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

Microsoft Corporation, a Washington State Corporation and LF Projects, LLC, a Delaware State Series Limited Liability Company, Plaintiffs, v. Abanoub Nady (also known as MRxC0DER), and John Does 1-4, Controlling A Computer Network and Thereby Injuring Plaintiffs and Its Customers, Defendants.	Civil Action No. **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5**

PLAINTIFFS' MEMORANDUM 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, Plaintiffs Microsoft Corporation ("Microsoft") and LF Projects, LLC ("LF Projects") (collectively "Plaintiffs"), respectfully submit this Memorandum in Support of their Motion for an Emergency *Ex Parte* Temporary Restraining Order ("TRO") and a Preliminary Injunction against Abanoub Nady and John Does 1-4, (collectively "Fake ONNX Defendants").

I. INTRODUCTION

This action involves the relentless and persistent phishing attacks conducted and facilitated by a foreign cybercrime organization designated as "Fake ONNX Defendants" against Microsoft, and its customers, including LF Projects. Fake ONNX Defendants, formerly known as "Caffeine," manufacture and sell phishing kits deceptively branded as "ONNX" that are designed to allow

users of the kit to steal sensitive information, compromise business email and perpetrate ransomware and financial fraud. This business model of selling phishing kits and services for use by other cybercriminals is also referred to as "Phishing-as-a-Service" or "PhaaS." The Fake ONNX Defendants sell these PhaaS kits to downstream cybercriminals who set up their own internet domains to perpetrate phishing attacks and add their domains to the Fake ONNX infrastructure. This results in a vast infrastructure overseen and administered by the Fake ONNX Defendants comprised of hundreds of domains that launch phishing attacks against Microsoft and its customers.

These phishing kits are particularly pernicious as they facilitate "adversary in the middle" ("AiTM") attacks whereby the attacker establishes a permanent presence in a victim's system with the ability to intercept communications and affirmatively circumvent the security features of Microsoft products 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. These illegal domains are identified 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' TRO Application ("Poston Decl.") ¶ 7.

Thus, each time a phishing kit is sold, it is done with the express purpose of hacking into Microsoft's products and systems.[1] Further, Fake ONNX Defendants have stolen and misused the trademarks and logo of a legitimate and unrelated brand known as ONNX that is owned by Plaintiff LF Projects. Defendants illegally and without authorization use the ONNX marks and logo to traffic their phishing kits.

These unlawful acts cause Microsoft and LF Projects irreparable harm for which no

[1] Fake ONNX Defendants create customized phishing kits that not only target Microsoft products and services, but other companies as well including Google, Yahoo, and Dropbox.

monetary recourse is available or sufficient. Plaintiffs seek *ex parte* injunctive relief to transfer ownership of the domains that form this infrastructure in order to cripple Fake ONNX Defendants' ability to carry out their phishing operation. Disabling these domains will minimize Fake ONNX Defendants' ability to carry out further attacks against Microsoft, its customers, LF Projects, its projects, and the public.

Ex parte relief is essential. Notice to Fake ONNX Defendants would provide them with an opportunity to destroy, move, conceal, or otherwise make inaccessible the instrumentalities they use to direct Fake ONNX operations and the evidence of their unlawful activity. Courts in numerous cases involving Microsoft have granted this form of relief to disable a cyber criminal's operations to prevent further illegal cybercrime schemes. 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. Microsoft® is a provider of the Windows® computer operating system, and a variety of other software and services including Azure®, Microsoft®, Microsoft 365®, Microsoft Defender®, Microsoft Exchange Server®, Microsoft Office®, Microsoft Sway®, Microsoft Teams®, MSN®, Office 365®, OneDrive®, Outlook®, SharePoint®, Windows®, and Windows Vista®.[2] Due to the high quality and effectiveness of Microsoft's products and services and the

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

expenditure of significant resources by Microsoft to market those products and services, 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. Microsoft has registered trademarks representing the quality of its products and services and its brand, including Azure®, Microsoft®, Microsoft 365®, Microsoft Defender®, Microsoft Exchange Server®, Microsoft Office®, Microsoft Sway®, Microsoft Teams®, MSN®, Office 365®, OneDrive®, Outlook®, SharePoint®, Windows®, and Windows Vista®.

B. LF Projects' Services and Reputation

LF Projects is a collection of limited liability companies that owns the registered trademarks associated with technology projects and ecosystems. LF Projects owns the trademarks for both the "ONNX" name and logo. These are linked to a project known as the Open Neural Network Exchange, or "ONNX." The ONNX Exchange is an open-source artificial intelligence ecosystem of technology companies and research organizations that establishes open standards for representing machine learning algorithms and software tools to promote innovation and collaboration in the AI sector.

C. Fake ONNX Defendants Control Phishing Operation

1.What are the Fake ONNX Defendants?

Fake ONNX Defendants are prolific cyber criminals that develop and sell ONNX-branded phishing kits, and also provide Phishing-as-a-Service ("PhaaS") to other cybercriminals. Downstream cybercriminals purchase the ONNX-branded phishing kits from the Fake ONNX Defendants and launch phishing attacks against a multitude of organizations across various industries. Declaration of Jason B. Lyons in Support of Plaintiffs' TRO Application ("Lyons Decl.") ¶¶ 6, 10. Fake ONNX Defendants first emerged in October 2017 under the brand name

""bl4ck-tools-net." *Id.* ¶ 11. From 2017 to 2020, Abanoub Nady used various branding in connection with his phishing kits. *Id.* In 2020, the phishing kit was distributed under the branding "Caffeine," which was used for several years. *Id.* Subsequently, in 2024, the Defendants transitioned to the brand "ONNX." *Id.* The focus of Fake ONNX Defendants is not limited to Microsoft and its customers. Indeed, Fake ONNX Defendants offer phishing kits designed to target a variety of companies across the technology sector, including Google, Dropbox, Rackspace, Yahoo, and Microsoft. Lyons Decl. ¶ 8.

The phishing operation is carried out by Abanoub Nady and John Does 1-4. *Id.* ¶¶ 12, 15-19. Microsoft was able to attribute the MRxC0DER username associated with Caffeine/ONNX to Defendant Abanoub Nady through their investigation into the Fake ONNX Defendants, which included a "test buy" of the phishing kit. *Id.* ¶ 12. Microsoft's investigation was validated on or around June 19, 2024, when security threat researchers published an article which connected MRxC0DER to Defendant Abanoub Nady. *Id.* ¶ 13.

In addition to causing significant harm to its phishing victims, Fake ONNX Defendants appear to have also stolen their name and logo from an unrelated and innocent third-party: the ONNX Exchange. Declaration of Michael Dolan in Support of Plaintiffs' TRO Application ("Dolan Decl.") ¶¶ 5-7.

2. Fake ONNX Defendants' *Modus Operandi*

Much like how legitimate companies develop and sell all-in-one do-it-yourself kits to normal customers for personal projects, Fake ONNX Defendants manufacture "do it yourself" phishing kits for cybercriminals to purchase and use for their cybercrime operations. Lyons Decl. ¶ 21. These cybercriminals become part of the Fake ONNX Defendants' operation when they, in turn, deploy the ONNX-branded phishing kits to conduct phishing attacks by positioning

themselves between communications directed to and from Microsoft customers. *Id.* Attacks based on positioning the attacker between Microsoft customers that use more complex tools to intercept data traffic are known as "Adversary-in-the-Middle" or ("AiTM") attacks. This positioning allows the attacker to intercept the traffic between Microsoft customers including the input of credentials and passwords to access a Microsoft customer's email systems. Phishing is the fraudulent practice of sending emails or other messages purporting to be from legitimate senders in order to induce recipients to reveal personal information, such as passwords or other credentials. Lyons Decl. ¶ 9. 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"). *Id.* ¶ 7. Fake ONNX Defendants develop and sell ONNX-branded phishing kits that 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. *Id.* ¶ 24.

