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**

DECLARATION OF JEFFREY L. POSTON IN SUPPORT OF PLAINTIFFS' *EX PARTE* APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Jeffrey L. Poston, hereby declare and state as follows:

1. I am a partner at the law firm of Crowell & Moring LLP ("Crowell"), and counsel of record, for Plaintiffs Microsoft Corporation ("Microsoft") and LF Projects. I make this declaration in support of Plaintiffs' Application for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"). I make this declaration of my own personal knowledge and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

I. PARTIES

2. Microsoft and LF Projects seek an Emergency *Ex Parte* Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction designed to disrupt the technical

infrastructure employed by Abanoud Nady and John Does 1-4 (collectively "Fake ONNX Defendants" and formerly known as "Caffeine"), who 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. ("Defendants"). Fake ONNX Defendants develop, advertise, purchase, and implement phishing kits that are designed to infiltrate Microsoft systems; these phishing kits are advertised based on this capability. These phishing kits include email templates, fake website templates, domain registration services, customer support features designed to evade detection and lead victims to believe they are dealing with legitimate products. The kits are essentially "how to" manuals for cybercriminals to develop and execute attacks on email systems through phishing campaigns. To manage and direct this illegal activity, these Defendants have established and operate an infrastructure of websites and domains, which they use to target their victims, compromise their online accounts, compromise the security of their networks, and steal sensitive information from them. The Fake ONNX Defendants' criminal acts cause irreparable harm to Microsoft, its customers, LF Projects, and the public.

3. As counsel of record for Plaintiffs, I am aware of previous efforts brought by Microsoft to disable other types of unlawful, cybercriminal activities, including the "**Waledac**" Botnet in February 2010 in the Eastern District of Virginia, the "**Rustock**" Botnet in March 2011 in the Western District of Washington, the "**Kelihos**" Botnet in September 2011 in the Eastern District of Virginia, the "**Zeus**" Botnets in March 2012 in the Eastern District of New York, the "**Bamital**" Botnet in February 2013 in the Eastern District of Virginia, the "**Citadel**" Botnets in May 2013 in the Western District of North Carolina, the "**ZeroAccess**" Botnet in November 2013 in the Western District of Texas, the "**Shylock**" Botnet in June 2014

in the Eastern District of Virginia, the "**Ramnit**" Botnet in February 2015 in the Eastern District of Virginia, the "**Dorkbot**" Botnet in November 2015 in the Eastern District of New York; the "**Strontium**" threat infrastructure in August 2016 in the Eastern District of Virginia; the "**Phosphorous**" threat infrastructure in March 2019 in the District of Columbia; the "**Thallium"** threat infrastructure in December 2019 in the Eastern District of Virginia; "**Trickbot**" threat infrastructure in October 2020 in the Eastern District of Virginia; the "**ZLoader**" malware operation in April 2022 in the Northern District of Georgia; the "**Bohrium**" threat infrastructure in May 2022 in the Eastern District of Virginia; the "**Cracked Cobalt Strike**" cybercriminal and malware operation in March 2023 in the Eastern District of New York; and the "**Star Blizzard**" spear phishing operation in September 2024 in the District of Columbia.

4. Based on our previous experience with similar cybercriminal defendants that conduct their operations using an infrastructure consisting of a set of websites and domains, *ex parte* relief is necessary, as notice to the Fake ONNX Defendants would allow them to destroy the evidence of their illicit activity and give them an opportunity to move the instrumentalities they use to conduct their unlawful activity. This would render the further prosecution of this matter futile.

5. Indeed, in circumstances where similarly situated cybercriminals and threat groups have learned of Microsoft's attempts to disable the cybercriminal operation, they have attempted to migrate the infrastructure or activate new domains to prevent their technical infrastructure from being taken down and seized. This has happened both when Microsoft previously brought a takedown against Rustock Botnet, Dorkbot Botnet, and ZeroAccess Botnet. Based on our knowledge of prior similar experiences, we conclude that there is a

similar risk that the Fake ONNX Defendants would take similar evasive action here if they were made aware of the attempts to takedown their technical infrastructure before the takedown was complete.

