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. 1:24-cv-2013 **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5**

***EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiffs Microsoft Corporation ("Microsoft") and LF Projects, LLC ("LF Projects") have filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962; (3) Conspiracy to Violate the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(d); (4) The Electronic Communications Privacy Act, 18 U.S.C. § 2701; (5) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (6) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 et seq.; (7) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); (8) common law trespass to chattels; (9) conversion; and (10) unjust enrichment. Plaintiffs have moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal

Rules of Civil Procedure, 15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act).

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiffs' *Ex Parte* Application for an Emergency Temporary Restraining Order and Order to Show Cause re Preliminary Injunction, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case, and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Abanoub Nady and John Does 1-4 ("Fake ONNX Defendants") under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962; (3) Conspiracy to Violate the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(d); (4) The Electronic Communications Privacy Act, 18 U.S.C. § 2701; (5) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (6) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.*; (7) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); (8) common law trespass to chattels; (9) conversion; and (10) unjust enrichment.

2. There is good cause to believe that Fake ONNX Defendants manufacture and sell illegal phishing kits deceptively branded as "ONNX" designed to steal sensitive information and perpetrate business email compromise, ransomware, and financial fraud against Microsoft customers.

3. There is good cause to believe that Fake ONNX Defendants target Microsoft's customers, including LF Projects, and the general public. Fake ONNX Defendants manufacture,

sell, and facilitate the deployment of pre-packaged sets of tools ("phishing kits") that enable other cybercriminals to launch phishing attacks with relative ease. 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."

4. There is good cause to believe that Fake ONNX Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962, 1962(d)), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), and constitute trespass to chattels, conversion, and unjust enrichment, and Plaintiffs, therefore, are likely to prevail on the merits of this action.

5. Microsoft owns the registered trademarks Microsoft®, Windows®, Microsoft 365®, Office365®, Office®, Microsoft Office®, SharePoint®, OneDrive®, Outlook®, Microsoft Exchange Server®, Teams®, Microsoft Defender®, Windows Vista®, Sway®, and Azure® and numerous other trademarks used in connection with its services, software and products.

6. 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 under LF Projects known as the Open Neural Network Exchange, or "ONNX."

7. There is good cause to believe that, unless Fake ONNX Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from Fake ONNX Defendants' ongoing violations. The evidence set forth in Plaintiffs' Memo in Support of *Ex Parte* Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary

Injunction ("TRO Application"), and the accompanying declarations of Jason Lyons, Michael Dolan, Jeffrey L. Poston, and supporting exhibits, demonstrates that Plaintiffs are likely to prevail on its claim that Fake ONNX Defendants have engaged in violations of the foregoing law by:

a. Intentionally accessing the protected computers and computer networks of Microsoft and the customers of Microsoft, without authorization or exceeding authorization, in order to steal and exfiltrate information from those computers and computer networks;

b. Engaging in phishing operations to steal credentials from unsuspecting victims who are tricked into believing they are accessing legitimate websites;

c. Developing mechanisms to circumvent technological security protocols;

d. Intentionally accessing, without authorization, the email inboxes of Microsoft customers, to support credentials theft, information exfiltration, and subsequent end-user terminal attacks which include business email compromise, ransomware, and financial fraud;

e. Operating a Racketeering Enterprise by leveraging each other's work to: (i) create, distribute, and operate the phishing technical infrastructure, (ii) sell, distribute, and use ONNX-branded phishing kits, (iii) to steal credentials from victims, and (iv) gain access to victim computers to further additional criminal activities like financial fraud, business email compromise, and deploying ransomware.

f. Infringing the protected marks of Plaintiffs for the purpose of causing confusion or mistake, whereby the victims of Fake ONNX Defendants' attacks mistakenly associate such conduct with Plaintiffs.

8. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, Microsoft's customers, LF Projects, and the public. There is good cause to believe that Fake ONNX Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court.

9. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, distribution, deployment, or use of the ONNX-branded phishing kits by Fake ONNX Defendants that is hosted at and otherwise operates through the Internet domains listed in **Appendix A** to this Order, and from the

destruction or concealment of other discoverable evidence of Fake ONNX Defendants' misconduct available via those domains, including on victims targeted by Fake ONNX Defendants, if they receive advance notice of this action. Based on the evidence cited in Plaintiffs' TRO Application and accompanying declarations and exhibits, Plaintiffs are likely to be able to prove that:

a. Fake ONNX Defendants are engaged in activities that directly violate United States law and harm Microsoft, its customers, LF Projects, and the public;

b. Fake ONNX Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;

c. Fake ONNX Defendants are likely to delete or to relocate Internet infrastructure in Plaintiffs' TRO Application and the harmful and malicious phishing kits disseminated through the Internet domains listed in **Appendix A**, thereby permitting them to continue their illegal acts; and

d. Fake ONNX Defendants are likely to warn their associates engaged in such activities if informed of Plaintiffs' action.