Fake ONNX Defendants' phishing kits are specifically developed to target Microsoft 365 and Azure users, and include two-factor (2FA) authentication bypass features for the Microsoft Authenticator application and Microsoft Office, specifically the Outlook application. Lyons Decl. ¶ 25. The incorporation of sophisticated tools like collecting 2FA codes and developing a way to bypass multi-factor authentication security features is an example of Fake ONNX Defendants using an AiTM attack as a method to facilitate its phishing operation. The malicious phishing kits developed by Fake ONNX Defendants support credentials theft, information exfiltration, and subsequent end-user terminal attacks which include business email compromise, ransomware, and financial fraud. *Id.* ¶¶ 20, 25, 44.

These Fake ONNX Defendants' phishing operations are made possible by leveraging a vast infrastructure of website domains. Lyons Decl. ¶ 14. Also known as a web address, domains are used to identify a website and allow users on the internet to access the website. *Id.* Fake ONNX Defendants include the domains in their phishing emails and when the victims click on the malicious domains they are redirected to a Fake ONNX-controlled webpage and then unknowingly provide their credentials to Defendants. *Id.* The identity of the website domains used by Fake ONNX Defendants to support their phishing operation are set forth at **Appendix A** to this Complaint and constitutes Fake ONNX Defendants' technical infrastructure. *Id.* A successful phishing attack relies on a victim being convinced that the email communication received or a website they are directed to is authentic. Lyons Decl. ¶ 22. This is made possible when the communication they receive appears to be from familiar contacts or organizations (even when the communication is not actually from a known contact or organization). *Id.* This is done by creating an email address that is designed to look similar to a legitimate email address, for example using "5" instead of "s" or "nn" instead of "m." *Id.* Similarly, when a victim is tricked into clicking on a Fake ONNX-controlled domain, they will be deceived into believing that the domain is benign, if the domain name appears to refer to a company name or its well-known products. *Id.* For example, if the authentic domain name is www.microsoft.com, a phishing domain may appear to be www.microsft.com or www.m1crosoft.com, where a letter is missing (the "o" in "soft") or a number is in place of a letter (here the number "1" in place of the letter "i"). *Id.* This is a practice known as either a "homoglyph" domain or "typosquatting." *Id.* As a result, the phishing domain may easily be perceived as the authentic domain. Lyon Decl. ¶ 22 This action seeks to takedown this technical infrastructure to render Fake ONNX Defendants incapable of continuing their attacks and transferring ownership and control of these domains to Microsoft. *Id.* ¶¶ 66-67.

Fake ONNX Defendants use Microsoft's logos in their phishing emails, such as Outlook and Microsoft 365 to further enhance the perceived legitimacy of the attack. Lyons Decl. ¶ 41. In doing so, Fake ONNX Defendants capitalize on and misuse the brand recognition that Microsoft has cultivated, and the trust Microsoft has built with its customers. *Id.* ¶ 60.

When a phishing victim is deceived to visit a website to enter their credentials, Fake ONNX Defendants lie in wait to collect those credentials in order to subsequently access their accounts to further their cybercrime. This AiTM attack makes the ONNX-branded phishing kits particularly dangerous because Fake ONNX Defendants trick users into clicking a link and completing MFA on the attacker's behalf and subsequently use this initial authorization to grant them continued access to accounts and later engage in further cybercriminal activities including business email compromise, financial fraud, and ransomware attacks.

3.The Attack Chain

Step 1: Development and Sale of ONNX-Branded Phishing Kits

The phishing kits that are designed, manufactured, and sold by the Fake ONNX Defendants are specifically designed to provide customers a do-it-yourself toolkit to phish Microsoft customers and infiltrate Microsoft systems. Lyons Decl. ¶ 24. Specifically, these 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. *Id.* For example, one observed phishing kit is named the "Office 2FA Cookies Stealer," because it is designed to intercept the transmission of a victim's 2FA (two factor authorization) code used to verify the victim's identity when they log into their Outlook account. *Id.* ¶ 25. These malicious phishing kits support

credentials theft, information exfiltration, and subsequent end-user attacks which include business email compromise, ransomware, and financial fraud. *Id.* ¶¶ 20, 25. Fake ONNX Defendants are able to execute these end-user attacks more readily when they are able to access a victim's Azure cloud platform, which serves as gateway to other computer applications, and where these applications are connected through global Microsoft network infrastructure. *Id.* ¶ 25.

The ability to infiltrate Microsoft's systems is a "selling point" of the ONNX-branded phishing kits. Lyons Decl. ¶ 26. Cybercriminal customers purchase these ONNX-branded kits because they have the capability to infiltrate Microsoft systems and the significant security protocols that Microsoft implements to protect against cyberattacks. *Id.*

Another advertised feature is the ability to customize logos and email templates to further mimic authenticity in the phishing email. Lyons Decl. ¶ 27. The Fake ONNX Defendants sell their ONNX-branding kits online at the "ONNX Store" (formerly known as the "Caffeine Store") for cybercriminals to purchase. Lyons Decl. ¶ 28.

The Fake ONNX-branded phishing kits are promoted through Telegram Messenger, a secure, cloud-based messaging platform. It is known for its end-to-end. Lyons Decl. ¶ 29. Fake ONNX Defendants have set up Telegram accounts and "channels" (a thread that allows the admin of the channel to post information to a larger audience) to facilitate private communications between the Fake ONNX Defendants and potential customers interested in purchasing the phishing kits. *Id.*

To advertise their phishing kits, Fake ONNX Defendants also use social media platforms, like YouTube to provide "how to" videos on the purchase and implementation of these phishing kits. Lyons Decl. ¶ 30. Mr. Nady also uses the MRxC0DER handle to advertise the phishing kits on Telegram. *Id.*

The Fake ONNX Defendants do not just sell their phishing kit for one-time use. Lyons Decl. ¶ 31. Rather, to maximize their financial gain, they take steps to ensure the repeated use of their products. *Id.* The Fake ONNX Defendants offer their customers a phishing kit subscription model, offering Basic, Professional, and Enterprise subscriptions, each for different tiers of access. *Id.* Enterprises users can also purchase the add-on feature of "Unlimited VIP Support," essentially ongoing technical support that provides step-by-step instructions on how to successfully commit cybercrime. *Id.*

Another advertised feature of the phishing kits is their undetectable nature. Lyons Decl. ¶ 32. Cybercriminals and threat actors generally make extensive efforts to avoid detection and conceal their identity. *Id.* This makes sense; if they remain undetected, they can avoid law enforcement and continue their criminal activities. *Id.* The Fake ONNX are no different. *Id.* Their phishing kits includes an anti-bot application programming interface ("API"). *Id.* Ordinarily legitimate websites check to determine if the user accessing the website is a human or a bot (a computer program that runs tasks without human intervention). *Id.* This may involve requiring the user to select all images that show the same object or require the end user to enter in a series of letters and numbers displayed in an image. Lyons Decl. ¶ 32. Only when the user correctly "proves" they are a human are they able to access a website. *Id.* The anti-bot API is used to circumvent and bypass these security tools on a victim's computer by preventing an email service from being able to scan for bot activity or scan to determine whether an email contains malicious content of links to malicious websites. *Id.* In general, an email service like Outlook has sophisticated security tools to scan incoming email for potential phishing emails, spam, or compromised messages. *Id.* The anti-bot API serves as a blocker to prevent these security tools from working as they are supposed to, which allows the Fake ONNX Defendants to circumvent

the security tools. *Id.*

Step Two: Activation of ONNX-Branded Phishing Kits and Malicious Domains

Once the Fake ONNX Defendants sell an ONNX-branded phishing kit to a cybercriminal customer, the customer must take several steps to activate the phishing kit and incorporate the malicious domain into the Fake ONNX Defendants internet infrastructure. Lyons Decl. ¶ 33.