6. Plaintiffs' counsel has not attempted to provide notice of the TRO Application to the Fake ONNX Defendants, and should not be required to provide notice at this time. We respectfully submit that good and sufficient reasons exist for this TRO Application to be made by Order to Show Cause in lieu of by notice of motion. Microsoft has previously sought and obtained *ex parte* temporary restraining orders against other cybercriminal groups in United States District Courts in *Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-00156 (E.D. Va. 2010) (Brinkema, J.); *Microsoft v. John Does, 1-11,* Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.); *Microsoft Corporation v. Dominique Piatti et al.*, Case No. 1:11-cv-01017 (E.D. Va., 2011) (Cacheris, J.); *Microsoft Corporation et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.); *Microsoft Corporation v. Peng Yong et al.,* Case No. 1:12-cv-1005 (E.D. Va. 2012) (Lee, J.); *Microsoft Corp. v. John Does 1-18 et al.*, Case No. 1:13-cv-139 (E.D. Va. 2013) (Brinkema, J.); *Microsoft v. John Does 1-82*, Case No. 3:13-CV-00319 (W.D. N.C. 2013) (Mullen, J.); *Microsoft v. John Does 1-8*, Case No. A-13-CV-1014 (Sparks, J.) (W.D. Tex 2013); *Microsoft v. John Does 1-8,* Case No. 1:14-cv-811 (O'Grady, J.) (E.D. Va. 2014); *Microsoft v. John Does 1-3,* Case No. 1:15-cv-240 (Brinkema, J.) (E.D. Va. 2015); *Microsoft v. John Does 1-5,* 1:15-cv-06565 (E.D.N.Y. 2015); *Microsoft Corporation v. John Does 1-2,* Case No. 1:16-cv-993 (E.D. Va. 2016) (Lee, J.); *Microsoft Corporation v. John Does 1-2*, Case No. 1:19-cv-00716 (D.C. 2019) (Berman-Jackson, J.); *Microsoft Corporation v. John Does 1-2,* Case No. 1:19-cv-01582 (E.D. Va. 2019) (O'Grady, J.); *Microsoft Corporation and FS-ISAC, Inc. v. John Does 1-2,* Case No. 1:20-cv-1171 (E.D.

Va. 2020) (Trenga, J.); *Microsoft Corporation, FS-ISAC, and Health-ISAC v. Malikov et al.*, Case No. 1:22-cv-1328 (N. D. Ga. 2022) (Cohen, J.); *Microsoft Corporation v. John Does 1-2*, Case No: 122-cv-607 (E.D. Va. 2022) (Trenga, J.); *Microsoft Corporation, Fortra LLC, and Health-ISAC v. John Does 1-16*, Case No. 23-cv-2447 (E.D.N.Y 2023) (DeArcy Hall, J.); and *Microsoft Corporation and NGO-ISAC v. John Does 1-2*, Case No. 24-cv-02719 (D.D.C. 2024) (Contreras, J.).

7. Plaintiffs have identified certain Internet domains as part of the infrastructure of the Fake ONNX Defendants. The domains associated with the Fake ONNX Defendants' infrastructure and the contact information for registrants of those domains are set forth in **Appendix A** to the Complaint. A true and correct copy of **Appendix A** to the Complaint is attached hereto as **Exhibit 1**.

8. Investigators in Microsoft's Digital Crimes Unit, including Jason Lyons who has provided a declaration in support of Plaintiffs' TRO Application, have worked to determine the true identities of the Fake ONNX Defendants. With respect to both Abanoud Nady and John Doe Defendants 1-4, who are also associated with the Fake ONNX criminal operation, the only publicly available contact information or identifying information associated with the Fake ONNX Defendants are the email addresses they used to register the domains that form the Fake ONNX technical infrastructure.[1] Based on our prior experience, it is likely that other contact information has been provided by the Fake ONNX Defendants to the Internet domain name registrars during the domain name registration and maintenance process, including, for example, individual and entity names, physical addresses, facsimile

[1] For Abanoud Nady, DCU Investigators were able to identify additional email addresses that are associates with Nady and his online persona, MRxC0DER.

numbers, telephone numbers, or payment information are fictitious.

9. Based on our experience, the email addresses provided to the domain registrars are most likely to be the most accurate contact information. This is because while the name, physical address, or phone numbers provided by the Fake ONNX Defendants may be purposefully false to obfuscate their identities, the Fake ONNX Defendants are more likely to use real emails address in connection with the registration efforts. When registrants set up website domains and associated infrastructure they must receive confirmation from the Internet domain registrars via email in order to utilize and access the Internet domains. In past experience relating to botnets, we have observed that the name, physical address, or telephone number were determined to be fraudulent or stolen, but the email address provided by defendants was, in fact, associated with them. Further supporting this conclusion, in May 2010, the Internet Corporation for Assigned Names and Numbers ("ICANN")—an organization that administers the domain name system—issued a study indicating the ease with which name and physical mailing addresses for domain registrations may be falsified. Attached hereto as **Exhibit 2** is a true and correct copy of the ICANN's May 2010 study, "WHOIS Proxy/Privacy Service Abuse – Definition."

