UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

MICROSOFT CORPORATION, a Washington State Corporation, Plaintiff, v. John Doe 1, John Doe 2, a/k/a SamCodeSign, a/k/a "Fox Tempest," and John Does 3–4, a/k/a "Vanilla Tempest," Defendants.	Civil Action No. **FILED UNDER SEAL**

DECLARATION OF ADAM S. HICKEY IN SUPPORT OF PLAINTIFF'S EMERGENCY *EX PARTE* APPLICATION FOR TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Adam S. Hickey, declare and state as follows:

1. I am a Partner at the law firm of Mayer Brown LLP ("Mayer Brown") and am counsel of record for Plaintiff Microsoft Corporation ("Microsoft") in the above-captioned action. I make this Declaration in support of Microsoft's Emergency *Ex Parte* Application for Temporary Restraining Order and Order to Show Cause re Preliminary Injunction ("TRO Application"). Unless otherwise noted, the facts set forth below are based on my personal knowledge or upon information and belief based on my review of evidence collected as part of Microsoft's investigation in this case.

I. PARTIES

2. Microsoft seeks an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction to disrupt the technical infrastructure used by John Does 1–4 (collectively "Defendants") to distribute code signing certificates and sign malware with those certificates. Defendants operate a sophisticated cybercriminal enterprise that fraudulently obtains code signing certificates from Microsoft, then uses those certificates to digitally sign malicious software for the express purpose of circumventing security measures designed to protect computer users from harmful code; this malware-signing operation enables Defendants and their co-conspirators to distribute ransomware and other malicious programs that appear to be legitimate, causing widespread harm to Microsoft's customers and undermining the integrity of Microsoft's code signing ecosystem.

3. To accomplish this illegal activity, Defendants divide the work. John Does 1–2 (the "Fox Tempest Defendants") are responsible for fraudulently obtaining Microsoft's code signing certificates and managing the network of virtual machines used by the enterprise to distribute the certificates. John Does 3–4 (the "Vanilla Tempest Defendants") are responsible for uploading and signing malware with the certificates before deploying them in various schemes, such as through websites carefully designed to mimic the authentic Microsoft Teams download page. After victims download the malware disguised as Teams, Vanilla Tempest Defendants infiltrate the victims' computers, steal or encrypt the victims' data, and then extort victims for payment in return for suppressing or restoring access to the impacted data. The Defendants' criminal acts cause irreparable harm to Microsoft, its customers, and the public.

4. As counsel of record for Microsoft, I am aware of prior Microsoft lawsuits brought to disrupt other types of cybercriminal activities, including disrupting the "Tycoon 2FA" phishing-

as-a-service operation in February 2026 in the Southern District of New York; the "RaccoonO365" phishing-as-a-service operation in August 2025 in the Southern District of New York; the "Fake ONNX" phishing-as-a-service operation in November 2024 in the Eastern District of Virginia; the "Star Blizzard" spear phishing operation in September 2024 in the District of Columbia; the "Storm-1152 CAPTCHA Fraud" cyber hacking operation in December 2023 in the Southern District of New York; the "Cracked Cobalt Strike" cybercriminal and malware operation in March 2023 in the Eastern District of New York; and the "Bohrium" threat infrastructure in May 2022 in the Eastern District of Virginia.

5. As part of my involvement in this case, I learned about Microsoft's prior experience with litigating claims against cybercriminals. Based on Microsoft's prior experiences in those matters, I believe that the requested *ex parte* relief is necessary here. Notice to Defendants would give them an opportunity to move infrastructure and destroy the evidence of their illicit activity. Microsoft's requested relief and prosecution of this matter would then be futile.

6. I have learned of multiple prior Microsoft cases to disrupt cybercriminals' activities in which the bad actors attempted to delete and/or move the targeted infrastructure when they learned of Microsoft's efforts. For example, in *Microsoft Corp. v. John Does 1–11*, No. 2:11-cv-00222 (W.D. Wa. 2011), when the operators of the Rustock Botnet learned of the attempt to disable the botnet, they attempted to move the botnet's command and control infrastructure to new IP addresses and to delete files from the seized host servers. Likewise, in *Microsoft Corp. v. John Does 1–8*, No. 1:13-cv-1014 (W.D. Tex. 2013), in response to a seizure of domains associated with the ZeroAccess Botnet, the operators immediately, unsuccessfully attempted to move the botnet's command and control infrastructure. Lastly, in *Microsoft Corp. v. John Does 1–5*, No. 1:15-cv-06565 (E.D.N.Y. 2015), a matter involving the Dorkbot Botnet, its operators

