishing kit is sold, it is done with the express purpose of hacking into Microsoft's products and systems, targeting Microsoft customers, or deceiving the public to believe that Microsoft is responsible for the cybercrime through Tycoon 2FA Defendants' deceptive, illegal, and unauthorized use of Microsoft's branding and logos.

These unlawful acts cause Microsoft and Health-ISAC irreparable harm for which no monetary recourse is available or sufficient. Plaintiffs seek *ex parte* injunctive relief to transfer

---

[1] The estimated financial impact of phishing in 2024 is over $3.5 billion US. Microsoft, *Microsoft Digital Defense Report 2024*, at p. 34, available at https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf (Oct. 2024) ("2024 *MDDR*").

ownership of the Defendants' domains to Microsoft and cripple Tycoon 2FA Defendants' ability to carry out their phishing operation.

Ex parte relief is essential. Tycoon 2FA Defendants actively take steps to conceal their operation and infrastructure. Notice to Tycoon 2FA Defendants would provide them with an opportunity to destroy, move, conceal, or otherwise make inaccessible the instrumentalities they use to direct Tycoon 2FA operations and the evidence of their unlawful activity. Multiple courts in multiple jurisdictions, including this Court, have granted Microsoft the same *ex parte* relief requested here and enjoined cybercriminals from continuing cyber-attacks against Microsoft customers.[2] Plaintiffs respectfully request that this Court grant the same here.

II.   STATEMENT OF FACTS

A. Microsoft's Services and Reputation

Microsoft is one of the world's leading technology companies, providing complete, open, and integrated computer software programs and hardware systems to individuals, businesses, and governments. Declaration of Derek Richardson ISO *Ex Parte* TRO Application ("Richardson Decl.") ¶ 2. Microsoft is a provider of the Windows computer operating system, and a variety of other software and services including Microsoft365, Office 365, Azure, and Outlook.[3] *Id.* Due to

---

[2] *See, e.g.*, *Microsoft and Health-ISAC v. Joshua Ogundipe and John Does 1-4*, 1:25-cv-07111 (S.D.N.Y. Aug. 2025) (Rakoff, J.); *Microsoft and LF Projects v. Abanoub Nady and John Does 1-4*, 1:24-cv-2013-RDA (E.D. Va. Nov. 13, 2024) (Alston, J.); *Microsoft and NGO-ISAC v. John Does 1-2*, Case No. 1:24-cv-02719-RC (D.D.C. Sep. 24, 2024), (Contreras, J.); *Microsoft Corporation v. Tu et al.*, Case No. 23-cv-10685 (S.D.N.Y Dec. 13, 2023) (Engelmayer, J.); *Microsoft, Fortra, and Health ISAC v. John Does 1-16* Case No. 23-cv-2447 (E.D.N.Y. 2023); *Microsoft, FS-ISAC, Health-ISAC v. Denis Malikov and John Does 1-4*, Case No. 1:22-cv-1328-MHC (N.D. Ga. 2022); *Microsoft v. John Does 1-2*, Case No. 1:19-cv-00716-ABJ (D.C. 2019) (Berman-Jackson, J.); *Microsoft v. John Does 1-2*, Case No. 1:19-cv-01582 (E.D. Va. 2019) (O'Grady, J.); *Sophos v. John Does 1-*2, Case No. 1:20-cv-00502 (E.D. Va. 2020); *Microsoft v. John Does 1-2,* Case No. 1:20-cv-00730 (E.D. Va. 2020) (O'Grady, J.); *DXC Technology Company v. John Does 1-2,* Case No. 1:20-cv-00814 (E.D. Va. 2020) (Alston, J.); *Microsoft and FS-ISAC v. John Does 1-2,* Case No. 1:20-cv-1171 (E.D. Va. 2020) (Trenga, J.).

[3] Microsoft 365 and Office 365 are product families of productivity software, collaboration and cloud-based services owned by Microsoft. Microsoft 365 and Office 365 include Microsoft Office, which is a bundle of productivity applications that contains, among other things: a word processor (Word), a spreadsheet

the high quality and effectiveness of Microsoft's products and services, the expenditure of significant resources by Microsoft to market those products and services, and the security services Microsoft provides to its customers to protect its systems against cyberattacks, Microsoft has generated substantial goodwill with its customers, establishing a strong brand and world-wide symbols that are well-recognized within its channels of trade. *Id.* Microsoft has registered trademarks representing the quality of its products and services and its brand, including Microsoft®, Windows®, Microsoft 365®, Office365®, Office®, Microsoft Office®, SharePoint®, OneDrive®, Outlook®, Microsoft Exchange Server®, and Excel®. Complaint, Appendix B (Microsoft Trademark Registrations).

B. Health-ISAC Services and Reputation

Plaintiff Health-ISAC is a non-profit membership organization comprised of public and private hospitals, ambulatory providers, health insurance payors, pharmaceutical/biotech manufacturers, laboratories, diagnostic, medical device manufacturers, medical schools, medical R&D organizations and other relevant health sector stakeholders. Declaration of Errol Weiss ISO *Ex Parte* TRO Application ("Weiss Decl.") ¶ 3. Health-ISAC represents the interests of its healthcare industry members in combating and defending against cyber threats that pose risk and loss to the industry. *Id.*

C. Tycoon 2FA Defendants Control Phishing Operation

1.Who are the Tycoon 2FA Defendants?

Tycoon 2FA Defendants are cyber criminals who manufacture and sell Tycoon 2FA-branded phishing kits and provide PhaaS to other cybercriminals, who then launch phishing attacks

---

program (Excel), a presentation program (PowerPoint), and an email client (Outlook). Microsoft Azure, or just Azure, is the cloud computing platform developed by Microsoft. It offers management, access and development of applications and services to individuals, companies, and governments through its global infrastructure.

against a multitude of organizations across various industries. Richardson Decl. ¶ 7. Tycoon 2FA

Defendants first emerged in Fall 2023. Richardson Decl. ¶ 13.

The phishing operation is carried out by Defendants Saad Fridi and John Does 1-4. *Id.*

Richardson Decl. ¶ 18, 19, 22-24. Microsoft has attributed the Tycoon 2FA Defendants'

cybercriminal activity to Defendant Saad Fridi by using information from his Microsoft accounts,

information that he made available in connection with selling the phishing kits, and open-source

intelligence. Richardson Decl. ¶¶ 18-19. Defendant Fridi resides in and operates from Pakistan.

Id. ¶ 19. Microsoft investigators conducted a test buy, purchasing a one-month subscription to the

Tycoon 2FA phishing kit. This allowed Microsoft to access the control panel, which is provided

with the kit, launch test phishes against Microsoft dummy accounts, and assess the operability and

scope of these kits. Richardson Decl. ¶¶ 33-35. As part of the test buys, Microsoft received

cryptocurrency payment information from Tycoon 2FA Defendants, which Microsoft was able to

trace and determine the financial scope of Defendants' operation. Richardson Decl. ¶¶ 33, 44-46.

The Tycoon 2FA Defendants operate in a fashion similar to other threat actors that have been

enjoined by U.S. federal courts such as the "RaccoonO365 Defendants" and the "Fake ONNX

Defendants." Both sold do-it-yourself phishing kits and operated as a PhaaS. Richardson Decl.

¶¶ 12-13. In November 2024, Microsoft filed a lawsuit in the Eastern District of Virginia and

obtained injunctive relief effectively crippling Fake ONNX's cybercriminal operations. *See*

Microsoft Corporation and LF Projects LLC v. Abanoub Nady and John Does 1-4, Civil Action

No. 1:24-cv-2013-RDA (E.D. VA. Nov. 12, 2024) (Alston, J.). In August 2025, Microsoft and

Health-ISAC filed a lawsuit in the Southern District of New York and obtained injunctive relief

(temporary restraining order and preliminary injunction), effectively crippling RaccoonO365's

cybercriminal operation. *Microsoft and Health-ISAC v. Joshua Ogundipe and John Does 1-4*,

1:25-cv-07111 (S.D.N.Y. Aug. 2025) (Rakoff, J.). Given the successful takedown of Fake ONNX and Tycoon 2FA, the Tycoon 2FA Defendants have steadily become the largest PhaaS operation (based on number of phishing attacks attributable to the Tycoon 2FA kit). Tycoon 2FA began their operations in Fall 2023. By Fall 2025, Tycoon 2FA was considered the most prolific PhaaS operation by volume. Richardson Decl. ¶ 13; Declaration of Selena Larson ISO Plaintiffs' *Ex Parte* Application for TRO ("Larson Decl.") ¶ 5. For example, by August 2025, internal Microsoft telemetry revealed that 62 percent of the phishing attacks blocked by Microsoft involved the use of the Tycoon 2FA kits. Richardson Decl. ¶ 17.

2.Tycoon 2FA Defendants' *Modus Operandi*

Much like how companies develop and sell all-in-one do-it-yourself kits to normal customers for personal projects, Tycoon 2FA Defendants develop do-it-yourself phishing kits for cybercriminals to purchase and use for their cybercrime operations. Richardson Decl. ¶ 26. The purchasers of these kits become part of the Tycoon 2FA Defendants' operation when they, in turn, use the Tycoon 2FA kit to create templates to conduct phishing and leverage the AiTM model[4] by positioning themselves between communications directed to and from Microsoft customers. *Id.*.

The purchasers of the Tycoon 2FA kits become part of the Tycoon 2FA infrastructure when they purchase a subscription, deploy the Tycoon 2FA-branded phishing kits, conduct phishing attacks, use the stolen credentials to infiltrate the victims' systems, and leverage this infiltration to conduct additional cybercrimes, such as ransomware attacks. Richardson Decl. ¶ 28.

