**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF NEW YORK**

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

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

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

**Page(s)**

**Cases**

**Statutes**

**Other Authorities**

Pursuant to Rule 65 of the Federal Rules of Civil Procedure, Plaintiff Microsoft Corporation ("Microsoft") respectfully submits this Memorandum of Law in Support of its Motion for an Emergency *Ex Parte* Temporary Restraining Order ("TRO Application") and a Preliminary Injunction against John Does 1–2 (collectively "Fox Tempest Defendants") and John Does 3–4 (collectively "Vanilla Tempest Defendants," and together with the Fox Tempest Defendants, the "Defendants").

## I. INTRODUCTION

This action involves an organized criminal enterprise—the "Certificate Abuse Enterprise"—that has systematically exploited Microsoft's code signing technology to facilitate the deployment of dangerous malware against Microsoft, Microsoft's customers, and the public.

Code signing is a critical security mechanism that cryptographically verifies both the origin and integrity of software, enabling users and operating systems to distinguish legitimate programs from malicious ones. To carry out the Certificate Abuse Enterprise, Fox Tempest Defendants have exploited Microsoft's Artifact Signing service to fraudulently obtain code signing certificates and sell them to Vanilla Tempest Defendants and other cybercriminals. Vanilla Tempest Defendants then disguise dangerous malware as legitimate software by signing the malware with these certificates that brand the software as trusted by Microsoft, packaging it to appear as legitimate Microsoft product, and employing malicious advertising campaigns and search engine optimization poisoning techniques to disseminate that malware. These efforts trick victims into downloading the malware onto their devices, allowing Vanilla Tempest Defendants to steal their information, deploy ransomware, and extort them for financial gain.

Vanilla Tempest Defendants and other cybercriminals have used the fraudulently obtained certificates from Fox Tempest Defendants to impact thousands of computers in the United States. Each time Defendants deploy malware signed with fraudulently obtained certificates, they do so

with the express purpose of bypassing the security features of Microsoft's products and systems, targeting Microsoft and Microsoft's customers, and deceiving the public into believing that the malware is legitimate software trusted by Microsoft. These unlawful acts cause Microsoft irreparable harm for which no monetary recourse is available or sufficient. Microsoft seeks *ex parte* injunctive relief to direct providers of the technological infrastructure used by Defendants to take specific actions to disrupt the scheme and prevent Defendants from continuing their criminal operation.

It is imperative that relief be *ex parte*. Notice to Defendants would provide them with an opportunity to destroy, move, or otherwise make inaccessible the infrastructure Defendants use to conduct the Certificate Abuse Enterprise's operations and the evidence of their unlawful activity. This District and other federal district courts have granted Microsoft the same *ex parte* relief requested here and enjoined cybercriminals from continuing cyberattacks against Microsoft customers.[1] Microsoft respectfully requests that this Court grant the same relief here.

## II. STATEMENT OF FACTS

### A. Microsoft's Services and Reputation

Microsoft is one of the world's leading technology companies. Decl. of Maurice Mason in support of TRO Application ("Mason Decl.") ¶ 69. Microsoft is a provider of the Windows® computer operating system, and a variety of other software and services including Microsoft 365®, OneDrive®, and Azure®. *Id*. Microsoft has invested substantial resources in creating reliable, high-quality, and secure products and services. These investments, combined with Microsoft's

[1] *See, e.g.*, *Microsoft Corp. v. Fridi*, No. 1:26-cv-01603 (S.D.N.Y. Feb. 26, 2026) (Cote, J.); *Microsoft Corp. v. Ogundipe*, No. 1:25-cv-07111 (S.D.N.Y. Aug. 27, 2025) (Rakoff, J.); *Microsoft Corp. v. John Does 1–2*, No. 24-cv-02719 (D.D.C. Sept. 25, 2024) (Contreras, J.); *Microsoft Corp. v. Nady*, No. 1:24-cv-02013 (E.D. Va. Nov. 13, 2024) (Alston, J.); *Microsoft Corp. v. Tu*, No. 23-cv-10685 (S.D.N.Y Dec.7, 2023) (Engelmayer, J.); *Microsoft v. John Does 1–16*, No. 23-cv-02447 (E.D.N.Y. Mar. 31, 2023) (Morrison, J.); *Microsoft Corp. v. John Does 1–2*, No. 1:22-cv-00607 (E.D. Va. May 27, 2022) (Trenga, J.).

consistent delivery of value and its commitment to protecting customers from cyberattacks, have generated substantial goodwill with Microsoft's customers and established a strong brand and world-wide symbols that are well-recognized within its channels of trade. *Id*. ¶ 69. Microsoft maintains registered trademarks representing the quality of its products, services, and brands, including Microsoft®, Windows®, Microsoft 365®, Microsoft Teams®, and Azure®. *Id*. Copies of the trademark registrations for these trademarks are attached as **Appendix A** to Microsoft's concurrently filed Complaint.