10. Based on our prior experience and from Plaintiffs' research, I believe that the most reliable contact information for effectuating communication with the Fake ONNX Defendants are the email addresses that have been discovered to be associated with the Fake ONNX Defendants domains, and the contact information, particularly email addresses, in possession of the Internet domain registrars. Based on our research, we conclude that such contact information is likely to be valid, as it is necessary to obtain Internet domain names or web hosting service. Upon provision of such contact information by the Internet domain

registrars and web hosting companies to Plaintiffs, notice of this proceeding and service of process may be attempted using such contact information. Through our research, we have not discovered any other information that would enable, at this point, further identification of or contact with Fake ONNX Defendants other than that in the possession of these companies. We believe that absent an order directing Doe discovery, these companies will be unlikely to share contact information necessary to provide notice and service to the Fake ONNX Defendants.

II. NOTICE AND SERVICE OF PROCESS

A. Plaintiffs Have Robust Plans To Provide Notice

11. On behalf of Plaintiffs, once the TRO has been issued and the domains have been transferred to Microsoft, Crowell will attempt notice of any preliminary injunction hearing, as well as service of the Complaint by sending the pleadings and/or links to the pleadings to e-mail addresses, facsimile numbers and mailing addresses associated with the Fake ONNX Defendants or otherwise provided by the Fake ONNX Defendants to the domain registrars.

12. On behalf of Plaintiffs, once the TRO has been issued and the domains have been transferred to Microsoft, Crowell will attempt notice of any preliminary injunction hearing and service of the Complaint by publishing those pleadings on a publicly accessible website located at: www.noticeofpleadings.com/fakeonnx. Crowell will publish such notice on the website for the duration of this litigation. The following information will be made available on the website:

a. The information contained in the case caption and the content of the summons.

b. The following summary statement of the object of the complaint and the demand for relief: "Plaintiffs Microsoft Corporation ("Microsoft") and LF

Projects have sued Defendants Abanoud Nady and John Does 1-4 associated with the Fake ONNX cybercriminal operation and domains listed in the documents set forth herein. Plaintiffs allege that the Fake ONNX Defendants have violated Federal and state law by hosting a cybercriminal operation through these domains and selling, distributing, purchasing, and implementing the "ONNX"-branded phishing kits that support a Phishing-as-a-Service enterprise. The phishing kits mad and sold by the Fake ONNX Defendants facilitate sophisticated spear phishing and are designed to steal sensitive information that is then used to perpetrate additional cybercrimes including business email compromise, financial fraud, and ransomware attacks. Fake ONNX Defendants have also committed intellectual property violations irreparably harming Plaintiffs and Plaintiffs' customers and member organizations. Plaintiffs seek a preliminary injunction directing the registrars associated with these domains to take all steps necessary to disable access to and operation of these domains and that all content and material associated with these domains are to be isolated and preserved pending resolution of the dispute. Plaintiffs seek a permanent injunction, other equitable relief and damages. Full copies of the pleading documents are available at www.noticeofpleadings.com/fakeonnx.

c. The date of first publication.

d. The following text: "NOTICE TO DEFENDANT: READ THESE PAPERS CAREFULLY! You must "appear" in this case or the other side will win automatically. To "appear" you must file with the court a legal document called a "motion" or "answer." The "motion" or "answer" must be given to the court clerk or administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on the Plaintiffs' attorneys, Jeffrey L. Poston at Crowell & Moring LLP, 1001 Pennsylvania Avenue NW, Washington D.C. 20004, jposton@crowell.com. If you have questions, you should consult with your own attorney immediately."

13. On behalf of Plaintiffs, Crowell will serve each of the Internet domain registries listed at **Appendix A** to the Complaint with all copies of all documents served on the Fake ONNX Defendants.

14. To the extent that Plaintiffs are able to determine that any of the Fake ONNX Defendants has a physical address in the United States, Crowell will also attempt notice of any preliminary injunction hearing, as well as service of the complaint by personal delivery on such Fake ONNX Defendant at their physical address in the United States.