The first activation step is purchasing domains. Lyons Decl. ¶ 34. The Fake ONNX Defendants' cybercriminal customers must purchase a domain from a registrar (a third-party company, like GoDaddy that makes domains available for purchase). [3] *Id.* The Fake ONNX Defendants follow a "bring your own domain" model, where each cybercriminal customer is responsible for bringing their own pre-purchased domain to connect into the overarching Fake ONNX internet infrastructure. *Id.* The domains registered are purposefully named by cybercriminals to appear, at first glance, to be related to Microsoft or its products. *Id.* But these domains actually contain subtle misspellings — e.g., "onliine" (with two of the letter "i) instead of "online" (the word correctly spelled), which is a practice known as using a "homoglyph" domain or "typosquatting." *Id.* ¶ 22. Because these domains will be used by the cybercriminal customers to carry out phishing attacks, Fake ONNX Defendants focus on manufacturing "legitimacy" and employing tactics like typosquatting to hide the sinister nature of the malicious domain. *Id.*

The second activation step is to establish the requisite infrastructure to obfuscate identity. Lyons Decl. ¶ 35. Fake ONNX Defendants direct their cybercriminal customers to create an account on Cloudflare, Inc. ("Cloudflare") to further evade detection. *Id.* Cloudflare is a company that provides a variety of legitimate network services and security features to protect their users

[3] In the earlier version of the Fake ONNX Defendants' phishing operation, Abanoub Nady would register malicious domains and incorporate it directly into the phishing operation. Fake ONNX Defendants have since transitioned to a "Bring Your Own Domain" model.

from online cyberthreats and attacks. *Id.* These features include IP proxying and a CAPTCHA service to authenticate that a website link is legitimately clicked by a human. *Id.*

Cloudflare provides an IP proxy feature for account holders, which acts like a middleman to protect the privacy of domain owners. Lyons Decl. ¶ 36. An IP Proxy allows legitimate, honest users to have an intermediary in place to determine the legitimacy of an incoming email. *Id.* The Fake ONNX Defendants have hijacked this proxy to conceal their "home address" (their real IP address). *Id.* This means that the IP address will show a fictitious location on domain records that list the domain's IP address, which further allows Fake ONNX Defendants to evade detection. *Id.*

CAPTCHAs help websites confirm that a user interacting with the website is a human and not a bot, which is an automated program designed to act without human direction to automatically do specific tasks (like access a website). Lyons Decl. ¶ 37. CAPTCHAs are designed to protect normal consumers. *Id.* In this instance, Fake ONNX Defendants use Cloudflare's CAPTCHA feature to prevent email security programs that would deploy automated programs (bots) to check if an email has malicious content or links to malicious websites. *Id.* Here, Fake ONNX Defendants use CAPTCHA to keep out security bots in order to prevent them from checking a website link in an email address to see if it is malicious. By eliminating the probability of being detected, Fake ONNX Defendants are able to deliver phishing emails to its victims without any alarm bells going off. *Id.*

The Fake ONNX Defendants abuse and misuse these legitimate services offered by Cloudflare to perpetrate their cybercrimes. Lyons Decl. ¶ 38. It is common for a cybercriminal to abuse and misuse an otherwise legitimate software or tool for the purposes of committing cybercrime. *Id.* This is done intentionally because the cybercriminal can simply retool an existing product, which is more efficient than creating one from scratch. *Id.* Additionally, the cybercriminal

can capitalize on the branding and goodwill associated with the legitimate product because victims will be unaware that they are interacting with a malicious version of a product or service that they would ordinarily consider to be "safe." *Id.*

By misusing Cloudflare's services, Fake ONNX Defendants can obscure the real location of their phishing websites and can employ measures like CAPTCHA to make it harder for automated security scanning systems to detect and block their phishing websites. Lyons Decl. ¶ 39. By preventing scanning, the Fake ONNX Defendants can increase their phishing campaign efficiency: they protect themselves from being discovered which lessens the chance that they are shutdown, either by the third-party registrars or law enforcement. *Id.*

Step Three: Connecting to the Fake ONNX Defendants' Phishing Operation

Next, Cloudflare provides an API key (a code used to identify and authenticate a user in Cloudflare). Lyons Decl. ¶ 40. At the request of the Fake ONNX Defendants, the cybercriminal customer provides the API key to Fake ONNX Defendants. *Id.* On the backend, the Fake ONNX Defendants use the API key code to connect the cybercriminal's domain (the one that is designed to look like it refers to Microsoft or a Microsoft product) into Fake ONNX Defendants' overarching infrastructure. *Id.*

Step Four: Further Phishing Attacks by Fake ONNX

The next step involves the Fake ONNX Defendants deploying the phishing kits and engaging in phishing attacks. Lyons Decl. ¶ 41. Cybercriminals who purchase phishing kits from Fake ONNX Defendants will send phishing emails to victims that prompt the victim to click on a link. *Id.* The phishing email will often use Microsoft's logos. *Id.* This unauthorized use of the logo makes it appear as if Microsoft is sending an email to its customer with a call to action related to one of Microsoft's services. *Id.*

The phishing email will also invite the victim to click on a link contained in the body of the email, click on a link contained within a PDF, of click on a QR code. Lyons Decl. ¶ 42. The link is one that was purchased by cybercriminal customers and connected to the overarching internet infrastructure. *Id.* As described above, because the domains appear to be related to Microsoft or a Microsoft product the victims believe the domain is safe, and they are lulled into a false sense of security. If the victim clicks on the link to the malicious phishing domain, they are directed to a website that contains a login page. *Id.* Although the login page is fabricated to look like an authentic Microsoft login page by using Microsoft's name and branding, in reality the login page is fraudulent. *Id.* Based on Microsoft's investigation, in many instances the fraudulent login page was created by using the template that was provided in the ONNX-branded phishing kit. *Id.* When the victim enters their login credentials (their real credentials for their Microsoft account), they will be directed to verify their password and complete the 2FA process. *Id.*

Through asking the victim to enter their password and verify their identity, Fake ONNX Defendants capture the victim's account credentials. Lyons Decl. ¶ 43. At this point, the Fake ONNX Defendants will prompt the victim to provide their phone number to receive their 2FA token to verify their identity and access their account. *Id.* A 2FA token is a unique piece of code that contains information about the user's identity and authorized access. *Id.* For example, it may be a six-digit code that the user must enter after they have entered their login credentials. *Id.* Once the victim enters their phone number, receives the 2FA token, and enters the token into Fake ONNX Defendants' fraudulent login page, their phone number and 2FA tokens are captured by Fake ONNX Defendants. *Id.*