---

[4] The Tycoon 2FA-branded phishing kit allows cyber criminals to infiltrate the systems of Microsoft customers undetected and collect the usernames and passwords of the users of the infiltrated network. This is known as AiTM, which is a form of cyberattack where the malicious actor intercepts communications between two parties without their knowledge. It is particularly common for AiTM attacks to leverage PhaaS platforms given the high volume of phishing emails that these phishing kits make possible. This enables these criminals to then enter the system using these purloined credentials and remain undetected. Microsoft has identified AiTM attacks as one of the Top 5 PhaaS models by volume. 2024 MDDR at 34-35.

Defendants advertise that their kits can circumvent the security features of Microsoft products. In reality, the kits do not exploit any alleged Microsoft vulnerability. Richardson Decl. ¶ 7. Rather, the kits misuse Microsoft logos and mimic the appearance of authentic communications to deceive victims into thinking that the email communication they receive, the files they are directed to open, or links to websites used to enter their personal credentials are authentic and Microsoft-approved. Richardson Decl. ¶¶ 7, 28. By doing so, Tycoon 2FA Defendants capitalize on and misuse the brand recognition that Microsoft has cultivated and the trust Microsoft has built with its customers. Richardson Decl. ¶ 43. When a victim clicks on a weaponized link or attachment, the Tycoon 2FA Defendants are essentially ushered in through the front door of the victim's system. Richardson Decl. ¶ 7.

These malicious phishing kits support credentials theft, information exfiltration, and subsequent end-user terminal attacks which include business email compromise, ransomware, and financial fraud. Richardson Decl. ¶ 28. Tycoon 2FA Defendants are able to execute these end-user terminal attacks more readily when they are able to access a victim's Microsoft platform, which serves as a gateway to other computer applications, and where these applications are connected by a global Microsoft network infrastructure. *Id.*, n. 8. These features are the "selling points" of the phishing kits, and Tycoon 2FA Defendants advertise the kits' abilities to target Microsoft customers. Richardson Decl. ¶¶ 16, 28.

The Tycoon 2FA Defendants' phishing operation is made possible by leveraging a vast infrastructure of website domains. Richardson Decl. ¶ 20. Also known as a web address, domains are used to identify a website and allow users on the internet to access the website. *Id.* Tycoon 2FA Defendants include the domains in their phishing emails and when the victims click on the malicious domains they are redirected to a Tycoon 2FA-controlled webpage and then unknowingly

provide their credentials to Defendants. *Id.* Microsoft has identified 330 illegal domains in **Appendix A** to Plaintiffs' concurrently filed Complaint; and also attached as **Exhibit 1** to the Declaration of Jeffrey L. Poston in Support of Plaintiffs' *Ex Parte* TRO Application ("Poston Decl.") ¶ 7. This action seeks to take down this technical infrastructure to render Tycoon 2FA Defendants incapable of continuing their attacks and transferring ownership and control of these 330 domains to Microsoft. Richardson Decl. ¶¶ 56-59.

3. The Attack Chain

Step 1: Development and Sale of Tycoon 2FA-Branded Phishing Kits

Much like how an e-commerce business sells its products in online stores for consumers to purchase, Tycoon 2FA Defendants sell their Tycoon 2FA-branded online, primarily using Telegram Messenger, a cloud-based, cross-platform, instant messaging service, to facilitate the sales. Richardson Decl. ¶ 29. The phishing kits are offered as a monthly subscription, with different package options ranging in prices based on the number and type of domains provided as well as kit- distinct package features, similar to the way the software subscription services offer different-priced subscription tiers. Richardson Decl. ¶ 30.

A subscription also includes access to the control panel. Richardson Decl. ¶ 31. The control panel, or dashboard, allows its customers to select and customize the pre-configured templates for their phishing campaigns, track recipients of phishing emails, track whether a phishing attack has been successful, track stolen credentials, and measure other metrics that Customer can use to assess the success of their cybercriminal activity. *Id.*

From the control panel, a purchaser of the Tycoon 2FA kit has access to customizable pre-configured templates (HTML links, PDFs, QR codes, etc.) with themes that a user can select for its phishing (for example, an email template containing a link to a "time sensitive" document).

Richardson Decl. ¶ 17. The Tycoon 2FA users choose which domains they want to be included in each of their templates that they download from the control panel. Richardson Decl. ¶ 20. Tycoon 2FA users send emails to encourage the victims to click on the malicious domains where they are redirected to a Tycoon 2FA-controlled webpage and then unknowingly provide their credentials to Defendants. *Id*.

The Tycoon 2FA Defendants do not just sell their phishing kit for one-time use. Richardson Decl. ¶ 31. By selling subscriptions on a monthly basis, Tycoon 2FA Defendants encourage their customers to become repeat purchasers and repeat attckers. *Id.* Additionally, Tycoon 2FA Defendants accept multiple forms of cryptocurrency as payment. Richardson Decl. ¶ 32. By diversifying the accepted method of payment, more customers are likely to purchase the kits. *Id*.

Step Two: Using the Tycoon 2FA Kit to Conduct Phishing Attacks

Once a cybercriminal purchases the Tycoon 2FA-branded phishing kit, they are granted access to the control panel and can begin phishing. Richardson Decl. ¶ 31.

With minimal effort, Tycoon 2FA Defendants can customize the phishing lures to target a myriad of victims across various industries, making it easy for Tycoon 2FA Defendants to scale their cybercriminal activity and target sensitive-information rich targets. Richardson Decl. ¶ 16. For example, the user can select which domain it wants to use in connection with the phishing email and the customized countermeasure it seekd to avoid detection. Richardson Decl. ¶¶ 20, 39.

The Tycoon 2FA Defendants who have purchased the kits will send phishing emails to victims that prompt the victim to click on a link. Richardson Decl. ¶ 36. The Tycoon 2FA kits give their customers the ability to customize the phishing email to promote greater efficacy. Richardson Decl. ¶¶ 31, 34. Tycoon 2FA Defendants use, without authorization, Microsoft's logos

and format to lull the victim into believing the website that the victim is directed to is legitimate. Richardson Decl. ¶¶ 28, 53. For example, a victim may receive a message with a link to a SharePoint document, with a message that the document requires "urgent" attention. Richardson Decl. ¶ 34.

Once the victim clicks on the link, she is redirected multiple times until the victim is taken to a login screen that mimics a Microsoft login screen. Richardson Decl. ¶ 36. The victim, thinking that this is a legitimate login page (and not one that is controlled by Tycoon 2FA Defendants) will enter her credentials. *Id.* As a final step, the victim is redirected to a legitimate Microsoft webpage, so that the victim has no reason to be suspicious of the process. *Id.* ¶ 36. The multi-layer redirection is a feature that differentiates Tycoon 2FA from other phishing kits that offer a single level of redirect. Richardson Decl. ¶¶ 13, 21. The 3-4 redirects demonstrate a technical sophistication and further obfuscates the cybercriminal operation. *Id.* ¶ 21.

The Tycoon 2FA Defendants are able to intercept the credentials and any session cookies. Richardson Decl. ¶ 26, n. 7. The credentials are delivered via a text file to the control panel, and the Tycoon 2FA Defendants now have the ability to log into each of the Microsoft services associated with the phished credentials for the victim. Richardson Decl. ¶ 28. The Tycoon 2FA Defendants subsequently exploit this access to their victim's devices to perpetrate further cybercrime such as ransomware, business email compromise, and financial fraud. Richardson Decl. ¶ 37.

Test Buy

Microsoft's Digital Crimes Unit ("DCU") is a Microsoft team responsible for protecting Microsoft and its customers against cybercrime threats. DCU is an international team of technical, legal, and business experts that has been fighting cybercrime, protecting individuals and

organizations, and safeguarding the integrity of Microsoft services since 2008.[5] One of DCU's responsibilities is to investigate cybersecurity threats and identify and attribute attacks, like it has done here with the Tycoon 2FA Defendants. Richardson Decl. ¶ 3. DCU also collaborates with Microsoft Threat Intelligence ("MTI"), which is made up of thousands of world-class experts, security researchers, analysts, and threat hunters. *Id.* As part of Microsoft's investigation, DCU was involved in a test buy, where DCU purchased a one-month subscription to the Tycoon 2FA phishing kits from Tycoon 2FA Defendants. Richardson Decl. ¶ 33. For the one-month subscription, Microsoft paid the subscription fee of $350 USD. *Id.* To conduct the test buy, the referral source that DCU relied on communicated with Defendants via the Defendant Fridi's Telegram account. *Id.* After expressing interest in purchasing a monthly subscription, Defendants provided cryptocurrency payment information, which Microsoft used to deliver payment.

From the test buy, Microsoft gained information regarding the structure and operational details of Tycoon 2FA Defendants. Richardson Decl. ¶ 35. Once Microsoft purchased the kits, Microsoft performed a test phishing attack to phish a Microsoft account that was specifically created for this investigation. Richardson Decl. ¶ 36. This provided Microsoft with information regarding functionality. Finally, Microsoft was able to use the cryptocurrency wallet information to trace the financial transactions associated with the sale of the Tycoon 2FA kits. Richardson Decl. ¶¶ 44-46. To date, Microsoft has been able to connect accounts associated with Defendant Fridi to approximately $200,000 in sales from May 2025 to present, which represents at least 500-600 subscriptions. Richardson Decl. ¶ 46 Because each subscription allows the purchaser to engage in endless phishing attacks, even 500-600 subscriptions represent widespread attacks.

4. Attribution to the Tycoon 2FA Defendants

---

[5] *Microsoft Digital Crimes Unit*, Microsoft available at https://www.microsoft.com/en-us/corporate-responsibility/customer-security-trust/digital-crimes-unit (last accessed Feb. 17, 2026).