attempted to activate dormant command and control domains to maintain control over the Dorkbot infected devices one day after Microsoft executed a temporary restraining order. Although those matters involved botnets, the cybercriminal infrastructure at issue there is materially similar to the infrastructure used by Defendants in this case. Like the botnet operators, Defendants rely on internet-based infrastructure—including web domains, virtual private servers, and other online accounts—that can be rapidly migrated to new providers, reconfigured, or deleted in response to legal process, and the evidence of their activity is stored in digital form that can be destroyed within minutes of detection. Defendants likewise possess the technical sophistication and operational control necessary to relocate their infrastructure, activate backup or dormant assets, and erase records on short notice if alerted to Microsoft's enforcement efforts. Even in this case, as described in more detail in the Mason Declaration, paragraphs 27 and 76, the Defendants evolved their operations in response to Microsoft's efforts to counter and disrupt their activities. Accordingly, based on these prior experiences of Microsoft, I believe that there is a similar risk that Defendants here would take similar actions to evade or obstruct a temporary restraining order in this case.

7. As of this submission, Microsoft's counsel has not attempted to provide notice of the Emergency *Ex Parte* Application for Temporary Restraining Order to Defendants, and I respectfully submit notice should not be required at this time. Rather, the risk that Defendants will attempt to evade or obstruct the relief sought by the TRO Application provides good and sufficient cause for the TRO Application to be made by Order to Show Cause in lieu of notice of motion. Microsoft has previously sought and received *ex parte* temporary restraining orders in this District and a number of other federal district courts, including *Microsoft Corp. v. Fridi*, No. 1:26-cv-01603 (S.D.N.Y. Feb. 26, 2026) (Dkt. 31) (Cote, J.) ("Tycoon 2FA"); *Microsoft Corp. and Health-*

ISAC v. Joshua Ogundipe and John Does 1–4, No. 1:25-cv-07111 (S.D.N.Y. Aug. 27, 2025) (Dkt. 13) (Rakoff, J.) ("RaccoonO365"); *Microsoft Corp. and LF Projects v. Abanoub Nady and John Does 1–4*, No. 1:24-cv-2013-RDA (E.D. Va. Nov. 13, 2024) (Dkt. 16) (Alston, J.) ("Fake ONNX"); *Microsoft Corp. v. Tu et al.*, No. 23-cv-10685 (S.D.N.Y. Dec. 7, 2023) (Dkt. 35-1) (Engelmayer, J.) ("Storm-1152"); *Microsoft Corp., Fortra, and Health ISAC v. John Does 1–16*, No. 23-cv-02447 (E.D.N.Y. Mar. 31, 2023) (Dkt. 13) (Morrison, J.) ("Cracked Cobalt Strike"); and *Microsoft Corp. v. John Does 1–2*, No. 1:22-cv-00607 (E.D. Va. May 27, 2022) (Dkt. 16) (Trenga, J.) ("Bohrium").

8. For the same reasons, Microsoft respectfully requests that the Complaint, the *Ex Parte* TRO Application, this Declaration, and all supporting papers and exhibits be filed and maintained under seal pending execution of any temporary restraining order issued by the Court. Public disclosure of these materials prior to execution of the requested relief would alert Defendants to the action and enable them to migrate, destroy, or conceal the infrastructure and evidence at issue, thereby frustrating the relief sought. As soon as reasonably practicable after the requested actions are carried out, Microsoft will move the Court to unseal the case and make the appropriate portions of the filings publicly accessible.

9. Microsoft has identified certain IP addresses associated with virtual machines that are believed to be part of the infrastructure used by the Defendants. The IP addresses associated with Defendants' infrastructure are set forth in **Appendix B** to Microsoft's Complaint in this case.

10. I understand that investigators of Microsoft's Digital Crimes Unit ("DCU"), including Maurice Mason, another declarant in this action, have worked to determine the true identities of Defendants. As part of Microsoft's investigation, DCU investigators (with assistance from a cooperating source) anonymously conducted two test purchases of the code signing service