This verification then allows Fake ONNX Defendants' malicious website to be perceived by victims' computers as legitimate and any potential access to the site or communication to the

victim may be fraudulently permitted. Lyons Decl. ¶ 44. At this point, Fake ONNX Defendants can log into the user's real account and take control of the account. *Id.* For example, if the victim entered their Outlook email credentials, Fake ONNX Defendants would now have complete access to the victim's Outlook account, including the inbox, the sent folder, their calendar, contact list, and any files attached to emails within the account. *Id.* Fake ONNX Defendants subsequently exploit this access to their victim's devices to perpetrate further cybercrime such as ransomware, business email compromise and financial fraud. *Id.* They can also use this access to identify additional phishing victims and facilitate those additional attacks. *Id.* For example, if the victim is a manager at a company, Fake ONNX Defendants can impersonate the manager and then phish other employees. *Id.*

Subsequently, a Fake ONNX Defendant may engage in additional phishing attack, may purchase additional domains to connect to the internet infrastructure, or if their subscription to the ONNX-branded phishing kits has lapsed, purchase an additional subscription. Lyons Decl. ¶ 45. This process can be replicated with ease, which allows Fake ONNX Defendants to scale their criminal organization. *Id.*

4. Test Buy

As part of Microsoft's investigation, on April 18, 2024, Microsoft conducted a test buy of the ONNX-branded phishing kits. Lyons Decl. ¶ 47. To do so, Microsoft first accessed the ONNX Store where Microsoft began communicating via Telegram, under a pseudonym, with the Fake ONNX Defendants who have the specific responsibility of promoting, advertising, and selling the ONNX-branded phishing kits. *Id.* Microsoft pretended to be interested in purchasing a phishing kit to further the communication with Fake ONNX Defendants. *Id.* Once Microsoft had demonstrated interest in purchasing a phishing kit, the chat administrator provided payment

information that would allow the transfer of money via a Bitcoin wallet. *Id.* Once the money was transferred, Microsoft received a message that the order had been successfully placed for the phishing kit. *Id.*

Once Microsoft successfully purchased the phishing kit, Microsoft was instructed to add the domain, and Microsoft was directed to the FAQ page with instructions on how to add the domain Microsoft separately purchased to the Fake ONNX Defendants' infrastructure. Lyons Decl. ¶ 48. The FAQ page includes a link to a how-to video on how to add the domain using the API key. *Id.*

In the video, the Fake ONNX Defendants walk through how to change where the malicious domain resolves (or redirects) to further obfuscate the identity. Lyons Decl. ¶ 49. This involves creating a free Cloudflare account, and then changing the name server of the malicious domain to Cloudflare. *Id.* A name server is a computer application that translates a domain name into an IP address, which connects the user to the website they are trying to visit. *Id.* By changing the name server to Cloudflare, someone trying to investigate the domain will simply see Cloudflare, but nothing more. *Id.* On the backend however, because the cybercriminal customer provided the API key to the Fake ONNX Defendants, the malicious domain redirects to the Fake ONNX internet infrastructure—but this is undetected. *Id.* Using the FAQ and how-to video, Microsoft was able to follow these steps to add the domains Microsoft had purchased to the ONNX phishing kit subscription was able to connect via API key to Cloudflare.

Because Microsoft purchased these domains, Microsoft was able to use the domains to gain telemetry about the Fake ONNX Defendants' infrastructure. Lyons Decl. ¶ 50. Additionally, Microsoft was able to conduct a test phishing attack by using the phishing kit Microsoft had purchased to "phish" a Microsoft account that was specially created for this investigation. *Id.* This

allowed Microsoft to observe how the phishing kit operated.

5. Attribution to the Fake ONNX Defendants

Microsoft investigated the online infrastructure used in the Fake ONNX Defendants' phishing campaign. Lyons Decl. ¶ 51. Microsoft determined that Defendants have registered Internet domains using fictitious names and fictitious physical addresses that are purportedly located in multiple cities and countries. *Id.* The Fake ONNX Defendants have registered domains using functioning email addresses by which they communicated with domain registrars to complete the registration process. *Id.*

Cybercriminals like the Fake ONNX Defendants are known to obfuscate their identities to evade capture by law enforcement and continue their cybercrime. Lyons Decl. ¶ 52.

In the course of the investigation, Microsoft engaged in the analysis and creation of "signatures" (which can be thought of as digital fingerprints) for the infrastructure used by the Defendants. Lyons Decl. ¶ 53. By identifying these signatures, Microsoft was able to determine that the domains identified in **Appendix A** belong to and are used by the Fake ONNX Defendants. *Id.* Specifically, the following indicators were used in the assessment: domain registration patterns, phishing URL patterns and components based on known Fake ONNX 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. *Id.*

These features, when taken together, provide a high level of confidence that a given domain is a Fake ONNX domain. Lyons Decl. ¶ 54. 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 Fake ONNX 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 Fake ONNX Defendants. *Id.* Other researchers in the security community have independently identified Fake ONNX domains and associated IP addresses, and these reports may be used to further validate Microsoft's analysis. *Id.* These high confidence domains are identified in **Appendix A.**

D. Harm to Microsoft and LF Projects

Fake ONNX Defendants have targeted Microsoft, its customers, and the public to advance their financially – motivated cybercrimes. Lyons Decl. ¶ 56. Fake ONNX Defendants have caused and continue to cause irreparable injury to Microsoft, its customers, LF Projects, and the public. *Id.* The Fake ONNX Defendants' activities irreparably harm Microsoft by damaging its reputation, brands, and customer goodwill. *Id.*

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. Microsoft® is a provider of the Windows® computer operating system, and a variety of other software and services including Microsoft 365®, Office365®, Office®, Microsoft Office®, SharePoint®, OneDrive®, Outlook®, Microsoft Exchange Server®, Teams®, Microsoft Defender®, Windows Vista®, Sway®, and Azure®. Lyons Decl. ¶ 57. Microsoft has invested substantial resources in developing high quality products and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, and has developed the Microsoft name and the names of its products and services into strong and famous worldwide symbols that are well-recognized within its channels of trade. *Id.*

The Fake ONNX Defendants' criminal acts directly harm Microsoft's reputation and goodwill that it has earned through its extensive branding efforts. Lyons Decl. ¶ 58.