15. To the extent the identity of the Fake ONNX John Doe Defendants become known to Plaintiffs, Crowell will prepare Requests for Service Abroad of Judicial or Extrajudicial Documents to attempt notice of any TRO and preliminary injunction hearing, as well as service of the Complaint on any Fake ONNX Defendants in this case that have provided contact information in foreign countries that are signatories to the Hague Convention on Service Abroad or any similar treaty, and will comply with the requirements of those treaties. Upon entry of any TRO, Crowell will execute and deliver these documents to the appropriate Central Authority and request, pursuant to the Hague Convention or similar treaty, that the Central Authority deliver these documents to the contact information provided by the Fake ONNX Defendants. I am informed, and therefore believe, that notice of the preliminary injunction hearing and service of the Complaint could take approximately three to six months or longer through this process.

B. Notice Under ICANN Domain Name Registration Policies

16. Attached hereto as **Exhibit 3** is a true and correct copy of a document describing ICANN's role. Exhibit 3 reflects the following: ICANN is a not-for-profit partnership formed in 1998. ICANN coordinates domain names and IP addresses (unique identifying numbers for computers throughout the world), which enables the operation of the global Internet. ICANN's responsibilities include running an accreditation system for domain name "registrars." Domain name registrars enter into arrangements with individual "registrants" who wish to register particular domain names. ICANN has a contractual relationship with all accredited registrars that sets forth the registrars' obligations. The purpose of the requirements of ICANN's accreditation agreements with registrars is to provide a consistent and stable environment for the domain name system, and hence the Internet.

17. A true and correct copy of the 2013 ICANN Registrar Accreditation Agreement between ICANN and domain name registrars is attached hereto as **Exhibit 4**.

18. The following summarizes provisions set forth in the ICANN accreditation agreements with registrars at Exhibit 4.

ICANN Requires That Registrants Agree To Provide Accurate Contact Information

19. Section 3.7.7.1 of the accreditation agreement provides that domain registrants will provide the registrar accurate and reliable contact information. In particular, the domain name registrant:

> "shall provide to Registrar accurate and reliable contact details and correct and update them within seven (7) days of any change during the term of the Registered Name registration, including: the full name, postal address, e-mail address, voice telephone number, and fax number if available of the Registered Name Holder; name of authorized person for contact purposes in the case of an Registered Name Holder that is an organization, association, or corporation…."

20. Section 3.7.7.2 of the accreditation agreement provides that if the registrant fails to respond for over 15 days to a registrar's inquiry about inaccurate contact information, the domain may be cancelled. In particular, the domain name registrant's:

> "willful provision of inaccurate or unreliable information, its willful failure to update information provided to Registrar within seven (7) days of any change, or its failure to respond for over fifteen (15) days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for suspension and/or cancellation of the Registered Name registration."

ICANN Requires That Registrants Agree To A Dispute Resolution Policy Under Which Notice Is Given By Sending The Complaint To The Registrant's Contact Information

21. Section 3.8 of the accreditation agreement provides that registrars shall require registrants to agree to the Uniform Domain Name Dispute Resolution Policy ("UDRP"). The UDRP is a policy between a registrar and its customer and is included in registration agreements

for all ICANN-accredited registrars. Attached hereto as **Exhibit 5** is a true and correct copy of the UDRP.

22. As part of the registrant's agreement to the UDRP, the registrant agrees to the Rules for Uniform Domain Name Dispute Resolution Policy ("Rules"). Attached hereto as **Exhibit 6** is a true and correct copy of the Rules.

23. Pursuant to the Rules, "Written Notice" of a complaint regarding a domain requires electronic transmittal of the complaint to a domain registrant and hardcopy notification that the complaint was sent by electronic means. In particular, "Written Notice" is defined as:

> "hardcopy notification by the Provider to the Respondent of the commencement of an administrative proceeding under the Policy which shall inform the respondent that a complaint has been filed against it, and which shall state that the Provider has electronically transmitted the complaint including any annexes to the Respondent by the means specified herein. Written notice does not include a hardcopy of the complaint itself or any annexes."