Microsoft investigated the online infrastructure used in the Tycoon 2FA Defendants' phishing campaign. Microsoft determined that Defendants have registered Internet domains using fictitious names and fictitious physical addresses that are purportedly located in multiple cities and countries. Richardson Decl. ¶ 40. The Tycoon 2FA Defendants have registered domains using functioning email addresses by which they communicated with legitimate domain registrars to complete the registration process. *Id*.

Cybercriminals like the Tycoon 2FA Defendants are known to obfuscate their identities to evade capture by law enforcement and continue their cybercrime. Richardson Decl. ¶ 41.

Microsoft investigated Tycoon 2FA Defendants' digital "signatures" (which can be thought of as digital fingerprints) for the infrastructure used by the Defendants. Richardson Decl. ¶¶ 42-43; *See also* Larson Decl. ¶¶ 14-20. By identifying these signatures, Microsoft determined that the domains identified in **Appendix A** belong to and are used by the Tycoon 2FA Defendants. Richardson Decl. ¶¶ 42-43; Larson Decl. ¶¶ 14-20. Specifically, Microsoft used the following indicators to assess these signatures: domain registration patterns, phishing URL patterns and components based on known Tycoon 2FA domains, the time period during which the domain was registered, analysis of WHOIS data, indicators from the Microsoft email detonation/protection system, domain resolution patterns, and Open-Source threat detection rules. Richardson Decl ¶¶ 42-43; Larson Decl. ¶¶ 14, 15.

These features, when taken together, provide a high level of confidence that a given domain is a Tycoon 2FA domain. Richardson Decl. ¶ 43. Each such domain is manually reviewed in detail by one or more subject matter experts as necessary to ascertain whether it is, in fact, a Tycoon 2FA domain. *Id*. Based on this analysis, Microsoft identified characteristics of the registration and maintenance of certain domains which, when coupled with the nature of the observed domain

activities, are a reliable method to connect such domains to actions undertaken by the Tycoon 2FA Defendants. *Id*. Other researchers in the security community have independently identified Tycoon 2FA domains and associated IP addresses, and these reports may be used to further validate Microsoft's analysis. Larson Decl. ¶¶ 14-20. These high confidence domains are identified in **Appendix A.**

III. LEGAL STANDARD

The purpose of a preliminary injunction is to protect the status quo and to prevent irreparable harm during the pendency of a lawsuit and to preserve the court's ability to render a meaningful judgment on the merits. *Univ. of Texas v. Camenisch*, 451 U.S. 390, 395 (1981). To be eligible for the requested injunctive relief, Plaintiffs 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. *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 24 (2008)); *UBS Fin. Servs., Inc. v. W Va. Univ. Hosps., Inc.*, 660 F.3d 643,648 (2d Cir. 2011). The standard is a flexible one and, in the Second Circuit, preliminary equitable relief is warranted when the movant demonstrates that serious questions going to the merits are raised and the balance of hardships is sharply in the movant's favor, assuming of course, that the other two *Winter* factors are met. *UBS Fin. Servs.*, 660 F.3d at 648.

IV. PLAINTIFFS' REQUESTED RELIEF IS WARRANTED

A. Plaintiffs Are Likely to Succeed on the Merits

Plaintiffs are likely to succeed on the merits of their claims and as such, their request for a TRO and a preliminary injunction should be granted. Plaintiffs allege violations of the following statutory and common law claims: Computer Fraud and Abuse Act (18 U.S.C. § 1030); Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. §§ 1962, 1962(d)); Electronic

Communications Privacy Act (18 U.S.C. § 2701); False Designation of Origin, Trademark Infringement, and Trademark Dilution under the Lanham Act, 15 U.S.C. §§ 1114 *et seq*.); and the common law claims of trespass to chattels, conversion, and unjust enrichment. Even at this early stage in the proceedings, the record demonstrates that Plaintiffs will be able to establish the elements of each of their claims. The evidence in support of the TRO Application is based on the diligent work of experienced investigators and is supported by substantial empirical evidence and forensic documentation. In short, there is no legitimate dispute about what Tycoon 2FA Defendants do and the damage they cause. Given the strength of Plaintiffs' evidence, the likelihood of success on the merits weighs heavily in favor of granting injunctive relief. In a similar case involving a similar threat actor, Judge Rakoff granted similar injunctive relief, finding good cause that the defendants engaged in violations of the same federal statutes at issue here and that this illegal conduct caused irreparable harm to Microsoft. *See See, e.g.*, *Microsoft and Health-ISAC v. Joshua Ogundipe and John Does 1-4*, 1:25-cv-07111 (S.D.N.Y. Aug. 27, 2025) (Rakoff, J.) Order at 2-4; Poston Decl. ¶ 49, Ex. 23.

1. **Tycoon 2FA Defendants' Violation of the Computer Fraud and Abuse Act**

Congress enacted the Computer Fraud and Abuse Act (the "CFAA") specifically to address computer crime. *See, e.g.*, *Univ. Sports Pub. Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 384 (S.D.N.Y. 2010) (concluding that the CFAA's language and legislative history show that Congress intended it to proscribe hacking); *In re Doubleclick Privacy Litig.*, 154 F. Supp. 2d 497, 525 (S.D.N.Y. 2001) (noting that activity that "Congress sought to punish and remedy in the CFAA -- namely, damage to computer systems and electronic information by hackers"). *Inter alia*, the CFAA penalizes a party that: (1) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage, 18 U.S.C. § 1030(a)(5)(C); or (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 to a protected computer, 18 U.S.C. § 1030(a)(5)(A).

A "protected computer" is a computer "used in or affecting interstate or foreign commerce or communication." *See United States v. Gasperini*, 2017 WL 2399693, at *3 (E.D.N.Y. June 1, 2017). This definition encompasses any computer with an internet connection. *See United States v. Yücel*, 97 F. Supp. 3d 413 (S.D.N.Y. 2015) (collecting cases and noting "widespread agreement in the case law" that "protected computer" includes any internet-connected computer). Each of the victims' computers that Tycoon 2FA Defendants attempted to infiltrate through the phishing scheme meets the definition of a protected computer.

"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 so to obtain or alter.'" *JBCHoldings NY, LLC v. Pakter*, 931 F. Supp. 2d 514, 523 (S.D.N.Y. 2013) (citing 18 U.S.C. § 1030(e)(6)). The entire purpose of Tycoon 2FA Defendants' phishing operation is to steal credentials to infiltrate the systems of their victims. Richardson Decl. ¶¶ 15 n.5, 26. Tycoon 2FA Defendants' end goal is to deceive the victim into providing credentials and multi-factor authentication information so that it can surreptitiously and without authorization take control. Indeed, by its very nature, the AiTM model employed by Tycoon 2FA Defendants exceeds authorized access. Richardson Decl. ¶ 15 n. 5.

To prosecute a civil claim under the CFAA, a plaintiff must demonstrate loss or damage in excess of $5,000. The CFAA defines loss as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program,

system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *JBCHoldings NY, LLC*, 931 F. Supp. 2d at 523-24 (citing 18 U.S.C. § 1030(e)(11)). "[D]amage, in turn, is defined as 'any impairment to the integrity or availability of data, a program, a system, or information.'" *Sewell v. Bernardin*, 795 F.3d 337, 340 (2d Cir. 2015) (citing 18 U.S.C. § 1030(e)(8)); *Nexans Wires S.A. v. Sark-USA, Inc.*, 166 F. App'x 559, 563 (2d Cir. 2006) (damage includes "investigating and remedying damage to a computer, or a cost incurred because the computer's service was interrupted"); *Univ. Sports Publ'ns Co.*, 725 F. Supp. 2d at 387 (loss includes "the costs of investigating security breaches constitute recoverable 'losses,' even if it turns out that no actual data damage or interruption of service resulted from the breach). The CFAA permits Plaintiffs to aggregate multiple intrusions or violations to meet the $5,000 statutory threshold. *See Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 473 (S.D.N.Y. 2004), aff'd, 166 F. App'x 559 (2d Cir. 2006). As a direct result of Tycoon 2FA Defendants' conduct, Microsoft has been forced to spend at least $925,000, investigating and remediating Tycoon 2FA Defendants' activities. Richardson Decl. ¶ 55. Similarly, as a direct result of Tycoon 2FA Defendants' conduct, Health-ISAC and its member organizations have been forced to spend at least $350,400 to investigate Tycoon 2FA Defendants' activities and mitigate the impact on its member organizations. Weiss Decl. ¶ 16.

Tycoon 2FA Defendants' conduct is precisely the type of activity that the Computer Fraud and Abuse Act is designed to prevent. *See e.g.*, *Penrose Computer Marketgroup, Inc. v. Camin*, 682 F. Supp. 2d 202 (N.D.N.Y. 2010); *Global Policy Partners, LLC v. Yessin*, 2009 U.S. Dist. LEXIS 112472, *9-13 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant was actionable under the CFAA); *Facebook, Inc. v. Fisher*, 2009 U.S. Dist. LEXIS

122578 (N.D. Cal. 2009) (granting a TRO under CFAA where defendants allegedly engaged in a phishing and spamming scheme that compromised the accounts of Facebook users); *Physicians Interactive v. Lathian Sys., Inc.*, 2003 U.S. Dist. LEXIS 22868, *25 (E.D. Va. 2003) (granting TRO and preliminary injunction under CFAA where the defendant hacked into a computer and stole confidential information); *see also United States v. Phillips,* 477 F.3d 215, 219 (5th Cir. 2007) (noting that CFAA is concerned with "outside hackers who break into a computer") (citations to legislative history omitted). Thus, Microsoft and Health-ISAC are likely to succeed on the merits of their CFAA claim.