First, ONNX-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. Lyons Decl. ¶ 59. Thus, each time a phishing kit is sold, it is done with the express purpose of hacking into Microsoft's products and systems—the very products and systems that Microsoft expends significant resources to protect the associated security, quality, and good will. *Id.*

Second, Fake ONNX Defendants leverage Microsoft systems and programs, such as Outlook and Microsoft 365 to further enhance the perceived legitimacy of the attack. Lyons Decl. ¶ 60. Similarly, because the login pages that Fake ONNX Defendants use includes 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, Fake ONNX 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. *Id.*

Third, the domains used by Fake ONNX are intentionally designed to mimic the name Microsoft and its products. Lyons Decl. ¶ 61. For example, sharepointonline-microsoft[.]com incorporates both "Microsoft" and "SharePoint," which is Microsoft's online document management platform. Likewise, loginoffice[.]com references "Office," which is the name Microsoft gives to the family of software that includes Word, Excel, and PowerPoint. *Id.* In each

instance, a victim who sees these domains would believe they are visiting a Microsoft website. *Id.*

Customers expect a certain quality from Microsoft. Lyons Decl. ¶ 62. When "Microsoft" systems and products are used in connection with cybercrime, customers will mistakenly believe that Microsoft is responsible for the attack. *Id.* 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 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 blames Microsoft for a phishing attack or believes that Microsoft's systems and products are not secure, it may be costly or impossible to convince the customer to return to Microsoft. *Id.*

Microsoft has invested significant resources in excess of $5,000 to address and attempt to remediate the harm caused by Fake ONNX Defendants' crimes. Lyons Decl. ¶ 64. Specifically, Microsoft has spent approximately $650,000, which represents the investment into personnel and the cost of time expended by Microsoft DCU personnel to investigate the Fake ONNX Defendants and their infrastructure. *Id.*

In addition to causing irreparable harm to its phishing victims, Fake ONNX Defendants have also stolen their name and logo from LF Projects' ONNX Exchange. Dolan Decl. ¶¶ 5-7. The "ONNX" name and logo are registered to LF Projects. ONNX Exchange and the ONNX-branded phishing kit share not only the same name, but also the same geometric shape as the logo. *Id.* This causes significant confusion between Plaintiff LF Projects' ONNX Exchange and Fake ONNX Defendants' ONNX-branded phishing kits. *Id.* ¶ 9-11. The mere fact that Plaintiffs had to create artificial names to describe Plaintiff LF Projects' Open Neural Network Exchange project

and Fake ONNX Defendants to distinguish the parties establishes the very real likelihood of confusion. Complaint, ¶ 7, n.2

In fact, through research and investigation, LF Projects has found that when searched online, the ONNX Exchange website (onnx.ai) and articles discussing the phishing activities perpetuated by Fake ONNX Defendants appear on the same results page and make clear reference to the "ONNX" name. Dolan Decl. ¶ 11.

Fake ONNX Defendants irreparably harms LF Projects' goodwill by damaging its projects' reputation, brands, and partner goodwill. Dolan Decl. ¶¶ 10, 13. Fake ONNX Defendants' use of the "ONNX" trademark leads to confusion as to the malicious phishing activities perpetrated by Fake ONNX Defendants and may lead to attribution to the ONNX Exchange. *Id.* Many major tech companies contribute to the community of the ONNX Exchange. Dolan Decl. ¶ 13. Malicious activities wrongly attributed to the ONNX Exchange would potentially implicate the community of organizations, and affect the goodwill and reputation cultivated over time through collective thoughtful works of the organizations who are members of the ONNX Exchange.

LF Projects has invested significant resources in excess of $5,000 to address and attempt to remediate the harm caused by Fake ONNX Defendants' crimes. Dolan Decl. ¶ 15. Specifically, LF Projects have spent $27,000 to investigate and address the harms caused by Fake ONNX. *Id.*

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. *United States v. South Carolina*, 720 F.3d 518, 524 (4th Cir. 2013) (citations omitted). "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) (citing *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008)).

IV. PLAINTIFFS' REQUESTED RELIEF IS WARRANTED

There is a high likelihood that Plaintiffs will succeed on the merits. Microsoft, its customers, LF Projects, its projects, and the public will continue to be irreparably harmed if Fake ONNX Defendants are able to continue their cybercriminal operation. Every day that passes gives Fake ONNX Defendants further opportunity to carry out additional phishing attacks, steal email credentials, and invade the privacy of the victims' email inboxes. Unless enjoined, Fake ONNX Defendants will continue to irreparably harm Plaintiffs. Plaintiffs' requested relief is warranted because the effect on third parties (such as domain registries) will be negligible and temporary. Comparatively, if a TRO and preliminary injunction are issued, no legitimate interest of Fake ONNX Defendants will not be harmed – indeed, they do not have *any* legitimate interest that would allow them to continue committing cybercrime. Finally, the public interest also weighs heavily in favor of relief because the same injury inflicted on Plaintiffs by the Fake ONNX Defendants affect the public, because they too are victims of Fake ONNX Defendants' criminal activity. Accordingly, this matter presents a quintessential case for injunctive relief.

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' Complaint alleges the 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 Plaintiffs' 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 Fake ONNX 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.

1. Fake ONNX 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., Big Rock Sports, LLC v. AcuSport Corp.*, No. 4:08-CV-159-F, 2011 WL 4459189, at *1 (E.D.N.C. Sept. 26, 2011). "Any computer with Internet access [is] subject [to] the statute's protection." *Id. 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 interstate or foreign commerce or communication." *See Estes Forwarding Worldwide LLC v. Cuellar*, 239 F. Supp. 3d 918, 926 (E.D. Va. 2017). "The phrase 'exceeds authorized access' means 'to access a computer without authorization and to use such access to obtain or alter information in the computer that the accessor

is not entitled to obtain or alter.'" *Id.* at 923 (citing 18 U.S.C. § 1030(e)(6)). In order 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." *Sprint Nextel Corp. v. Simple Cell, Inc.*, No. CIV. CCB-13-617, 2013 WL 3776933, at *6 (D. Md. July 17, 2013) (citing 18 U.S.C. § 1030(e)(8)). "'[D]amage . . . means any impairment to the integrity or availability of data, a program, a system, or information.'" *Id.* (citing 18 U.S.C. § 1030(e)(11)). The Fourth Circuit has recognized that this "broadly worded provision plainly contemplates consequential damages" such as "costs incurred as part of the response to a CFAA violation, including the investigation of an offense." *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009). The CFAA permits plaintiffs to aggregate multiple intrusions or violations for the purposes of meeting the $5,000 statutory threshold. *See Sprint Nextel Corp.,* 2013 WL 3776933, at *7 (citations omitted).

In sum, in order to prevail on their CFAA claim, Plaintiffs must establish that Fake ONNX Defendants (1) accessed a protected computer; (2) without authorization; (3) for the purpose of obtaining information or defrauding others; (4) resulting in loss or damage in excess of $5,000. Jason Lyons' Declaration establishes that Fake ONNX Defendants' conduct satisfies each of these elements. Fake ONNX Defendants knowingly and intentionally accessed and continue to access protected computers without authorization and knowingly caused the transmission of a program, information, code, and commands, resulting in damage to the protected computers, the software residing thereon, and Microsoft. The amount of harm caused by the Fake ONNX Defendants

exceeds $5,000. For example, Microsoft alone spent at least $650,000 and 3,500 hours investigating and remediating Fake ONNX Defendants' activities, including engaging teams across four different countries. Lyons Decl. ¶ 64. LF Projects has spent at least $27,000 investigating and remediating the harms caused by Fake ONNX. Dolan Decl. ¶ 15.

Fake ONNX Defendants' conduct is precisely the type of activity that the Computer Fraud and Abuse Act is designed to prevent. *See, e.g.*, *Physicians Interactive v. Lathian Sys., Inc.*, No. CA 03-1193-A, 2003 WL 23018270, at *1 (E.D. Va. Dec. 5, 2003) (granting TRO and preliminary injunction under CFAA where defendant hacked into a computer and stole confidential information); *Glob. Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant actionable under the CFAA); *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 is likely to succeed on the merits of its CFAA claim.