"Artifact Signing" is Microsoft's fully managed, end-to-end code signing solution integrated with Microsoft's Azure platform. *Id*. ¶ 17-18. The service, which Microsoft launched in 2024, enables software developers to digitally sign their applications, a process that protects software against tampering and verifies the identity of the signing entity. *Id*. ¶¶ 5, 17. A digital signature generated via Artifact Signing confirms that the underlying code remains unmodified and identifies the responsible party through an associated certificate. *Id.* ¶¶ 5, 17. When end users view the properties of software signed through this service, the certificates display the Microsoft® trademark, identifying Microsoft as the issuing certificate authority. *Id*. ¶ 70; Fig. 15.

The Windows operating system treats software bearing a valid digital signature—such as one from an Artifact Signing certificate—as authenticated and trustworthy. *Id*. ¶ 6. In particular, a valid signature allows software to satisfy security mechanisms that would otherwise alert users that the software is malicious, including Microsoft's SmartScreen filter, User Account Control ("UAC"), and Smart App Control ("SAC"), which Windows 11 introduced to automatically block unsigned or low-reputation software, preventing the execution of untrusted applications regardless of a user's intent. *Id*. ¶¶ 6–7, 33. These features are intended to protect or caution users before they install or run software from unverified or unfamiliar sources. *Id*. ¶ 6. The presence of a valid digital

signature causes the operating system to suppress these warnings and, in some cases, bypass the automatic block on software execution. *Id*. ¶¶ 6–7, 33.

### B. Defendants' Activities

This action involves the Fox Tempest Defendants and Vanilla Tempest Defendants who, together with other cybercriminals, comprise the Certificate Abuse Enterprise that has systematically exploited Microsoft's code signing technology to facilitate the deployment of dangerous malware against Microsoft, its customers, and the public. *Id.* ¶¶ 4, 12.

#### 1. Defendants' Procurement and Distribution of Code Signing Certificates

Since at least May 2025, Fox Tempest Defendants have operated an underground code signing service that supplies fraudulently obtained certificates to Vanilla Tempest Defendants and other cybercriminals. *Id.* ¶ 12. The certificates allow Vanilla Tempest Defendants to disguise malware as legitimate software, causing victims' Windows operating systems to treat the malicious code as trustworthy and bypass security features that would otherwise flag or block it. *Id.* ¶¶ 6–7, 33.

To obtain the certificates they sell, Fox Tempest Defendants fraudulently create Microsoft tenants that bypass Microsoft's identity validation requirements for Artifact Signing. *Id.* ¶¶ 17–21. To date, they have created more than 580 such fraudulent tenants and used them to generate certificates, which they then sell to Vanilla Tempest Defendants and other cybercriminals. *Id.*

Fox Tempest Defendants employ multiple fraudulent techniques to bypass the Microsoft entity and identity validation systems and processes required to set up Artifact Signing. *Id.* ¶ 21. These techniques include: exploiting the partner sign-up process by registering domains with fake names and contact information; submitting fake government identification; and creating fraudulent shell companies or fabricated business registration documents. *Id.*

Fox Tempest Defendants communicate with customers and prospective buyers through Telegram, a cloud-based instant messaging service. *Id.* ¶ 28. John Doe 2, operating under the alias "SamCodeSign," manages the Telegram channel and markets the code signing service through direct purchases and auctions managed via Google Sheets. *Id.* Metadata from one such Google Sheet identified the account gacermalkin@gmail.com as the document owner—the same email address used as the technical contact for hundreds of the fraudulent Microsoft tenants that John Doe 1 created to access Artifact Signing. *Id.* ¶ 29.

Fox Tempest Defendants distribute certificates to cybercriminals, including Vanilla Tempest Defendants, through two primary channels: (1) the website signspace.cloud, and (2) virtual machines hosted by RouterHosting LLC (d/b/a "Cloudzy"), a virtual private server provider. *Id.* ¶¶ 22–26.