from John Doe 2 ("SamCodeSign") in February and March of 2026. The source contacted SamCodeSign on Telegram, a cloud-based instant messaging service that allows users to communicate anonymously through pseudonymous usernames, and expressed interest in purchasing certificates. SamCodeSign directed the source to a Google Form to select a purchase tier and requested payment via Bitcoin. Using the wallet address provided by SamCodeSign, Microsoft traced associated financial transactions and identified payments between Vanilla Tempest Defendants and another wallet linked to SamCodeSign. Following payment, SamCodeSign provided the source with instructions to access a virtual machine, including the username, password, and IP address. The virtual machine was hosted by RouterHosting LLC (d/b/a/ "Cloudzy,") a commercial virtual private server ("VPS") and cloud hosting provider that offers on-demand Windows and Linux virtual machines. A DCU investigator logged in to the virtual machine using these credentials and successfully signed a file with a certificate controlled by Fox Tempest Defendants. From this access, Microsoft was able to identify additional virtual machines hosted by Cloudzy that Fox Tempest Defendants use to distribute certificates to Vanilla Tempest Defendants and other cybercriminals. DCU investigators analyzed the Azure tenant and subscription information visible on the virtual machine, which revealed configuration data linking to other virtual machines within the same infrastructure. This analysis, combined with IP address correlation and review of the code signing endpoints referenced in the configuration files, enabled Microsoft to map the broader network of Cloudzy-hosted virtual machines used by Fox Tempest Defendants.

11. Based on our experience and from Microsoft's research, I believe that the most reliable contact information for effectuating communication with Defendants are the email addresses associated with Defendants' infrastructure—including the email address

gacermalkin@gmail.com that was used as the technical contact for hundreds of Microsoft tenants created by Fox Tempest Defendants and as the owner of the Google Sheet used by SamCodeSign to administer the service—as well as email addresses provided by Defendants to Microsoft in the course of registering for Artifact Signing, the contact information provided to the registrar for signspace.cloud, teams-download[.]buzz, teams-install[.]run, and teams-download[.]top, and the contact information provided to Microsoft by Defendants to access the Cloudzy virtual machine. Microsoft will provide notice using such contact information.

II. NOTICE AND SERVICE OF PROCESS

A. Microsoft Will Provide Notice

12. Once the TRO has been issued and the Defendants' infrastructure has been disabled, transferred, or otherwise made inaccessible to Defendants, Mayer Brown 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 the e-mail addresses and mailing addresses associated with the Defendants or otherwise provided by the Defendants to Microsoft and other third parties through which Defendants accessed Microsoft's services.

13. On behalf of Microsoft, Mayer Brown 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.net/opfauxsign. Mayer Brown 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. A summary stating that Microsoft seeks a preliminary injunction directing the domain registrar and virtual machine provider identified in **Exhibit 2** and

Appendix B to the Complaint to take all steps necessary to disable access to and operation of the Defendants' infrastructure and that all content and material associated with that infrastructure are to be isolated and preserved pending resolution of the dispute. Microsoft seeks a permanent injunction, other equitable relief, and damages. Full copies of the pleading documents are available at www.noticeofpleadings.net/opfauxsign.

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 Microsoft's attorney, Adam S. Hickey at Mayer Brown LLP, 1221 Avenue of the Americas, New York, NY 10020, ahickey@mayerbrown.com. If you have questions, you should consult with your own attorney immediately."

14. On behalf of Microsoft, Mayer Brown will serve each of the third parties identified in Microsoft's [Proposed] Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause with copies of all documents served on Defendants.

15. On behalf of Microsoft, Mayer Brown will attempt notice of any preliminary injunction hearing, as well as service of the Complaint, by personal delivery on any Defendant in this case that has provided existing physical addresses in the United States.

16. On behalf of Microsoft, Mayer Brown will prepare Requests for Service Abroad of Judicial or Extrajudicial Documents to attempt notice of any preliminary injunction hearing, as well as service of the Complaint, on any Defendant that has 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.

17. Upon entry of any TRO and to the extent Microsoft identifies and locates the John Doe Defendants, Mayer Brown 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 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 Microsoft's Terms of Use for Artifact Signing

18. To use Microsoft's Artifact Signing service and obtain code signing certificates, every user must first sign up for an Azure subscription and tenant and then set up the service through the Azure Portal. To activate their Azure subscriptions, Fox Tempest Defendants were required to click on a verification email sent by Microsoft; they also used these email addresses for multi-factor authentication to access their Azure accounts. Mason Decl. ¶ 20. Fox Tempest Defendants accessed Microsoft's Artifact Signing service in exactly that manner, creating more than 580 fraudulent Microsoft tenants and using those tenants to obtain access to the Artifact Signing service and generate the code signing certificates at issue in this case.

19. All users of the Artifact Signing service are bound by Microsoft's Terms of Use for Artifact Signing ("Terms of Use"), a contract that governs access to and use of the service. A true and correct copy of the Terms of Use, last updated January 5, 2026, is attached as **Exhibit 1** to the

Complaint. By creating Microsoft tenants and accessing the Artifact Signing service, Fox Tempest Defendants accepted and became bound by the Terms of Use.