2. Tycoon 2FA Defendants Violate the Racketeer Influenced and Corrupt Organizations Act

The Racketeer Influenced and Corrupt Organizations Act ("RICO") prohibits "any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity." 18 U.S.C. § 1962(c). RICO also makes it unlawful "for any person to conspire to violate" that provision, regardless of whether that conspiracy ultimately comes to fruition. 18 U.S.C. §1962(d). "Any person injured in his business or property by reason of a violation of' either of these provisions is entitled to recovery, 18 U.S.C. § 1964(c), and this Court has "jurisdiction to prevent and restrain" such violations "by issuing appropriate orders." 18 U.S.C. 1964(a). *See also United States v. Carson,* 52 F.3d 1173, 1181-82 (2d Cir. 1995) ("the jurisdictional powers in § 1964(a) serve the goal of foreclosing future violations," and "the equitable relief under RICO is intended to be broad enough to do all that is necessary"); *United States v. Sasso,* 215 F.3d 283, 290 (2d Cir. 2000) (same); *Trane Co. v. O'Connor Sec.,* 718 F.2d 26, 29 (2d Cir. 1983) (preliminary injunction proper under RICO where plaintiff establishes "a likelihood of irreparable harm").

Defendants in this case have formed and associated with such an enterprise affecting foreign and interstate commerce and have engaged in an unlawful pattern of racketeering activity involving thousands of predicate acts of fraud and related activity in connection with violations of (i) the Computer Fraud and Abuse Act (18 U.S.C. § 1030(a)(5)(A)), incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(G) and 18 U.S.C. § 2332b(g)(5)(B), and (ii) wire fraud (18 U.S.C. § 1343), incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(B).

The Racketeering Enterprise

An associated in fact enterprise consists of "a group of persons associated together for a common purpose of engaging in a course of conduct" and "is proved by evidence of an ongoing organization, formal or informal, and by evidence that the various associates function as a continuing unit." *Boyle v. United States,* 556 U.S. 938, 945 (2009). An enterprise requires "at least three structural features: a purpose, relationships among those associated with the enterprise, and longevity sufficient to permit these associates to pursue the enterprise's purpose." *Id.*

The Racketeering Enterprise has existed at least since Fall 2023 when Defendants Saad Fridi and John Does 1-2 conspired to, and did, form an associated in fact Racketeering Enterprise with a common purpose of developing, selling, and implementing phishing kits, as well as operating a phishing infrastructure resulting in business email compromise, financial fraud, and ransomware. Richardson Decl. ¶¶ 26-28. Specifically, John Does 1-2 work in tandem with Defendant Fridi to provide technical, administrative, and financial support, including for example, managing the administrative panel and customer dashboard that is made available to customers and managing the cryptocurrency wallets associated with Fridi. Richardson Decl. ¶¶ 22-23. John Does 3-4 joined the conspiracy and began participating in the Racketeering Enterprise at various times thereafter, specifically when they purchased the kit and began using the kits to conduct

phishing attacks. *Id.* ¶ 24; *see also United States v. Eppolito,* 543 F.3d 25, 49 (2d Cir. 2008) (an

enterprise "may continue to exist even though it undergoes changes in membership"). John Does

3-4 are the customers of the Tycoon 2FA, who purchase phishing kits. phish. When they purchase

the kit, use the infrastructure provided by Fridi, and carry out phishing attacks, these customers

join the Racketeering Enterprise. Richardson Decl. ¶ 25. Although Microsoft has not been able to

identify the exact number of customers and purchasers, the cryptocurrency payments demonstrate

that Racketeering Enterprise contains hundreds of cybercriminals who all purchase and use the

Tycoon 2FA kit to commit phishing attacks and other cybercrimes. *Id.*

The Racketeering Enterprise has continuously and effectively carried out its purpose of

operating their PhaaS business model with use of the Tycoon 2FA-branded phishing kits at the

core of the operation and will continue to do so absent the relief Plaintiffs request.

Both the purpose of the Racketeering Enterprise and the relationship between Tycoon 2FA

Defendants is proven by: (1) the dissemination of Tycoon 2FA-branded phishing kits; (2) the

subsequent development and operation of the phishing operations' Internet infrastructure to

proliferate phishing attacks and leveraging of the infrastructure for PhaaS; and (3) Tycoon 2FA

Defendants' respective and interrelated roles in the sale, operation of, and profiting from the

Tycoon 2FA-branded phishing kits in furtherance of Tycoon 2FA Defendants' common financial

interests. *Boyle,* 556 U.S. at 945 (relationship and common interest may be inferred from "evidence

used to prove the pattern of racketeering activity"); *Eppolito,* 543 U.S. at 50 ("evidence of prior

uncharged crimes . . . may be relevant . . . to prove the existence, organization and nature of the

RICO enterprise, and a pattern of racketeering activity by each defendant.").

Defendants' Pattern of Racketeering Activity

A pattern of racketeering activity "requires at least two acts of racketeering activity, one of

which occurred after [October 15, 1970,] and the last of which occurred within ten years . . . after the commission of a prior act of racketeering activity." *H.J Inc. v. Northwestern Bell Tel. Co.,* 492 U.S. 229, 237 (1989). A threat of continuing activity "is generally presumed when the enterprise's business is primarily or inherently unlawful." *Spool v. World Child Int'l Adoption Agency,* 520 F.3d 178, 185 (2d Cir. 2008). Tycoon 2FA Defendants have conspired to conduct and have conducted and participated in the operations of the Racketeering Enterprise through a continuous pattern of racketeering activity. Each predicate act is related to and in furtherance of the common unlawful purpose shared by the members of the Racketeering Enterprise. These acts are ongoing and will continue unless and until this Court grants Plaintiffs' request for a temporary restraining order.

Tycoon 2FA Defendants' racketeering acts include persistent violations of the Computer Fraud and Abuse Act, *see supra* Section IV.A.1 (establishing that Plaintiffs establish violations of CFAA). Violation of the CFAA is incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(G) and 18 U.S.C. § 2332b(g)(5)(B).

Tycoon 2FA Defendants' conduct is also "racketeering activity" in the form of wire fraud under 18 U.S.C. § 1343. Wire fraud requires "(1) the existence of a scheme to defraud, (2) the defendant's knowing participation in the scheme, and (3) the use of wire, mail, or television communications in interstate commerce in furtherance of the scheme." *Chanayil v. Gulati*, 169 F.3d 168, 170–71 (2d Cir. 1999).

Existence of a scheme to defraud. The entire purpose of a phishing operation is to deceive and defraud the victims into providing their credentials to the Tycoon 2FA Defendants. Richardson Decl. ¶¶ 7, 26. The phishing kits provide template documents that incorporate logos of Microsoft or other reputable companies to facilitate the deception. While a victim may be

suspicious of a phishing email from an unknown email address from an unknown company, the victim is more likely to open the email if he or she is tricked into thinking it is from a trusted source. Richardson Decl. ¶¶ 52-53.

Knowing participation in scheme. Defendants' knowledge is evident from how the phishing kit is advertised and how it is used. The kit allows its purchasers to create templates leveraging Microsoft branding, products, and services allowing them to more effectively target Microsoft customers. Richardson Decl. ¶¶ 50-53. Given that the email templates and attachments are fraudulently created (*e.g.*, a fake attachment purporting to be a document requiring urgent attention), the Tycoon 2FA Defendants' decision to deceive is knowing and intentional. *Id.* ¶ 53.

Use of wire communication in interstate commerce to further the scheme. Tycoon 2FA Defendants are located globally and send phishing emails (*e.g.*, wire communications) to victims located across the United States, including, but not limited to, New York, Texas, and California. Richardson Decl. ¶ 48, Figure 15. The purchasers of the phishing kits are likewise located across the United States and the world (including at least in Pakistan)). Richardson Decl. ¶ 19; *Lateral Recovery LLC v. Queen Funding, LLC*, 2022 WL 2829913, at *3 (S.D.N.Y. July 20, 2022) (use of wire for purposes of wire fraud include email communications).

These transmissions resulted not only in defrauding victims to provide their credentials, but it also allowed Tycoon 2FA Defendants to receive monetary benefits through the sale of the Tycoon 2FA-branded phishing kits.

Defendants' Racketeering Activity Harmed Plaintiffs

As a direct result of Tycoon 2FA Defendants' conduct, Microsoft and Health-ISAC have been harmed. There has been damage to their brands and reputations, customers and member organizations have been deceived and defrauded, and both Microsoft and Health-ISAC have

incurred significant damages and costs to investigate and remediate the harm caused by Tycoon 2FA. Accordingly, "there [is] a direct relationship between [the] injury and the defendant's injurious conduct" and "the RICO violation was the but-for (or transactional) cause of [the] injury." *UFCW Local 1776 v. Eli Lilly & Co.*, 620 F.3d 121, 132 (2d Cir. 2010) (citing *Holmes v. Sec. Investor Prat. Corp.*, 503 U.S. 258, 268 (1992)). Where the pattern of racketeering activity consists of fraud, as here, a plaintiff need not show that it relied on or was deceived by the defendant's fraud -- third party reliance is sufficient. *Id.* (quoting *Bridge v. Phoenix Bond & Indem. Co.*, 533 U.S. 639, 657-58 (2008)). Accordingly, Plaintiffs are likely to succeed on the merits of their RICO claim.

3. Tycoon 2FA Defendants' Violation of the Electronic Communications Privacy Act

The Electronic Communications Privacy Act prohibits "intentionally access[ing] without authorization a facility through which electronic communications are provided" or doing so in excess of authorization, and, in so doing, obtaining, altering, or preventing authorized access to an electronic communication while it is in electronic storage. 18 U.S.C. § 2701(a); *Organization JD LTDA v. United States DOJ*, 124 F.3d 354, 359 (2d Cir. 1997) ("The ECPA was enacted to 'protect against the unauthorized interception of electronic communications.'"); *In re Doubleclick Privacy Litig.*, 154 F. Supp. 2d at 507 ("18 U.S.C. § 2701 *et. seq.* … aims to prevent hackers from obtaining, altering, or destroying certain stored electronic communications.").