24. Pursuant to the Rules, notice of a complaint may be achieved by the registrar forwarding the complaint to the postal address, facsimile number and e-mail addresses of the domain registrant. In particular, the Rules define the procedure for providing notice as follows:

> "(a) When forwarding a complaint, including any annexes, electronically to the Respondent, it shall be the Provider's responsibility to employ reasonably available means calculated to achieve actual notice to Respondent. Achieving actual notice, or employing the following measures to do so, shall discharge this responsibility:
>
> (i) sending Written Notice of the complaint to all postal-mail and facsimile addresses (A) shown in the domain name's registration data in Registrar's Whois database for the registered domain-name holder, the technical contact, and the administrative contact and (B) supplied by Registrar to the Provider for the registration's billing contact; and
>
> (ii) sending the complaint, including any annexes, in electronic form by e-mail to:

(A) the e-mail addresses for those technical, administrative and billing contacts;

(B) postmaster@<the contested domain name>; and

(C) if the domain name (or "www." followed by the domain name) resolves to an active web page other than a generic page the Provider concludes is maintained by a registrar or ISP for parking domain-names registered by multiple domain-name holders), any e-mail address shown or e-mail links on that web page; and

(iii) sending the complaint, including any annexes, to any e-mail address the Respondent has notified the Provider it prefers and, to the extent practicable, to all other e-mail addresses provided to the Provider by Complainant..."

25. The effect of the UDRP and the Rules is that domain name registrants agree that notice of a complaint relating to their domains may be provided by the foregoing means, including by sending the complaint to postal, facsimile and email addresses provided by registrants.

ICANN Requires That Registrants Agree That Domains May Be Suspended Or Cancelled Pursuant To The Dispute Resolution Policy

26. Section 3.7.7.11 of the accreditation agreement provides that registrars shall require that a domain name registrant "shall agree that its registration of the Registered Name shall be subject to suspension, cancellation, or transfer" pursuant to ICANN's policies for the resolution of disputes concerning domain names.

ICANN Requires That Registrants Agree Not To Use Domains In An Illegal Manner

27. Under Section 2 of the UDRP, the domain registrant agrees that:

"By applying to register a domain name, or by asking us to maintain or renew a domain name registration, you hereby represent and warrant to us that (a) the statements that you made in your Registration Agreement are complete and accurate; (b) to your knowledge, the registration of the domain name will not infringe upon or otherwise violate the rights of any third party; (c) you are not registering the domain for an unlawful purpose; and (d) you will not knowingly use the domain name in violation of any applicable

> laws or regulations. It is your responsibility to determine whether your domain name registration infringes or violates someone else's rights."

28. Similarly, Section 3.7.7.9 of the accreditation agreement provides that the domain name registrant "shall represent that, to the best of the Registered Name Holder's knowledge and belief, neither the registration of the Registered Name nor the manner in which it is directly or indirectly used infringes the legal rights of any third party."

The Fake ONNX Defendants' Internet Domain Registrars Send Account-Related Information To Customer-Provided Contacts

29. The terms of service for Internet domain registrars used by the Fake ONNX Defendants provide that their customers must provide contact information, including the email address, postal address, and a valid telephone number where they can reach their customers. These Internet domain registrars further provide that they may contact their respective customers based on the information provided by that customer. In particular, NameSilo, LLC's ("NameSilo") General Terms and Conditions, available at https://www.namesilo.com/Support/General-Terms-and-Conditions, include such provisions. Similarly, Key-Systems GmbH's ("Key-Systems") Registration Agreement, available at https://www.key-systems.net/en/registration-agreement, also includes such provisions. A true and correct copy of each NameSilo's General Terms and Conditions and Key-Systems' Registration Agreement are attached hereto as **Exhibit 7**.

30. Based on our past experience and our research of third parties that the Fake ONNX Defendants use to provide domain name services, the other third party Internet domain name registrars require that similar contact information be provided.

The Fake ONNX Defendants' Internet Domain Name Registrars' Terms Of Service Prohibit Customers From Using Services In An Illegal Manner

31. The Internet domain registrars' terms of service prohibit customers, including

the Fake ONNX Defendants, from using the services in an illegal manner, and customer accounts may be terminated for violation of those terms. For example, NameSilo's agreement prohibits, among other conduct, the registered domain being used to:

e. registration of prohibited domain name(s),

f. abuse of NameSilo's services,

g. payment irregularities,

h. illegal conduct,

i. failure to keep account or WHOIS information accurate and up to date,

j. failure to respond to inquiries from NameSilo for over three (3) calendar days,

k. if use of NameSilo's services involves NameSilo in a violation of any third party's rights or acceptable use policies, including but not limited to the transmission of unsolicited email, the violation of any copyright, or the distribution of any form of malware (defined to include, without limitation, malicious code or software that might affect the operation of the Internet),

l. to comply with any applicable court orders, laws, government rules or requirements, requests of law enforcement or other governmental agency or organization, or any dispute resolution process,

m. to avoid any liability, civil or criminal, on the part of NameSilo, as, well as its affiliates, subsidiaries, officers, directors, and employees,

n. to protect the integrity, security and stability of the Domain Name system (DNS), or

o. failure to respond to inquiries from NameSilo regarding payment inquiries for over 24 hours

32. NameSilo's policies also provide that it may suspend or terminate its customer's services if that customer has been found to engage in prohibited conduct. Based on our past experience and our current research of other Internet domain registrars, and on information and belief, the other Internet domain registrars used by the Fake ONNX Defendants prohibit similar unlawful conduct.