20. Section 5 of the Terms of Use, "Account, Password, and Security," provides that, to use the Services, the user must "complete the registration process by providing Microsoft with current, complete, and accurate information as prompted by the applicable registration form[.]"

21. Similarly, in Section 2(b) of the Terms of Use, the user "represents and warrants" that "(i) all the Submitted Information and all representations Company makes to Microsoft in any Services applications are accurate," and "(ii) Company will inform Microsoft if the Submitted Information or the representations it made to Microsoft in any Services application changed or is no longer valid." "Submitted Information" is defined in Section 2 to include the "personal and other information" required for vetting to verify the user's identity, such as "the e-mail address of Company's personnel who submitted such information, if applicable."

22. Section 15(b) of the Terms of Use, entitled "Notices," expressly authorizes service of notice by email and provides that the user "consents to Microsoft providing notices about the Services or TOU, or information the law requires Microsoft to provide, via email to the address Company specified when it signed up for the Services. Notices emailed to Company will be deemed given and received when the email is sent." Section 15(b) further provides that, "[i]f Company does not consent to receive notices electronically, it must stop using the Services."

23. Section 15(f) of the Terms of Use likewise confirms that, with respect to "notices pertaining to the Managed Certificates or signatures, including with regard to their use or status, or access credentials related to same," such notices "will be provided electronically … to the email address provided by Company with its Submitted Information."

24. The effect of the foregoing provisions is that every user of Microsoft's Artifact Signing service—including Fox Tempest Defendants in connection with each of the more than 580 fraudulent Microsoft tenants they created to access the service—has agreed that notice from Microsoft about the Services or the Terms of Use, or information that the law requires Microsoft to provide, may be given by sending an email to the address that the user provided to Microsoft when signing up for the Services, and that such notice is deemed given and received when the email is sent.

25. Section 2(b) of the Terms of Use further provides that the user represents and warrants that "the Submitted Information (including the email address of Company's personnel who submitted such information, if applicable) has not been and will not be used for any unlawful purpose," and that "Company will use the Services exclusively for authorized and legal purposes consistent with this TOU."

26. Section 2(g) of the Terms of Use, the "Code of Conduct," further provides that "Company may not use the Services to (or to assist any third party to): (i) do anything illegal; (ii) engage in any activity that exploits, harms, or threatens to harm anyone; … (v) engage in false or misleading activity; (vi) engage in activity that harms the Services or others; (vii) infringe on or misappropriate the rights of others; . . . or (xi) enable access to the Services by unauthorized third-party applications."

C. <u>Notice under ICANN Domain Name Registration Policies</u>

27. Attached hereto as **Exhibit 1** is a true and correct copy of a document describing the role of the Internet Corporation for Assigned Names and Numbers ("ICANN"). **Exhibit 1** 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 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.

28. A true and correct copy of the 2013 ICANN Registrar Accreditation Agreement (as updated by the 2024 global amendment) between ICANN and domain name registrars is attached hereto as **Exhibit 2**.

29. The following summarizes provisions set forth in the ICANN accreditation agreements with registrars at **Exhibit 2**.

ICANN Requires that Registrants Agree to Provide Accurate Contact Information

30. Section 3.7.7.1 of the ICANN Registrar 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 [sic] Registered Name Holder that is an organization, association, or corporation …."

31. Section 3.7.7.2 of the accreditation agreement provides that if the registrant fails to respond for over fifteen (15) days to a registrar's inquiry about inaccurate contact information, the domain may be canceled. 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

32. 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 3** is a true and correct copy of the UDRP.

33. 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 4** is a true and correct copy of the Rules.

34. 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. "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."

35. Pursuant to the Rules, notice of a complaint may be achieved by the registrar forwarding the complaint to the postal address, facsimile number, and email 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..."

36. 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

37. 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

38. 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."

39. 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."

D. Notice under GoDaddy.com LLC's Domain Name Registration Policy

40. Fox Tempest Defendants registered for the domain, signspace.cloud, with GoDaddy.com LLC ("GoDaddy"). In doing so, Fox Tempest Defendants accepted and became bound by GoDaddy's Domain Name Registration Agreement (the "GoDaddy Agreement"), available at https://www.godaddy.com/legal/agreements/domain-name-registration-agreement. A true and correct copy of the GoDaddy Agreement, last revised November 3, 2025, is attached hereto as **Exhibit 5**.