2. Fake ONNX Defendants' Violation of 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. § 1 964(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 2020 when Abanoub Nady, John Doe 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 criminal activities including business email compromise, financial fraud, and ransomware. John Does 3-4 joined the conspiracy and began participating in the Racketeering

Enterprise at various times thereafter. *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"). The Racketeering Enterprise has continuously and effectively carried out its purpose of operating their PhaaS business model, with use of the ONNX-branded phishing kits at the core of the operation ever since and will continue to do so absent the relief Plaintiffs request.

Both the purpose of the Racketeering Enterprise and the relationship between Fake ONNX Defendants is proven by: (1) the repeated development and dissemination of ONNX-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 Phishing as a Service; and (3) Fake ONNX Defendants' respective and interrelated roles in the sale, operation of, and profiting from the ONNX-branded phishing kits in furtherance of Fake ONNX 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). Fake ONNX Defendants have conspired to, and have, conducted, and participated in the operations of the Racketeering Enterprise through a continuous pattern of

racketeering activity. Each predicate act is related and in furtherance of the common unlawful purpose shared by the members of the Racketeering Enterprise. These acts are continuing and will continue unless and until this Court grants Plaintiffs' request for a temporary restraining order.

Fake ONNX Defendants' racketeering acts include persistent violations of the Computer Fraud and Abuse Act (CFAA). Whoever knowingly and with intent to defraud traffics in any password or similar information through which a computer may be accessed without authorization, if such trafficking affects interstate or foreign commerce, violates the Computer Fraud and Abuse Act. 18 U.S.C. § 1030(a)(6)(A). 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).

Fake ONNX Defendants' conduct is also "racketeering activity" in the form of wire fraud under 18 U.S.C. § 1343 (violation where one "having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire ... communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice."). Fake ONNX Defendants transmitted communication amongst themselves and to their victims via wire (email communications and online Telegram messages) that crossed U.S. state and international boundaries. These transmissions resulted not only in defrauding victims to provide their credentials, but it also allowed Fake ONNX Defendants to receive monetary benefits through the sale of the ONNX-branded phishing kits.

Plaintiffs Were Harmed as a Direct Result of Defendants' Racketeering Activity

As a direct result of Fake ONNX Defendants' conduct, Microsoft has been forced to spend at least $650,000 and 3,500 hours investigating and remediating Fake ONNX Defendants'

activities, including engaging teams across four different countries. Similarly, as a direct result of Fake ONNX Defendants' conduct, LF Projects has been forced to spend at least $27,000 to investigate Fake ONNX Defendants' activities and mitigate the impact to its projects. *See* Dolan Decl. ¶¶ 15. 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 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. Fake ONNX Defendants' Violation of the Electronic Communications Privacy Act

The Electronic Communications Privacy Act ("ECPA") 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). ECPA is violated when defendant logs into Plaintiffs' customers' account without permission (including with stolen credentials) and intentionally accesses the contents of an inbox. *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).

Fake ONNX Defendants' conduct in carrying out their criminal objectives violates the ECPA because they break into computer networks using ill-obtained credentials with the direct intention of acquiring the contents of the victims' email inbox and exfiltrating sensitive business or personal information. Microsoft's Windows operating system software and Microsoft's customers' computers running such software are facilities through which electronic communication services are provided to users and customers. *See* Lyons Decl. ¶ 25, n.5. Fake ONNX Defendants knowingly and intentionally accessed the Windows operating system and associated software, services, and computers upon which this software and services run without authorization or in excess of any authorization granted by Microsoft. *See* Lyons Decl. ¶ 44.

Through this unauthorized access, Fake ONNX 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. *See* Lyons Decl. ¶¶ 9, 25.

Obtaining stored electronic information in this way, without authorization, is a per se violation of ECPA. *See Council on Am.-Islamic Relations v. Gaubatz*, 667 F. Supp. 2d 67, 71-73 (D.D.C. 2009) (granting preliminary injunction in case where plaintiff brought ECPA claims after defendant removed 12,000 internal, sensitive documents including emails and other documents and made video and audio recordings of private meetings and published this information); *Human Touch*, 2015 WL 12564162, at *2 (plaintiff likely to succeed on merits for purpose of TRO where defendant accessed Capitol View's email system without authorization for purpose of accessing sensitive communications and patient information). Thus, Microsoft is likely to succeed on the merits of its ECPA claims.

4. Fake ONNX 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. *See JFJ Toys, Inc. v. Sears Holdings Corp.,* 237 F. Supp. 3d 311, 340 (D. Md. 2017) (citing 15 U.S.C. § 1114(1)(a)). Fake ONNX Defendants distribute copies of Plaintiffs' registered and distinctive trademarks in fraudulent schemes designed to mislead victims into clicking on links to interact with malicious websites, and in fraudulent versions of Defendants' websites, which deceive victims, causes them confusion, and causes them to mistakenly associate Plaintiffs with this activity. Fake ONNX Defendants make use of counterfeit reproductions of Plaintiffs' marks, *inter alia*, by causing the deceptive use of such marks in domain names and websites, and by causing consumers to engage with malicious phishing domains that bear the Microsoft trademarks. Fake ONNX Defendants' creation and use of counterfeit trademarks in connection with such fraud is likely to cause confusion and mistake and to deceive consumers. Fake ONNX Defendants also stole the name and logo belonging to the Open Neural Network Exchange, one of LF Projects' projects. *See* Dolan Decl. ¶¶ 6, 7, 10, 11. An online search of "ONNX" results in articles discussing Fake ONNX Defendants' malicious activities on the same results page as the work conducted by the Open Neural Network Exchange. Fake ONNX Defendants' creation and use of counterfeit LF Projects' trademarks in connection with its phishing operation is likely to cause confusion and mistake and to deceive the public.

This is a clear violation of the Lanham Act and Plaintiffs are likely to succeed on the merits. Indeed, "courts have almost unanimously presumed a likelihood of confusion upon a showing that the defendant intentionally copied the plaintiff's trademark *or* trade dress." *Larsen v. Terk Techs. Corp.*, 151 F.3d 140, 149 (4th Cir. 1998) (emphasis included).

In addition to constituting infringement under section 1114 of the Lanham Act, Fake ONNX 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).

Fake ONNX Defendants' misleading and false use of Microsoft's trademarks—including Azure®, Microsoft®, Microsoft 365®, Microsoft Defender®, Microsoft Exchange Server®, Microsoft Office®, Microsoft Sway®, Microsoft Teams®, MSN®, Office 365®, OneDrive®, Outlook®, SharePoint®, Windows®, and Windows Vista®, and LF Projects' ONNX trademarks – causes confusion and mistakes as to their affiliation with Fake ONNX 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 Garden & Gun, LLC v. TwoDalGals, LLC*, No. CIV 3:08CV349, 2008 WL 3925276, at *1 (W.D.N.C. Aug. 21, 2008) (granting preliminary injunction against misleading use of trademarks under Section 1125(a)); *Brookfield Commc'ns, Inc. v. W. Coast Entm't Corp.,* 174 F.3d 1036, 1065 (9th Cir. 1999) (entering preliminary injunction under Lanham Act §1125(a) for infringement of trademark in software and website code); *Hotmail Corp. v. Van$ Money Pie Inc.,* No. C 98-20064 JW, 1998 WL 388389, at *5 (N.D. Cal. Apr. 16, 1998) (granting preliminary injunction; copying the Hotmail trademarks in "e-mail return addresses" constituted false designation of origin; also constituted trademark "dilution" under §1125(c)). Thus, Plaintiffs are likely to succeed on the merits of their Lanham Act claims.