ECPA is violated when Defendants log into Plaintiffs' customers' account without permission (including with stolen credentials) and intentionally access the contents of an inbox. *See Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp*, LLC, 759 F. Supp. 2d 417 (S.D.N.Y. 2010) (holding that an employer's unauthorized access of an employee's personal emails stored on a third-party communication service provider's system violated the ECPA); *see*

also McPherson v. Harker, 2021 WL 1820290, at *11 (D.D.C. May 6, 2021) (husband violated ECPA "when he 'intentionally access[ed]' Facebook's servers, by logging into his wife's account without her permission, in order to 'obtain[ ] . . . a[n] electronic communication,' namely the Facebook messages between Mrs. Thomas and plaintiff, in 'electronic storage' on those servers) (alteration in original). Here, the object of Tycoon 2FA Defendant's scheme is to obtain the credentials and then surreptitiously infiltrate the victims' systems. Richardson Decl. ¶¶ 26-28. From there, the cybercriminals move within the system, including accessing email inboxes for the purpose of identifying additional targets for subsequent phishing and engaging in business email compromise to exfiltrate sensitive emails and information. Richardson Decl. ¶ 28. The Tycoon 2FA Defendants do not have permission or authority to access the contents of the victims' inboxes; they use stolen credentials and violate ECPA.

Through this unauthorized access, Tycoon 2FA Defendants intercepted, had access to, obtained, and altered, and/or prevented legitimate, authorized access to, wire and electronic communications transmitted through the computers and infrastructure of Microsoft and its users. Richardson Decl. ¶¶ 36, 37. Obtaining stored electronic information in this way, without authorization, is a per se violation of ECPA. Thus, Microsoft is likely to succeed on the merits of its ECPA claims.

4. Tycoon 2FA Defendants' Violation of the Lanham Act

Section 1114(1) of the Lanham Act prohibits use of a reproduction, counterfeit, copy or "colorable imitation" of a registered mark in connection with the distribution of goods and services where such use is likely to cause confusion or mistake or to deceive. 15 U.S.C.§ 1114(1)(a). The Lanham Act also 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.

15 U.S.C. § 1125(a).

Tycoon 2FA Defendants use Plaintiffs' registered and distinctive trademarks in fraudulent schemes designed to mislead victims into clicking on links to interact with malicious websites and fraudulent versions of Defendants' websites. Richardson Decl. ¶¶ 50-54. This conduct deceives victims, engenders confusion, and causes them to mistakenly associate Plaintiffs with this activity. Richardson Decl. ¶ 54.

For example, when victims click on a link in a malicious phishing email, the victim is routed to a login page that appears to be a Microsoft login page. Richardson Decl. ¶26, n. 7. In the screenshot below, which is a screenshot that Microsoft captured in connection with its investigation and was able to attribute to Tycoon 2FA, the 2FA page has an image of Microsoft's trademarked logo on the page. Richardson Decl. ¶ 36. Anyone seeing this page would naturally believe that they were interacting with a legitimate login page. Beyond the logo, the look and feel of the page is identical to a legitimate Microsoft login page. *Id.*. This is done intentionally: to deceive customers, to create confusion, and to trick customers into believing that it is authentic. *Id.*. This is textbook trademark infringement.
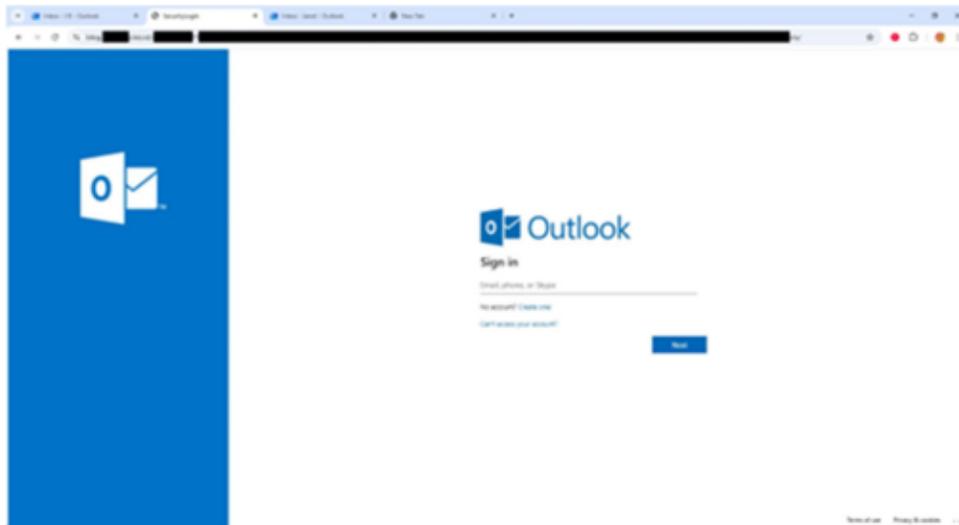
Figure 1

This is a clear violation of the Lanham Act. *Audi AG v. Shokan Coachworks, Inc.*, 592 F. Supp. 2d 246, 279 (N.D.N.Y. 2008) (holding that the use of the plaintiffs' marks in the defendants' email addresses created a likelihood of consumer confusion); *Kuklachev v. Gelfinan*, 629 F. Supp. 2d 236,258 (E.D.N.Y. 2008) (entering preliminary injunction under Lanham Act § 1114 for infringement of trademarks where confusion was likely to result from use of plaintiffs' name and images in connection with defendants' advertisements); *Broolqield Commc'ns. v. W. Coast Entm't Corp.*, 174 F.3d 1036, 1066-1067 (9th Cir. 1999) (entering preliminary injunction under Lanham Act § 1114 for infringement of trademark in software and website code).

In addition to constituting infringement under section 1114 of the Lanham Act, Tycoon 2FA Defendants' conduct also constitutes false designation of origin under section 1125(a), which prohibits use of a registered mark that "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." 15 U.S.C. § 1125(a)(1)(A); *see also CJ Prods. LLC v. Snuggly Plushez LLC*, 809 F. Supp. 2d 127, 147-48 (E.D.N.Y. 2011) (entering a preliminary injunction under the Lanham

Act § 1125(a) for infringement of trademark on a website); *Brookfield Commc'ns.*, 174 F. 3d at 1066-67 (entering preliminary injunction under Lanham Act § 1125(a) for infringement of trademark in software and website code); *Hotmail Corp. v. Van$ Money Pie, Inc.*, 47 U.S.P.Q.2d (BNA) 1020,1024, 1025- 26 (N.D. Cal. 1998) (granting preliminary injunction; copying the Hotmail trademarks in "e-mail return addresses" constituted false designation of origin).

The Lanham Act further provides that the owner of a famous, distinctive mark "shall be entitled to an injunction against another person" who uses the mark in a way "that is likely to cause dilution by blurring or dilution by tarnishment of the famous mark. . . ." 15 U.S.C. § 1125(c). Here, Tycoon 2FA Defendants' misuse of Plaintiffs' famous marks in connection with malicious conduct aimed at Plaintiffs' customers and the public dilutes the famous marks by tarnishment and by blurring consumers' associations with the marks.

Specifically, Tycoon 2FA Defendants' misleading and false use of Microsoft's trademarks—including Microsoft®, Windows®, Microsoft 365®, Office365®, Office®, Microsoft Office®, SharePoint®, OneDrive®, Outlook®, and Azure®—causes confusion and mistakes as to their affiliation with Tycoon 2FA Defendants' malicious conduct. *See supra*. This activity is a clear violation of Lanham Act § 1125(a), and Plaintiffs are likely to succeed on the merits. *See e.g.*, *Hamzik v. Zale Corp.*, 2007 U.S. Dist. LEXIS 28981 (N.D.N.Y. April 18, 2007); *Hotmail Corp.,* 47 U.S.P.Q.2d at 1024, 1025-26; (spam e-mail with purported "from" addresses including plaintiff's trademarks constituted dilution).

5. Tycoon 2FA's Conduct is Tortious Under New York Law

Tycoon 2FA Defendants' conduct is tortious under the common law doctrines of trespass to chattels, conversion, and unjust enrichment. Under New York law, ""[c]onversion is the unauthorized assumption and exercise of the right of ownership over goods belonging to another

to the exclusion of the owner's rights." *Pac. M. Int'l Corp. v. Raman Int'l Gems, Ltd.*, 888 F. Supp. 2d 385, 396 (S.D.N.Y. 2012). Conversion applies to electronic computer records and data. *Thyroff. Nationwide Mut. Ins. Co.*, 8 N.Y.3d 283,288-89 (2007); *see also Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 697 (D. Md. 2011) (holding defendant liable for conversion where defendant replaced current version of plaintiffs' website with former version, because such action effectively "dispossessed [plaintiff] of the chattel;" *i.e.*, its website).

The related tort of trespass to chattels applies where personal property of another is used without authorization, but the conversion is not complete. *Sch. of Visual Arts v Kuprewicz*, 3 Misc. 3d 278, 281 (2003); *Yo! Braces Orthodontics, PLLC v. Theordorou*, 2011 N.Y. Misc. LEXIS 1820, *8 (Apr. 19, 2011). New York law recognizes the tort of trespass to chattels in connection with computer intrusion. *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 404 (2d Cir. 2004) (affirming grant of injunction against defendants accessing plaintiff's computers using automated software); *Democratic Nat'l Comm. v. Russian Fed'n*, 392 F. Supp. 3d 410, 449 (S.D.N.Y. 2019) ("Hacking a computer network may qualify as trespass to chattels.")