10. Plaintiffs' request for this emergency *ex parte* relief is not the result of any lack of diligence on Plaintiffs' part, but instead, is based upon the nature of Fake ONNX Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be **GRANTED** without prior notice to Fake ONNX Defendants, and accordingly, Plaintiffs are relieved of the duty to provide Fake ONNX Defendants with prior notice of Plaintiffs' motion and requested relief.

11. There is good cause to believe that Fake ONNX Defendants have operated their phishing operations through certain instrumentalities – specifically through the website domains identified in **Appendix A**.

12. There is good cause to believe that Fake ONNX Defendants have (i) engaged in illegal activity by using the domain registration facilities of the domain registries identified in

Appendix A, to register the Internet domains identified in **Appendix A**, (ii) violated Plaintiffs' trademarks in order to: (iii) deceive Plaintiffs' customers to steal credentials for their email accounts, infiltrate the email systems, and have unfettered access to the contents of those email accounts for purposes of data exfiltration.

13. There is good cause to believe that Fake ONNX Defendants have engaged in illegal activity by using deceptive and fraudulent methods to steal computer users' account credentials and to use such credentials for illegal purposes.

14. There is good cause to believe that to immediately halt the injury caused by Fake ONNX Defendants, they must be prohibited from accessing Plaintiffs' services without authorization, prohibited from the unlawful intrusion and data theft of the victims' email accounts, from using Plaintiffs' marks to perpetrate their unlawful and criminal scheme, and prevented from using the Internet domains identified in **Appendix A** to operate the Internet infrastructure to further its phishing operation.

15. There is good cause to believe that Fake ONNX Defendants have engaged in illegal activity using the Internet domains identified in **Appendix A** to carry out their illegal phishing campaign. There is good cause to believe that to immediately halt the injury caused by Fake ONNX Defendants, each of Fake ONNX Defendants' domains set forth in **Appendix A** must be immediately transferred beyond the control of Fake ONNX Defendants' criminal operation, thus making them inaccessible to Fake ONNX Defendants.

16. There is good cause to believe that to immediately halt the injury, the execution of this Order should be carried out in a coordinated manner by Plaintiffs and by the domain registries identified in **Appendix A** on such date and time within five (5) days of this Order as may be reasonably requested by Plaintiffs.

17. There is good cause to believe that Fake ONNX Defendants have specifically directed their activities to Eastern District of Virginia.

18. There is good cause to believe that if Fake ONNX Defendants are provided advance notice of Plaintiffs' TRO Application or this Order, they would move Fake ONNX Defendants' infrastructure, allowing them to continue their misconduct and that they would destroy, move, hide, conceal, or otherwise make inaccessible to the Court evidence of their misconduct, Fake ONNX Defendants' infrastructure's activity, the infringing materials, the instrumentalities used to make the infringing materials, and the records evidencing the manufacture and distributing of the infringing materials.

19. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Fake ONNX Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Fake ONNX Defendants to Fake ONNX Defendants' domain registrars and hosting companies and as agreed to by Fake ONNX Defendants in their domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Fake ONNX Defendants, to the extent Fake ONNX Defendants provided accurate contact information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Fake ONNX Defendants, to the extent Fake ONNX Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

20. There is good cause to believe that Fake ONNX Defendants have no legitimate interest in carryout their cybercriminal activities.

21. There is good cause to believe that the harm to Plaintiffs in denying the relief requested in their TRO Application outweighs any harm to any legitimate interest of Fake ONNX Defendants (of which there is none) and that there is no undue burden to any third party.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED that, Fake ONNX Defendants, their representatives, and persons who are in active concert or participation with Fake ONNX Defendants and associated criminal operation, are temporarily restrained and enjoined from: (1) intentionally accessing the protected computers without authorization, (2) engaging in phishing campaigns, (3) stealing credentials from victims of phishing campaigns, (4) using the credentials to access the email inboxes of victims, (4) unlawfully accessing, viewing, exfiltrating, or otherwise stealing the contents of the compromised email inboxes, (5) capitalizing on the trademarks of Plaintiffs to fabricate legitimacy of the phishing campaign, (6) misappropriating that which rightfully belongs to Microsoft, its customers, or in which Microsoft or its customers have a proprietary interest; (7) destroying the goodwill and reputation of Plaintiffs, (8) impersonating Plaintiffs, their systems, products, and services, (9) configuring, deploying, operating, or otherwise participating in or facilitating infrastructure described in the TRO Application, including but not limited to the Internet domains set forth in **Appendix A** and through any other component or element of Fake ONNX Defendants' illegal infrastructure at any location, including infrastructure Fake ONNX Defendants may attempt to rebuild, and (10) undertaking any similar activity that inflicts harm on Microsoft, Microsoft's customers, LF Projects, or the public.