5. Fake ONNX Defendants' Conduct is Tortious

Fake ONNX Defendants' conduct is tortious under the common law doctrines of trespass

to chattels, conversion, and unjust enrichment. Under Virginia law, the tort of conversion "encompasses any wrongful exercise or assumption of authority . . . over another's goods, depriving him of their possession; and any act of dominion wrongfully exerted over property in denial of the owner's right, or inconsistent with it." *Microsoft Corp. v. Does 1-2,* No. 1:16CV993, 2017 WL 5163363, at *5 (E.D. Va. Aug. 1, 2017), *report and recommendation adopted*, No. 1:16-CV-00993 (GBL/TCB), 2017 WL 3605317 (E.D. Va. Aug. 22, 2017); *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—sometimes referred to as "the little brother of conversion"—applies where personal property of another is used without authorization, but the conversion is not complete. *Id.*; *see also Vines v. Branch*, 418 S.E.2d 890, 894 (1992). Here, Fake ONNX Defendants exercised dominion and authority over Microsoft's proprietary services like Outlook and Azure by intruding into its servers supporting those services and over Microsoft's proprietary systems in order to gain access to content stored on those servers like email and access to other applications on the Azure platform. These acts deprived Microsoft of its right to control the content, functionality, and nature of its software and services. District courts in the Fourth Circuit have recognized that computer hacking can amount to tortious conduct under the doctrines of conversion and trespass to chattels. *See supra*; *see also Microsoft Corp. v. Does 1-18*, No. 1:13CV139 LMB/TCB, 2014 WL 1338677, at *9 (E.D. Va. Apr. 2, 2014) ("The unauthorized intrusion into an individual's computer system through hacking, malware, or even unwanted communications supports actions under these claims"); *Microsoft Corp. v. John Does 1-8*, No. 1:14-CV-811, 2015 WL 4937441, at *12 (E.D. Va. Aug. 17, 2015).

Plaintiffs are likely to succeed on the merits of their unjust enrichment claim. Plaintiffs have demonstrated that that (1) Plaintiffs conferred a benefit on the Fake ONNX Defendants; (2) Defendants' knowledge of conferring the benefit; and, (3) Fake ONNX Defendants' acceptance or retention of the benefit under circumstances that "'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. The Fake ONNX 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. Lyons Decl. ¶¶ 56-62; Dolan Decl. ¶¶ 8-13. In order to ensure greater efficacy of their criminal operation, Fake ONNX Defendants usurp this goodwill. Moreover, once Fake ONNX Defendants complete a phishing attack and gain access to a victims' account, Fake ONNX Defendants are further unjustly enriched through the access they have obtained through ill-gotten means. It is inequitable for Fake ONNX Defendants to retain these benefits.

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

B. Fake ONNX Defendants Cause Irreparable Harm

It is well-settled that consumer confusion and injury to business goodwill constitute irreparable harm. *See MicroAire Surgical Instruments, LLC v. Arthrex, Inc.*, 726 F. Supp. 2d 604, 635 (W.D. Va. 2010) ("The loss of goodwill is a well-recognized basis for finding irreparable harm"); *Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.*, 22 F.3d 546 (4th Cir. 1994)), *abrogated on other grounds*, *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 24, 129 S. Ct. 365, 376, 172 L. Ed. 2d 249 (2008). A finding of irreparable harm usually follows a finding of unlawful use of a trademark and a likelihood of confusion. *Ledo Pizza Sys., Inc. v.*

Singh, No. CIV. WDQ-13-2365, 2013 WL 5604339, at *3 (D. Md. Oct. 10, 2013); *Nabisco Brands, Inc. v. Conusa Corp.*, 722 F. Supp. 1287, 1290 (M.D.N.C. 1989) ("In the context of a trademark infringement dispute, several courts have held that where likelihood of confusion is established likelihood of success on the merits as well as risk of irreparable harm follow.").

Here, Fake ONNX Defendants tarnish Microsoft's and LF Projects' valuable trademarks, injuring Plaintiffs' goodwill, creating confusion as to the source of Defendants' false messages, and damaging the reputation of and confidence in the services of Microsoft and LF Projects. *See supra*. These injuries are sufficient in and of themselves to constitute irreparable harm. In addition, Fake ONNX Defendants are causing monetary harm that is unlikely to ever be compensated—even after final judgment—because Fake ONNX Defendants are elusive cybercriminals whom Plaintiffs are unlikely to be able to enforce judgments against. "[C]ircumstances[] such as insolvency or unsatisfiability of a money judgment, can show irreparable harm." *Khepera-Bey v. Santander Consumer USA, Inc.*, No. CIV. WDQ-11-1269, 2013 WL 3199746, at *4 (D. Md. June 21, 2013); *accord Burns v. Dennis-Lambert Invs., Ltd. P'ship*, 2012 Bankr. LEXIS 1107, *9 (Bankr. M.D.N.C. Mar. 15, 2012) ("[A] preliminary injunction may be appropriate where 'damages may be unobtainable from the defendant because he may become insolvent before final judgment can be entered.'"); *Rudolph v. Beacon Indep. Living LLC*, No. 3:11-CR-00617-W, 2012 WL 181439, at *2 (W.D.N.C. Jan. 23, 2012) ("Irreparable harm exists here because of Defendant Beacon's continued occupancy of the Facility without paying any rents, particularly in light of the threat of insolvency by one or more Defendants.").

1. Irreparable Harm to Microsoft

To carry out its criminal operation, Fake ONNX Defendants use Microsoft based software and services. This is done intentionally to improperly leverage Microsoft's brandings, trademarks,

and reputation and to deceive victims into believing that Fake ONNX Defendants' malicious phishing attacks are associated or endorsed by Microsoft. Lyons Decl. ¶ 60. If a customer mistakenly believes that Microsoft endorses the cybercriminal behavior of Fake ONNX Defendants, Microsoft's reputation and goodwill is harmed beyond repair—indeed, in such circumstances the customer may be lost forever. *Id.* ¶ 62.

2. Irreparable Harm to LF Projects

In addition to causing irreparable harm to its phishing victims, Fake ONNX Defendants have also stolen their name and logo from LF Projects' ONNX Exchange. Dolan Decl. ¶¶ 6, 7. The "ONNX" name and logo are registered by LF Projects. *Id.* ¶ 5. ONNX Exchange and the ONNX-branded phishing kit share not only the same name, but also the same geometric shape as the logo. *Id.* ¶ 6. This causes significant confusion between Plaintiff LF Projects' ONNX Exchange and Fake ONNX Defendants' ONNX-branded phishing kits. *Id.* ¶¶ 9-11. The mere fact that Plaintiffs had to create artificial names to describe Plaintiff LF Projects' Open Neural Network Exchange project and Fake ONNX Defendants to distinguish the parties establishes the very real likelihood of confusion.