Here, Tycoon 2FA Defendants exercised dominion and authority over Microsoft's proprietary services like Outlook by intruding into its servers supporting those services to gain access to content stored on those servers like email and access to other applications on the Outlook platform. Richardson Decl. ¶ 25. These acts deprived Microsoft and its customers of their right to control the content, functionality, and nature of its software and services, and such computer hacking amounts to tortious conduct under the doctrines of conversion and trespass to chattels.

Plaintiffs are likely to succeed on the merits of their unjust enrichment claim. The elements of a claim of unjust enrichment are that a (1) defendant benefitted, (2) at plaintiff's expense, and (3) equity and good conscience require restitution. *Beth Israel Med. Ctr. v. Horizon Blue.Cross*

and Blue Shield, 448 F.3d 573,586 (2d Cir. 2008). Tycoon 2FA Defendants' misuse of Microsoft's and Health-ISAC member organizations' brand and reputations constitutes unjust enrichment. Defendants have been unjustly enriched through their unlawful use of Plaintiffs' trademarks, brand names, goodwill, goods, and services to carry out their PhaaS enterprise. Plaintiffs have spent considerable resources to develop their brands, such that the customers and public trust their branding and reputation. Richardson Decl. ¶ 53; Weiss Decl. ¶¶ 25, 26. In order to ensure greater efficacy of their criminal operation, Tycoon 2FA Defendants usurp this goodwill. Richardson Decl. ¶¶ 2, 50. Weiss Decl. ¶ 26. By leveraging and misusing the branding and reputations, Tycoon 2FA Defendants benefit because it is more likely that their phishing attacks are successful. The benefit to Tycoon 2FA Defendants (greater success at committing cybercrime) is at the expense of Microsoft and Health-ISAC, who suffer brand tarnishment and harm to customers and member organizations as a result. *Id.* Moreover, Tycoon 2FA Defendants' acceptance or retention of this benefit "'render it inequitable for the defendant to retain the benefit without paying for its value.'" *Microsoft Corp. v. John Does 1-8*, 2015 WL 49037441, at *12. Ordinarily, Microsoft places restrictions on how its branding can be used; and certainly, it does not authorize any use of its branding or marks for the purpose of conduct criminal activity. Richardson Decl. ¶ 54. Finally, once Tycoon 2FA Defendants complete a phishing attack and gain access to a victim's account, Tycoon 2FA Defendants are further unjustly enriched through the access they have obtained through ill-gotten means. It is inequitable for Tycoon 2FA Defendants to retain these benefits.

Thus, Plaintiffs are likely to succeed on the merits of their common law claims.

B. Tycoon 2FA Defendants Cause Irreparable Harm

It is well-settled that consumer confusion and injury to business goodwill constitute irreparable harm. *See Tom Doherty Assocs., Inc. v. Saban Entm't, Inc.*, 60 F.3d 27, 37-38 (2d Cir.

1995) (recognizing that the loss of prospective business or goodwill supports a finding of irreparable harm); *Broker Genius, Inc. v. Volpone*, 313 F. Supp. 3d 484, 496 (S.D.N.Y. 2018) (same).

Here, Defendants tarnish Plaintiffs' valuable trademarks, injuring Microsoft's goodwill, creating confusion about the source of Defendants' malware, and damaging the reputation of and confidence in the services of Microsoft's products including Office 365.

First, Tycoon 2FA-branded phishing kits are customized to circumvent the security features of Microsoft products, use Microsoft logos, and mimic the appearance of authentic communications to deceive victims into thinking that the email communication they receive, the files they are directed to open, or links to websites used to enter their personal credentials are authentic and Microsoft-approved. Richardson Decl. ¶ 52. Thus, each time a phishing kit is sold, it is done with the express purpose of hacking into Microsoft's products and systems that Microsoft has expended significant resources to build and protect.

Second, Tycoon 2FA Defendants leverage Microsoft systems and programs, such as Outlook, Microsoft 365, and Office 365 to further enhance the perceived legitimacy of the attack. Richardson Decl. ¶¶ 7, 26. Similarly, because the login pages that Tycoon 2FA Defendants use include the Microsoft name and logo, the victim will be completely unaware of the threat and believe that the link is to a legitimate Microsoft webpage and trustworthy, when in fact, it is malicious. *Id*. In doing so, Tycoon 2FA Defendants capitalize on and misuse the brand recognition that Microsoft has cultivated, and the trust Microsoft has built with its customers and that customers have come to expect. Richardson Decl. ¶¶ 51-55.

Customers expect certain quality from Microsoft. When "Microsoft" systems and products are used in connection with cybercrime, customers will mistakenly believe that Microsoft is

responsible for the attack. Richardson Decl. ¶ 54. Customers subjected to the negative effects of Defendants' phishing attacks sometimes incorrectly believe that Microsoft is the source of the problem, and thus there is a significant risk that Microsoft customers will be confused in this way in the future. *Id*. There is a great risk that because Tycoon 2FA Defendants misuse Microsoft's branding and trademarks and rely on this misuse to deceive, Microsoft customers may incorrectly attribute these problems to Microsoft and associate these problems with Microsoft's products and services, thereby diluting and tarnishing the value of these trademarks and brands. *Id*. If a customer leaves Microsoft due to improperly blaming Microsoft for a phishing attack or believes that Microsoft's systems and products are not secure (because customers are unaware of Tycoon 2FA Defendants' deception), it may be costly or impossible to convince the customer to return to Microsoft. *Id.*.

Phishing attacks continue to be a major cybersecurity concern for Health-ISAC members and the broader health sector, with significant financial and operational consequences. Weiss Decl. ¶ 7. Phishing is the top infection vector for cyberattacks in the healthcare industry. For example, phishing simulations conducted in healthcare organizations result in a click rate of 10-30% for employees who are deceived by the phishing email. *Id.* The average downtime for a healthcare company successfully attacked by a cybercriminal is 19 days—during which time patient care can be severely impacted through canceled surgeries, diverted ambulances, and compromised medical records. *Id.*

As described above, Health-ISAC member organizations have already been targeted by phishing emails attributable to Tycoon 2FA. Weiss Decl. ¶ 10-15. Tycoon 2FA kits offers the ability to customize the phishing kits to target specific victims. Staff members at these organizations have already opened these emails, clicked on the links or attachments, and in some

cases, even provided their credentials to Tycoon 2FA. Weiss Decl. ¶¶ 14, 15. This is the precursor to other cybercrimes, including ransomware and malware attacks. Weiss Decl. ¶ 23. Once a cybercriminal has successfully infiltrated a Health-ISAC member organization, it is only a matter of time before subsequent cybercrime attacks are launched. *Id*. When there is a malware or ransomware attack on a healthcare organization, the consequences are devastating and can endanger people's lives. This includes ambulances being forced to divert, delayed, disruption, or cancellation of providing care, the inability to access patient records when electronic health record systems are taken offline, data breaches of patient information, and financial losses. Weiss Decl. ¶¶ 21, 25-26.

Tycoon 2FA-branded phishing kits harm the brand reputation of Health-ISAC's member organizations. For example, when member organizations are attacked, their brand and reputation are irreparably harmed when patients are no longer able to rely on the security of patient data and the healthcare network system as a whole is put at risk. Weiss Decl. ¶ 25. Because Health-ISAC organizations are under attack, they are forced to expend tremendous resources to defend themselves. *Id*.

These injuries are sufficient in and of themselves to constitute irreparable harm. In addition, Tycoon 2FA Defendants are causing monetary harm for which they will not be compensated—even after final judgment—because Tycoon 2FA Defendants are elusive cybercriminals against whom Plaintiffs are unlikely to enforce a judgment. "[W]e have held that a finding of irreparable harm may lie in connection with an action for money damages where the claim involves an obligation owed by an insolvent or a party on the brink of insolvency." *CRP/Extell Parcel I, L.P. v. Cuomo*, 394 F. App'x 779, 781 (2d Cir. 2010) (*citing Brenntag Int'l Chems. Inc. v. Bank of India*, 175 F.3d 245, 249-50 (2d Cir. 1999)); *accord* paying any rents,

particularly in light of the threat of insolvency by one or more Defendants.").

C. Balance of Equities Strongly Favors Injunctive Relief

Defendants will suffer no harm to any legitimate interest if a TRO and preliminary injunction are issued, because Defendants have no legitimate interest in committing cybercrime and violating U.S. laws. Moreover, because Defendants are engaged in an illegal scheme to defraud consumers and injure Plaintiffs, the balance of equities is in favor of granting an injunction. *See, e.g.*, *N. Atl. Operating Co., Inc. v. Evergreen Distributors*, LLC, 2013 WL 5603602, at *13 (E.D.N.Y. Sept. 27, 2013) ("Where '[t]he only hardship to Defendant from [an] injunction would be to prevent him from engaging in further illegal activity, [] the balance clearly weighs in Plaintiffs' favor.'" (*quoting DISH Network L.L.C. v. DelVechhio*, 831 F. Supp. 2d 595, 601-02 (W.D.N.Y. 2011)). On one side of the scales of equity rests the harm to Microsoft, its customers, Health-ISAC, its member organizations, and the public, caused by Tycoon 2FA Defendants, while on the other side, Tycoon 2FA Defendants can claim no legally cognizable harm because an injunction would only require Tycoon 2FA Defendants to cease illegal activities.