IT IS FURTHER ORDERED that, Fake ONNX Defendants, their representatives, and

persons who are in active concert or participation with Fake ONNX Defendants and associated criminal operation are temporarily restrained and enjoined from (1) using and infringing Plaintiffs' trademarks, including specifically Microsoft's registered trademarks Microsoft®, Windows®, Microsoft 365®, Office365®, Office®, Microsoft Office®, SharePoint®, OneDrive®, Outlook®, Microsoft Exchange Server®, Teams®, Microsoft Defender®, Windows Vista®, Sway®, and Azure®, and the trademarks of LF Projects, and its projects, including specifically the Open Neural Network Exchange's registered trademarks and its logo, and/or other trademarks, trade names, service marks, or Internet domain addresses or names containing or infringing such trademarks, trade names or service marks, as set forth in **Appendix B and C** to this Order; (2) using in connection with Fake ONNX Defendants' activities, products, or services any false or deceptive designation, representation or description of Fake ONNX Defendants or of their activities, whether by symbols, words, designs or statements, which would damage or injure Plaintiffs or give Fake ONNX Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that Fake ONNX Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Plaintiffs, or passing off Fake ONNX Defendants' activities, products or services as Plaintiffs'.

IT IS FURTHER ORDERED that, with respect to any currently registered Internet domains set forth in **Appendix A** to this Order, the domain registries located in the United States shall take the following actions:

A. Within **five (5) business days** of receipt of this Order, shall unlock and change the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. To the extent the registrar of record does not assist in changing the registrar of record for the domain under its control, the domain registry for the domain, or its administrators, including

backend registry operators or administrators, within five (5) business days of receipt of this Order, shall change, or assist in changing, the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. The purpose of this paragraph is to ensure that Microsoft has control over the hosting and administration of the domain in its registrar account at MarkMonitor or such other registrar specified by Microsoft. Microsoft shall provide to the domain registry or registrar of record any requested information or account details necessary to effectuate the foregoing.

B. The domain registries shall be made active and shall resolve in the manner set forth in this order, or as otherwise specified by Microsoft, upon taking control of the domain.

C. The domain registries shall take reasonable steps to work with Microsoft to ensure the transfer of the domain and to ensure that Fake ONNX Defendants cannot use it to make unauthorized access to computers, infect computers, compromise computers and computer networks, monitor the owners and users of computers and computer networks, steal information from them, or engage in any other activities prohibited by this Order;

D. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following, or other information as may be specified by Microsoft:

Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
United States
Phone: +1.4258828080
Facsimile: +1.4259367329
domains@microsoft.com

E. Prevent transfer, modification or deletion of the domain by Fake ONNX Defendants and prevent transfer or control of the domain to the account of any party other than

Microsoft;

F. Take all steps required to propagate to the foregoing changes through the Domain Name System ("DNS"), including domain registrars.

2. With regard to the domain registries and registrars located outside of the United States, the Court respectfully requests, but does not order, that they take the same or substantially similar actions as the foregoing so as to neutralize the threat posed by Fake ONNX Defendants to the citizens of all countries, including their own. Fake ONNX Defendants, their representatives and persons who are in active concert or participation with them are ordered to consent to whatever actions are necessary for non-United States registries, registrars and registrants or hosts, set forth in **Appendix A** to this Order, to effectuate this request.

IT IS FURTHER ORDERED that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Fake ONNX Defendants to their domain registrars and/or hosting companies and as agreed to by Fake ONNX Defendants in the domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Fake ONNX Defendants provided accurate contact information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Fake ONNX Defendants, to the extent they provided accurate contact information in foreign countries that are signatories to such treaties.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that Fake ONNX Defendants shall appear before this Court on December 4, 2024 at 1:00 p.m., to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling

on the Complaint against Fake ONNX Defendants, enjoining Fake ONNX Defendants from the conduct temporarily restrained by the preceding provisions of this Order. Due to the Thanksgiving holiday and this Court's schedule, this order shall remain in place until that date.

IT IS FURTHER ORDERED that Microsoft, on behalf of Plaintiffs, shall post bond in the amount of $50,000 to be paid into the Court registry.

IT IS FURTHER ORDERED that Fake ONNX Defendants shall file with the Court and serve on Plaintiffs' any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than two (2) days prior to the hearing on Plaintiffs' request for a preliminary injunction. Plaintiffs may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for Fake ONNX Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Eastern Standard Time) on the appropriate dates listed in this paragraph.

IT IS SO ORDERED

Entered this 13 day of November, 2024

UNITED STATES DISTRICT JUDGE
ED VA