Fake ONNX Defendants irreparably harms LF Projects' goodwill by damaging its projects' reputation, brands, and partner goodwill. Fake ONNX Defendants' use of the "ONNX" trademark leads to confusion as to the malicious phishing activities perpetrated by Fake ONNX Defendants and may lead to attribution to the ONNX Exchange. *Id.*

Many major tech companies are actively involved in the community of the ONNX Exchange and malicious activities of wrongly attributed to the ONNX Exchange would potentially implicate the community of organizations, and the goodwill cultivated through their joint collaboration to advance work in the artificial intelligence space. Dolan Decl. ¶ 13.

C. Balance of Equities Strongly Favors Injunctive Relief

Because Defendants are engaged in an illegal scheme to defraud consumers and injure Plaintiffs, the balance of equities clearly tips in favor of granting an injunction. *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). On one side of the scales of equity rests the harm to Microsoft, its customers, LF Projects, its projects, and the public, caused by Fake ONNX Defendants, while on the other side, Fake ONNX Defendants can claim no legally cognizable harm because an injunction would only require Fake ONNX Defendants to cease illegal activities. *US Airways,* 13 F. Supp. 2d at 736.

D. Public Interest Favors Injunctive Relief

It is clear that an injunction would serve the public interest here. Every day that passes, Fake ONNX 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. Moreover, 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., BSN Med., Inc. v. Art Witkowski*, 2008 U.S. Dist. LEXIS 95338, at *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 WL 4829420 (W.D.N.C. Oct. 12, 2011) (similar); *Dish Network LLC v. Parsons,* 2012 U.S. Dist. LEXIS 75386, at **8-9 (W.D.N.C. May 30, 2012) (public interest weighed in favor of injunction to enforce ECPA); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, at *32 (E.D. Va. Jan. 6, 2014) (public interest weighed in favor of injunction to enforce CFAA).

Notably, numerous courts have granted requests for injunctive relief targeted at disabling malicious computer botnets, such as those enabled by the Fake ONNX Defendants.[1] *See Microsoft and NGO-ISAC v. John Does 1-2*, Case No. 1:24-cv-02719-RC (D.C. Sep. 24, 2024), (Contreras, R.); *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.). 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 Fake ONNX 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); *United States v. X,* 601 F. Supp. 1039, 1042 (D. Md. 1984) (All Writs Act permits the district court to order a third party to provide "nonburdensome technical assistance" in aid of valid warrant); *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) (same; 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'"); *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."); *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).

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 take 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 bring it 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.

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, Fake ONNX Defendants' technical sophistication and ability to move their malicious infrastructure if given advance notice of Plaintiffs' request for injunctive relief. 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 Fake ONNX Defendants will be able to quickly mount an alternate infrastructure and direct the vast majority of the phishing

operation to begin to operate through that alternate structure before the TRO can have any remedial effects. Lyons Decl. ¶¶ 69-72. 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 under circumstances such as the instant case, where notice would render the requested relief ineffective. *See, e.g., 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); *Little Tor Auto Ctr. v. Exxon Co., U.S.A.*, 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"); *Crosby v. Petromed, Inc.*, 2009 WL 2432322, at *2 (E.D. Wash. Aug. 6, 2009) (granting *ex parte* TRO as "notice to Defendants of this TRO request could result in further injury or damage to Plaintiffs...."). 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.

Here, there is specific evidence that the Fake ONNX Defendants will attempt to move the infrastructure if given notice, as the Fake ONNX Defendants have persistently changed infrastructure once it becomes known to the security community, in order to stay ahead of cybersecurity countermeasures. Lyons Decl. ¶¶ 71, 72. Accordingly, granting *ex parte* relief

without first providing notice is appropriate. Indeed, district courts have previously granted similar relief in cases brought by Microsoft to halt similarly situated cybercriminal operations.

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 Fake ONNX Defendants and to serve the complaint.

A. Plaintiffs Will Provide Notice to the Fake ONNX Defendants by Personal Delivery and Through Treaty if Possible

Plaintiffs have identified domains from which Fake ONNX Defendants' infrastructure operates, and, pursuant to the TRO, will obtain from the domain registrars/registries any and all physical addresses of Fake ONNX Defendants, to the extent those are available or not fictitious. Pursuant to Rules 4(e)(2)(A) and 4(f)(3), and if Plaintiffs are able to identify the physical addresses. 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, 15. If valid physical addresses of Fake ONNX John Doe Defendants can be identified outside of the Unitized States , Plaintiffs will notify the Fake ONNX Defendants and serve process upon them through the Hague Convention on service of process or similar treaty-based means. *Id.*

B. Plaintiffs Will Provide Notice to Fake ONNX Defendants by Email, Facsimile, and Mail

Plaintiffs have identified email addresses, mailing addresses and/or facsimile numbers provided by Fake ONNX Defendants, and will further identify such contact information pursuant to the terms of the requested TRO. *Id.* ¶ 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 Fake ONNX Defendants provided to the registrars and registries. *Id.* When Fake ONNX Defendants registered for domain names, they agreed not to engage in abuse such as that at issue in this case and agreed that notice of disputes regarding hosting could be provided to them by sending complaints to the email, facsimile and mail addresses provide by them. *Id.* ¶ 19, 20.

C. **Plaintiffs Will Provide Notice to Fake ONNX Defendants by Publication**:

Plaintiffs will notify Fake ONNX Defendants of the preliminary injunction hearing and the Complaint against their misconduct 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 Fake ONNX 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)); *FMAC Loan Receivables v. Dagra,* 228 F.R.D. 531, 535-36 (E.D. Va. 2005) (acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means); *BP Products N. Am., Inc. v Dagra*, 236 F.R.D. 270, 271-73 (E.D. Va. 2006) (approving notice by publication); *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 Fourth Circuit. See *FMAC Loan Receivables*, 228 F.R.D. at 534 (following *Rio); BP Products N. Am., Inc. v. Dagra*, 232 F.R.D. 263, 264 (E.D. Va. 2005) (same); *Williams v. Adver. Sex LLC,* 231 F.R.D. 483, 486 (N.D. W. Va. 2005) ("The Fourth Circuit Court of Appeals has not addressed this issue. Therefore, in the absence of any controlling authority in this circuit, the Court adopts the

reasoning of the Ninth Circuit in Rio Properties, Inc. . . .")

In this case, the e-mail addresses provided by Fake ONNX Defendants to the domain registrars, in the course of obtaining services that support Fake ONNX Defendants' operation, are likely to be the most accurate and viable contact information and means of notice and service. Poston Decl. ¶¶ 19-20. Moreover, Fake ONNX Defendants will expect notice regarding their use of the domain registrars' services to operate the phishing operation by those means, as Fake ONNX 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.[4]

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. Pro. 4(f)(3) satisfy due process and are reasonably calculated to notify Fake ONNX Defendants of this action.

VII. CONCLUSION

For the reasons set forth herein, Plaintiffs respectfully request that this Court grant the instant Motion for an Emergency *Ex Parte* Temporary Restraining Order and a Preliminary Injunction.

[4] Additionally, if the physical addressees provided by the Fake ONNX 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.").

Dated: November 12, 2024

Robbie Rogart Jost (VA Bar No. 84877)
David J. Ervin (VA Bar No. 34719)
Jeffrey L. Poston (*pro hac vice* forthcoming)
Garylene Javier (*pro hac vice* forthcoming)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington, DC 20004
T: 202-624-2500
F: 202-628-5116
RJost@crowell.com
DErvin@crowell.com
JPoston@crowell.com
GJavier@crowell.com

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

Counsel for Plaintiffs Microsoft Corporation and LF Projects LLC