D. Public Interest Favors Injunctive Relief

It is clear that an injunction would serve the public interest here. Every day that passes, Tycoon 2FA Defendants intrude into more victim accounts, deceive more members of the public, and steal more information from the accounts and computers of their innocent victims. The public interest is clearly served by enforcing statutes designed to protect the public, such as the Lanham Act, CFAA, and ECPA. *See, e.g.*, *ProFitness Phys. Therapy Ctr. v. Pro-Fit Ortho. And Sports Phys. Therapy P.C.*, 314 F.3d 62, 68 (2d Cir. 2002) (finding a "strong public interesting in preventing public confusion"); *Juicy Couture, Inc. v. Bella Intern. Ltd.*, 930 F. Supp. 2d 489, 505 (S.D.N.Y. 2013) (finding that grant of a preliminary injunction in case under the Lanham Act

would not disserve the public interest, where there was a strong interest in preventing public confusion over parties' competing trademark); *FXDirectDealer, LLC v. Abadi*, 2012 WL 1155139, at *8 (S.D.N.Y. Apr. 5, 2012) (public interest weighed in favor of injunction to enforce CFAA); *DISH Network L.L.C. v. DelVechhio*, 831 F. Supp. 2d 595, 601-02 (W.D.N.Y. 2011) (public interested weighed in favor of injunction to enforce ECPA).

Notably, numerous courts have granted requests for injunctive relief to disable malicious computer botnets, such as those enabled by the Tycoon 2FA Defendants. *See*, *supra* fn. 2. Microsoft respectfully submits that the same result is warranted here.

V. THE ALL WRITS ACT AUTHORIZES THE COURT TO DIRECT THIRD PARTIES TO PERFORM THE NECESSARY ACTS TO AVOID FRUSTRATION OF THE REQUESTED RELIEF

Plaintiffs' Proposed Order directs that the third-party domain registrars and registries whose infrastructure Tycoon 2FA Defendants rely on to operate the phishing infrastructure reasonably cooperate to effectuate the TRO. Critically, these third parties are the primary entities within the United States that can effectively disable internet infrastructure, and thus their cooperation is necessary.

Plaintiffs request this relief under the All Writs Act. The All Writs Act provides that a court may issue all writs necessary or appropriate for the administration of justice. 28 U.S.C. § 1651(a). The Supreme Court has recognized that narrow direction to third parties necessary to effect the implementation of a court order is authorized by the All Writs Act:

> The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice, and encompasses even those who have not taken any affirmative action to hinder justice.

United States v. New York Tel. Co., 434 U.S. 159, 174 (1977) (citations omitted) (order to telephone company to assist in implementation of a pen register warrant was authorized under the

All Writs Act); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398 at *30 (invoking All Writs act and granting relief similar to that requested herein); There are two steps to any analysis of the AWA as applied to third parties. First, there are three threshold requirements: (1) issuance of the writ must be "in aid of" the issuing court's jurisdiction; (2) the type of writ requested must be "necessary or appropriate" to provide such aid to the issuing court's jurisdiction; and (3) the issuance of the writ must be "agreeable to the usages and principles of law." *In re Apple, Inc.*, 149 F. Supp. 3d 341, 351 (E.D.N.Y. 2016). If these threshold requirements are met, the court in its discretion may consider whether "(1) the third party must be closely connected with the underlying controversy…; (2) the order must not adversely affect the basic interests of the third party or impose an undue burden; (3) the assistance of the third party must be absolutely necessary*." United States v. Hall*, 583 F. Supp. 717, 719 (E.D. Va. 1984) (citing *New York Tel. Co.*, 434 U.S. at 174-77); *see also In re Apple, Inc.*, 149 F. Supp. 3d at 344 (reciting similar three factors); *In re Baldwin-United Corp.*, 770 F.2d 328, 338-39 (2d Cir. 1985) ("An important feature of the All-Writs Act is its grant of authority to enjoin and bind non-parties to an action when needed to preserve the court's ability to reach or enforce its decision in a case over which it has proper jurisdiction"; "[The Court does] not believe that Rule 65 was intended to impose such a limit on the court's authority provided by the All Writs Act to protect its ability to render a binding judgment."); *Moore v. Tangipahoa Parish Sch. Bd.*, 507 Fed. App'x. 389, 396 (5th Cir. 2013) (unpublished) ("The All Writs Act provides 'power [to] a federal court to issue such commands . . . as may be necessary or appropriate to effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained.'") (citing *New York Tel. Co*., 434 U.S. at 172); see also *In re Application of United States of Am. for an Order Authorizing An In-Progress Trace of Wire Commc'ns Over Tel. Facilities*, 616 F.2d 1122, 1129 (9th Cir. 1980) (noting of *New York Tel. Co*.,

434 U.S. at 175, "the Court made the commonsense observation that, without the participation of the telephone company, 'there is no conceivable way in which the surveillance authorized could have been successfully accomplished'"); *Dell, Inc. v. Belgium Domains, LLC*, 07-22674, 2007 WL 6862341, at *6 (S.D. Fla. Nov. 21, 2007) (All Writs Act applied in conjunction with trademark seizure under Rule 65 and Lanham Act).

Plaintiffs have plainly met the threshold factors. First, this action is commenced under various federal statutes – the Lanham Act, Racketeer Influenced and Corrupt Organizations Act, the Electronic Communications Protection Act, and the Computer Fraud and Abuse Act. Thus, this Court "unquestionably has subject matter jurisdiction over this action pursuant to 28 U.S.C. Section 1331, and, therefore, has jurisdiction to issue the requested [AWA] Order." *United Spinal Ass'n v. Bd. of Elections in City of New York*, 2017 WL 8683672, at *5 (S.D.N.Y. Oct. 11, 2017), report and recommendation adopted, 2018 WL 1582231 (S.D.N.Y. Mar. 27, 2018). It is also "necessary or appropriate" here. As the Supreme Court stated in *New York Telephone* "'[u]nless appropriately confined by Congress, a federal court may avail itself of all auxiliary writs as aids in the performance of its duties." The requested writ is necessary here given the structure of Tycoon 2FA Defendants' technical infrastructure—which takes advantage of the infrastructure and businesses of third parties such as domain registries and registrars. Because of Defendants' unique command and control and randomized registration domain infrastructure, an order enjoining the Defendants here without an AWA directed to domain registries will leave Plaintiffs and then this Court in the unenviable task of playing a game of "whack-a-mole." *See, e.g.*, Arista Records, LLC v. Tkach, 122 F. Supp. 3d 32, 34 (S.D.N.Y. 2015) (noting that, in a domain name seizure case, "Plaintiffs explain that they were then drawn into what they describe as a technological globetrotting game of 'whack-a-mole' in an effort to enforce the TRO").

Requiring these third parties to reasonably assist in the execution of this order will not offend Due Process as the Proposed Order (1) requires only minimal assistance from the third parties in executing the order (transferring domain ownership, which is an act that registrars and registries undertake in the ordinary course of their operations), (2) requires that it be implemented with the least degree of interference with the normal operation of third parties, (3) does not deprive the third parties of any tangible or significant property interests and (4) requires Plaintiffs to compensate the third parties for the assistance rendered. If, in the implementation of the Proposed Order, any third party wishes to bring an issue to the attention of the Court, Plaintiffs will alert the Court immediately. The third parties will have an opportunity to be heard at the preliminary injunction hearing, which must occur shortly after the execution of the Proposed Order. Fed. R. Civ. P. 65(b)(2). The directions to third parties in the Proposed Order are thus narrow, satisfy Due Process, and are necessary to effectuate the requested relief to ensure that the relief is not rendered fruitless. Federal courts across multiple jurisdictions have consistently invoked the All Writs Act to effectuate relief similar to what Microsoft and Health-ISAC are requesting here. *See supra* fn. 2.

VI. AN *EX PARTE* TRO IS THE ONLY EFFECTIVE MEANS OF RELIEF, AND ALTERNATIVE SERVICE IS WARRANTED UNDER THE CIRCUMSTANCES

The TRO that Plaintiffs request must issue *ex parte* for the relief to be effective at all because of the extraordinary factual circumstances here—namely, Tycoon 2FA Defendants' technical sophistication and ability to move their malicious infrastructure if given advance notice. Rule 65 of the Federal Rules of Civil Procedure permits an *ex parte* TRO where the moving party sets forth facts that show an immediate and irreparable injury and why notice should not be required. Fed. R. Civ. P. 65(b)(1); *see Granny Goose Foods, Inc. V. Brotherhood of Teamsters & Auto Truck Drivers, Local No. 70,* 415 U.S. 423, 439 (1974) ("*Ex parte* temporary restraining

orders are no doubt necessary in certain circumstances. . . .").

If notice is given prior to issuance of a TRO, it is likely that the Tycoon 2FA Defendants will quickly mount an alternate infrastructure and direct the vast majority of the phishing operation to operate through that alternate structure before the TRO can have any remedial effects. Richardson Decl. ¶¶ 60-63. Thus, providing notice of the requested TRO will undoubtedly facilitate efforts by the cybercriminals to continue to operate the phishing operation. *Id.* It is well established that *ex parte* relief is appropriate where notice would render the requested relief ineffective. *See, e.g.*, *In re Vuitton Et Fils S.A.*, 606 F.2d 1, 4-5 (2d Cir. 1979) (holding that notice prior to issuing TRO was not necessary where notice would "serve only to render fruitless further prosecution of the action"; prior experience taught that once one member of the counterfeiting enterprise received notice, contraband would be transferred to another unknown); *AT&T Broadband v. Tech Commc'ns, Inc.*, 381 F.3d 1309, 1319-20 (11th Cir. 2004) (affirming *ex parte* search and seizure order to seize contraband technical equipment, given evidence that in the past defendants and persons similarly situated had secreted evidence once notice given); *Little Tor Auto Ctr. v. Exxon Co.*, USA, 822 F. Supp. 141, 143 (S.D.N.Y. 1993) (*ex parte* TRO appropriate where contraband "may be destroyed as soon as notice is given"); *see also AllscriptsMisys, LLC v. Am. Dig. Networks, LLC*, 2010 U.S. Dist. LEXIS 4450, at *2 (D. Md. Jan. 20, 2010) (granting an *ex parte* TRO where "Defendant may dissipate the funds and/or take action to render it difficult to recover funds"); *AT&T Broadband v. Tech Commc'ns, Inc*., 381 F.3d 1309, 1319-1320 (11th Cir. 2004) (affirming *ex parte* search and seizure order to seize contraband technical equipment, given evidence that in the past defendants and persons similarly situated had secreted evidence once notice given). Similarly, in *FTC v. Pricewert LLC*, the district court issued an *ex parte* TRO suspending Internet connectivity of a company enabling botnet activity and other illegal computer-

related conduct on the basis that "Defendant is likely to relocate the harmful and malicious code it hosts and/or warn its criminal clientele of this action if informed of the [plaintiff's] action." *See FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal.) (Whyte, J.) at 3.