III. OTHER AUTHORITY AND EVIDENCE

33. The requested *ex parte* relief Plaintiffs seek has been granted against similarly situated cybercriminal organizations in the past. Additionally, Plaintiffs' proposed alternative service has previously been granted in other actions brought by Microsoft to halt other cybercriminal organizations that, like the Fake ONNX Defendants, carryout their unlawful activity through the use of a technical infrastructure using Internet domains.

34. Attached hereto as **Exhibit 8** is a true and correct copy of the March 15, 2019 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft v. John Does 1-2*, Case No. 1:19-cv-00716-ABJ (D.C. 2019) (Berman-Jackson, J.).

35. Attached hereto as **Exhibit 9** is a true and correct copy of the December 18, 2019 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft v. John Does 1-2,* Case No. 1:19-cv-01582 (E.D. Va. 2019) (O'Grady, J.).

36. Attached hereto as **Exhibit 10** is a true and correct copy of the May 1, 2020 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Sophos v. John Does 1*-2, Case No. 1:20-cv-00502 (E.D. Va. 2020) (O'Grady, J.).

37. Attached hereto as **Exhibit 11** is a true and correct copy of the July 1, 2020 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft v. John Does 1-2,* Case No. 1:20-cv-00730 (E.D. Va. 2020) (O'Grady, J.).

38. Attached hereto as **Exhibit 12** is a true and correct copy of the July 22, 2020 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *DXC Technology Company v. John Does 1-2,* Case No. 1:20-cv-00814 (E.D. Va. 2020) (Alston, J.).

39. Attached hereto as **Exhibit 13** is a true and correct copy of the October 6, 2020 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft*

and FS-ISAC v. John Does 1-2, Case No. 1:20-cv-1171 (E.D. Va. 2020) (Trenga, J.).

40. Attached hereto as **Exhibit 14** is a true and correct copy of the April 8, 2022 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft, FS-ISAC, and Health-ISAC v. Malikov et al.*, Case No. 1:22-cv-1328 (N. D. Ga. 2022) (Cohen, J.)

41. Attached hereto as **Exhibit 15** is a true and correct copy of the May 27, 2022 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft v. John Does 1-2*, Case No: 122-cv-607 (E.D. Va. 2022) (Trenga, J.)

42. Attached hereto as **Exhibit 16** is a true and correct copy of the March 31, 2023 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft, Fortra, and Health-ISAC v. John Does 1-16*, Case No. 23-cv-2447 (E.D.N.Y 2023) (Morrison, J.)

43. Attached hereto as **Exhibit 17** is a true and correct copy of the September 25, 2024 *Ex Parte* Temporary Restraining Order and Order to Show Cause in the matter of *Microsoft and NGO-ISAC v. John Does 1-2*, Case No. 24-cv-02719 (D.D.C. 2024) (Contreras, J.)

44. Attached hereto as **Exhibit 18** is a true and correct copy of the August 5, 2016 *Ex Parte* Temporary Restraining Order and Order to Show Cause in the matter of *Microsoft Corporation v. John Does 1-2*, Case No. 16-cv-00993 (E.D. Va. 2016) (Lee, J.)

45. Attached hereto as **Exhibit 19** is a true and correct copy of the July 16, 2021 *Ex Parte* Temporary Restraining Order and Order to Show Cause in the matter of *Microsoft Corporation v. John Does 1-2*, Case No. 21-cv-00822 (E.D. Va. 2021) (Alston, J.)

46. Attached hereto as **Exhibit 20** is a true and correct copy of the December 2,

2021 *Ex Parte* Temporary Restraining Order and Order to Show Cause in the matter of *Microsoft Corporation v. John Does 1-2*, Case 21-cv-01346 (E.D. Va. 2019) (Brinkema, J.)

47. In each of the cases identified in the foregoing paragraphs, the Court granted similar *ex parte relief* to takedown the cybercriminal operation's technical infrastructure and authorized alternative service as requested here.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 11th day of November, 2024 in Washington D.C.

Jeffrey L Poston

Jeffrey L. Poston