41. Section 5 of the GoDaddy Agreement provides that the customer "agree[s] to notify GoDaddy within five (5) business days when any of the information you provided as part of the application and/or registration process changes," and that "[i]t is your responsibility to keep this

information in a current and accurate status. Failure by you, for whatever reason, to provide GoDaddy with accurate and reliable information on an initial and continual basis, shall be considered to be a material breach of this Agreement and a basis for suspension and/or cancellation of the domain name." Section 5 further provides that, "for each domain name registered by you, the following contact data is required: postal address, email address, telephone number, and if available, a facsimile number for the Registered Name Holder and, if different from the Registered Name Holder, the same contact information for, a technical contact, an administrative contact and a billing contact."

42. Section 2 of the GoDaddy Agreement provides that, by submitting an application or registering or renewing a domain name, the customer "represent[s] and warrant[s] that: (a) all information provided to register or renew the domain name (including all supporting documents, if any) is true, complete and correct, and is not misleading in any way, and the application is made in good faith." Section 2 further provides that the customer "acknowledge[s] and agree[s] that the Registry or the registrar can cancel the registration of the domain name if any of the warranties required are found to be untrue, incomplete, incorrect or misleading."

43. Section 1 of the GoDaddy Agreement provides that "GoDaddy may occasionally notify you of changes or modifications to this Agreement by email. It is therefore very important that you keep your [account] information, including your email address, current."

44. The effect of the foregoing provisions is that Fox Tempest Defendants have agreed with GoDaddy to provide and maintain accurate contact information, including a current email address, and that GoDaddy may communicate with them by email at the address on file.

45. Section 8 of the GoDaddy Agreement provides that the customer "represent[s] and warrant[s] to the best of [its] knowledge that, neither the registration of the domain nor the manner

it is directly or indirectly used, infringes the legal rights of any third party," and that the customer "will comply with all applicable laws." Section 8 further authorizes GoDaddy to suspend, cancel, or transfer any registration "to comply with any applicable court orders, laws, government rules or requirements, requests of law enforcement, or any dispute resolution process," or "to avoid any liability, civil or criminal, on the part of registry operator."

III. OTHER AUTHORITY AND EVIDENCE

46. Many courts have granted Microsoft's requested *ex parte* relief against similarly situated cybercriminal organizations. Additionally, Microsoft's proposed alternative service has previously been approved in other actions brought by Microsoft to halt cybercriminal organizations that, like the Defendants here, carry out their unlawful activity through the use of a technical infrastructure of Internet domains, hosting providers, instant messaging platforms, virtual machines, and cryptocurrency.

47. Attached hereto as **Exhibit 6** is a true and correct copy of the February 26, 2026 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft Corp. v. Fridi*, No. 1:26-cv-01603 (S.D.N.Y. Feb. 26, 2026) (Dkt. 31) (Cote, J.) ("Tycoon 2FA").

48. Attached hereto as **Exhibit 7** is a true and correct copy of the August 27, 2025 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft Corp. v. Ogundipe*, No. 1:25-cv-07111 (S.D.N.Y. Aug. 27, 2025) (Dkt. 13) (Rakoff, J.) ("RaccoonO365").

49. Attached hereto as **Exhibit 8** is a true and correct copy of the November 13, 2024 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft Corp. v. Nady*, No. 1:24-cv-2013-RDA (E.D. Va. Nov. 13, 2024) (Dkt. 16) (Alston, J.) ("Fake ONNX").

50. Attached hereto as **Exhibit 9** 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 Corp. v. John Does 1–2*, No. 1:24-cv-02719 (D.D.C. 2024) (Dkt. 12) (Contreras, J.) ("Star Blizzard").

51. Attached hereto as **Exhibit 10** is a true and correct copy of the December 7, 2023 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft Corp. v. Tu*, No. 23-cv-10685 (S.D.N.Y. Dec. 7, 2023) (Dkt. 35-1) (Engelmayer, J.) ("Storm-1152").

52. Attached hereto as **Exhibit 11** is a true and correct copy of the March 31, 2023 *Ex Parte* Temporary Restraining Order, Seizure Order, and Order To Show Cause in the matter of *Microsoft Corp. v. John Does 1–16*, No. 23-cv-02447 (E.D.N.Y. Mar. 31, 2023) (Dkt. 13) (Morrison, J.) ("Cracked Cobalt Strike").

53. Attached hereto as **Exhibit 12** 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 Corp. v. John Does 1–2*, No. 1:22-cv-00607 (E.D. Va. May 27, 2022) (Dkt. 16) (Trenga, J.) ("Bohrium").

54. In each of the cases identified in the foregoing paragraphs, the Court granted similar *ex parte* relief to take down 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 4 day of May, 2026, in New York, New York.

Adam S. Hickey