It is common, once a cybercriminal's infrastructure becomes publicly known, for the cybercriminal to change or move the infrastructure to evade detection. Richardson Decl. ¶ 60. Microsoft has observed this in prior actions. Richardson Decl. ¶ 63. Like other cybercriminals, Tycoon 2FA Defendants have taken steps to obfuscate their identities (*e.g.*, using legitimate Cloudflare services to circumvent detection). Richardson Decl. ¶¶ 38-39. Thus, Microsoft believes that if given notice, Tycoon 2FA Defendants will take similar steps to shutter their operation. Richardson Decl. ¶ 62-63. Accordingly, granting *ex parte* relief without first providing notice is appropriate. District courts have previously granted similar relief in cases brought by Microsoft to halt similarly situated cybercriminal operations. *See infra* fn. 2.

To ensure due process, immediately upon entry of the requested *ex parte* TRO, Plaintiffs will undertake extraordinary efforts to effect formal and informal notice of the preliminary injunction hearing to the Tycoon 2FA Defendants and to serve the complaint.

A. Plaintiffs Will Provide Notice to the Tycoon 2FA Defendants by Personal Delivery and Through Treaty if Possible.

Plaintiffs have identified domains from which Tycoon 2FA Defendants' infrastructure operate, and, pursuant to the TRO, will obtain from the domain registrars/registries any and all physical addresses of Tycoon 2FA Defendants, to the extent those are available or not fictitious. Pursuant to Rules 4(e)(2)(A) and 4(f)(3), Plaintiffs plan to effect formal notice of the preliminary injunction hearing and service of the complaint by personal delivery of the summons, Plaintiffs' Complaint, the instant motion and supporting documents, and any Order issued by this Court to such addresses in the United States. Poston Decl. ¶ 14. If valid physical addresses of Tycoon 2FA

John Doe Defendants can be identified outside of the United States, Plaintiffs will notice Tycoon 2FA Defendants and serve process upon them through the Hague Convention or similar treaty-based means. *Id.*

B. Plaintiffs Will Provide Notice to Tycoon 2FA Defendants by Email, Facsimile, and Mail

Plaintiffs have identified email addresses, mailing addresses and/or facsimile numbers provided by Tycoon 2FA Defendants, and will seek to identify additional contact information pursuant to the terms of the requested TRO. Poston Decl. ¶ 11. Plaintiffs will provide notice of the preliminary injunction hearing and will effectuate service of the Complaint by immediately sending the same pleadings described above to the email addresses, facsimile numbers and mailing addresses that Tycoon 2FA Defendants provided to the registrars and registries. *Id*. When Tycoon 2FA Defendants registered for domain names, they agreed that notice of disputes regarding hosting could be provided to them by sending complaints to the email, facsimile and mail addresses they provided. *Id.* ¶ 9.

C. Plaintiffs Will Provide Notice to Tycoon 2FA Defendants by Publication:

Plaintiffs will notify Tycoon 2FA Defendants of the preliminary injunction hearing and the Complaint by publishing the materials on a centrally located, publicly accessible source on the Internet. Poston Decl. ¶ 12.

D. Plaintiffs' Proposed Methods of Service Satisfy Due Process

Notice and service by the foregoing means satisfy due process, are appropriate, sufficient, and reasonable to apprise Tycoon 2FA Defendants of this action and are necessary under the circumstances. Plaintiffs hereby formally request that the Court approve and order the alternative means of service discussed above. First, legal notice and service by e-mail, facsimile, mail, and publication satisfies due process as these means are reasonably calculated, in light of the

circumstances, to apprise the interested parties of the TRO, the preliminary injunction hearing, and the lawsuit. *See Mullane v. Cent. Hanover Bank & Tr. Co*., 339 U.S. 306, 314 (1950). Such methods are also authorized under Federal Rule of Civil Procedure 4(f)(3), which allows a party to serve defendants by means not prohibited by international agreement. The methods of notice and service proposed by Plaintiffs have been approved in other cases involving international defendants attempting to evade authorities. *See e.g.*, *Rio Properties, Inc. v. Rio Int'l. Interlink*, 284 F.3d 1007, 1014-15 (9th Cir. 2002) (authorizing service by e-mail upon an international defendant); *Microsoft Corp*., 2014 WL 1338677, at *3 (finding service was proper where plaintiff sent "copies of the original Complaint, Russian translations, a link to all pleadings, and the TRO notice language to all email addresses associated with the Bamital botnet command and control domains" and "published in English and Russian the Complaint, Amended Complaint, Summons, and all orders and pleadings in this action at the publicly available website www.noticeofpleadings.com") (citing Fed.R.Civ.P. 4(f)(3)); *Payne v. McGettigan's Mgmt. Servs. LLC*, 2019 WL 6647804, at *1 (S.D.N.Y. Nov. 19, 2019) (noting courts have found various alternative methods of service appropriate and authorizing service via email on foreign defendant); *Elsevier, Inc. v. Siew Yee Chew*, 287 F. Supp. 3d 374, 379-80 (S.D.N.Y. 2018) (finding that in trademark infringement action, proposed means of service on foreign defendants via email satisfied constitutional standards of due process);\ *AllscriptsMisys, LLC v. Am. Dig. Networks*, LLC, 2010 U.S. Dist. LEXIS 4450, at *3 (D. Md. 2010) (granting *ex parte* TRO and order prompting "notice of this Order and Temporary Restraining Order [] can be effected by telephone, electronic means, mail or delivery services."). Such a service is particularly warranted in cases such as this involving Internet-based misconduct, carried out by international defendants, causing immediate, irreparable harm. As the Ninth Circuit observed:

[Defendant] had neither an office nor a door; it had only a computer terminal. If any method of communication is reasonably calculated to provide [Defendant] with notice, surely it is e-mail-the method of communication which [Defendant] utilizes and prefers. In addition, e-mail was the only court-ordered method of service aimed directly and instantly at [Defendant] . . . Indeed, when faced with an international ebusiness scofflaw, playing hide-and-seek with the federal court, e-mail may be the only means of effecting service of process.

Rio Properties, Inc., 284 F.3d at 1018. Notably, *Rio Properties* has been followed in the Second Circuit. *See Payne*, 2019 WL 6647804, at *1; Elsevier, Inc., 287 F. Supp. 3d at 379- 80.

In this case, the e-mail addresses provided by Tycoon 2FA Defendants to the domain registrar are likely to be the most accurate and viable contact information and means of notice and service. Poston Decl. ¶¶ 9. Moreover, Tycoon 2FA Defendants will expect notice regarding their use of the domain registrars' services to operate the phishing operation by those means, as Tycoon 2FA Defendants agreed to such in their agreements. *See Nat'l Equip. Rental, Ltd. v. Szukhent*, 375 U.S. 311, 315-16 (1964) ("And it is settled . . . that parties to a contract may agree in advance to submit to the jurisdiction of a given court, to permit notice to be served by the opposing party, or even to waive notice altogether."). For these reasons, notice and service by e-mail and publication are warranted and necessary here.[6]

Thus, Plaintiffs request that the Court order that the means of notice of the preliminary injunction hearing and service of the Complaint set forth herein meet Fed. R. Civ. P. 4(f)(3), satisfy due process and are reasonably calculated to notify Tycoon 2FA Defendants of this action.

VII.   CONCLUSION

For the reasons set forth herein, Plaintiffs respectfully request that this Court grant the

---

[6] Additionally, if the physical addressees provided by the Tycoon 2FA Defendants to domain registrars turn out to be false and their whereabouts are unknown, the Hague Convention will not apply in any event and alternative means of service, such as email and publication, would be appropriate for that reason as well. *BP Prod. N. Am., Inc. v. Dagra*, 236 F.R.D. 270, 271 (E.D. Va. 2006) ("The Hague Convention does not apply in cases where the address of the foreign party to be served is unknown.").

Motion for an Emergency *Ex Parte* Temporary Restraining Order and a Preliminary Injunction.

Dated: February 24, 2026

Respectfully submitted,

CROWELL & MORING LLP
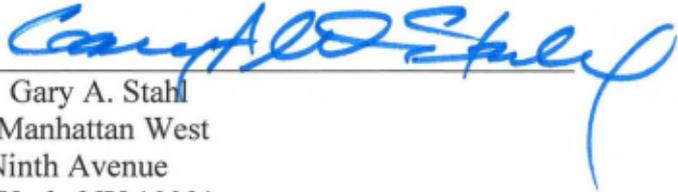
By: _____
    Gary A. Stahl
Two Manhattan West
375 Ninth Avenue
New York, NY 10001
Telephone: (212) 223-4000
Fax: (212) 223-4134
gstahl@crowell.com

Jeffrey L. Poston (*pro hac vice* forthcoming)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington, DC 20004
Telephone: 202-624-2500
Fax: 202628-5116
JPoston@crowell.com

Amanda (Anna) Z. Saber (*pro hac vice* forthcoming)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Telephone: 415-986-2800
Fax: 415-986-2827
ASaber@crowell.com

*Attorneys for Plaintiffs Microsoft Corporation
and Health-ISAC*