*Signspace.cloud.* Fox Tempest Defendants operate signspace.cloud as a platform for delivering their code signing service. *Id.* ¶ 23. The registrar for signspace.cloud is GoDaddy.com, LLC ("GoDaddy"), a company based in the United States. *Id.* ¶ 24. The signspace.cloud website enables customers to upload code and sign it using certificates obtained by Fox Tempest Defendants. *Id.* ¶ 23. After submitting payment, customers receive instructions on how to log in to their user pages, upload malicious code, and download it with the certificate attached. *Id.* An administrator panel allows Fox Tempest Defendants to manage user accounts and provide certificates. *Id.*

*Virtual Machines.* Beginning in January 2026, Fox Tempest Defendants transitioned to using virtual machines for their code signing service. *Id.* ¶ 26. They provide customers access to these machines through Remote Desktop Protocol and instruct them on how to sign their code. *Id*.

Microsoft has identified more than 149 virtual machines hosted by Cloudzy that Fox Tempest Defendants have used to distribute code signing certificates. *Id*.

### 2. The Attack Chain

**Step 1: Purchasing Fraudulently Obtained Certificates.**

To acquire the certificates used to sign malware, Vanilla Tempest Defendants purchase code signing certificates from Fox Tempest Defendants. Vanilla Tempest Defendants have made numerous payments to a wallet Fox Tempest Defendants control, likely for the purpose of obtaining these code signing certificates. *Id.* ¶¶ 31, 64.

**Step 2: Signing Malware.**

After payment, Fox Tempest Defendants provide Vanilla Tempest Defendants with access to signspace.cloud or a virtual machine (hosted by Cloudzy) where Vanilla Tempest Defendants sign their malware with the fraudulently obtained certificates. Vanilla Tempest Defendants use these certificates to sign malware designed to collect system information, steal credentials, execute commands, download additional malware (including ransomware) and maintain persistence on infected machines by creating scheduled tasks. *Id.* ¶¶ 32, 34.

**Step 3: Creating Fraudulent Installer Files and Websites.**

To distribute their signed malware, Vanilla Tempest Defendants create fraudulent installer files named "MSTeamsSetup.exe," designed to appear as legitimate Microsoft Teams installers. *Id.* ¶ 36. They host these files on malicious domains that mimic Microsoft Teams websites, including "teams-download[.]buzz," "teams-install[.]run," and "teams-download[.]top." Mason Decl. ¶ 36. These websites display Microsoft's logo and trademarks, including Microsoft® and Microsoft Teams®. Mason Decl. ¶ 36; Fig. 3.

**Step 4: Deploying Malware.**

Vanilla Tempest Defendants employ search engine optimization poisoning to direct victims to the malicious download sites mimicking Microsoft Teams. *Id.* ¶¶ 9, 35. When victims execute the fake installer files, those files deliver a malicious loader that installs the fraudulently signed malware, which ultimately deploys ransomware. *Id.* ¶ 37.

Because the Oyster malware deployed has been fraudulently signed by a certificate from Microsoft's Artifact Signing service, the Windows operating system initially treats it as legitimate software rather than flagging or blocking it as suspicious. *Id.* ¶ 33; *see also* Mason Decl. Figs. 24, 21-22.

Through this scheme, Vanilla Tempest Defendants gain unauthorized access to victims' computers, exfiltrate personal and confidential information, deploy ransomware that encrypts victims' files and systems, and extort victims by demanding payment to restore access to or suppress their data. Mason Decl. ¶ 37. Those victims' payments can then be used by Vanilla Tempest Defendants to procure additional infrastructure to support additional hacking operations, such as by purchasing additional certificates from the Fox Tempest Defendants.

### 3. Test Purchase

As part of Microsoft's investigation into the Certificate Abuse Enterprise, Microsoft's Digital Crimes Unit ("DCU"), the division tasked with investigating cybercrime threats, anonymously conducted two test purchases of the code signing service from John Doe 2 ("SamCodeSign") in February and March 2026 with assistance from a cooperating source. *Id.* ¶ 42. The source contacted SamCodeSign on Telegram and expressed interest in purchasing certificates. *Id.* ¶ 43. SamCodeSign directed the source to a Google Form to select a purchase tier: Standard ($5,000), Priority ($7,500), or Expedited ($9,500), corresponding to how quickly the certificates would be provided. *Id.* ¶ 44; Mason Decl. Fig. 6. The form also requested information about how

frequently the purchaser would need certificates, along with contact information and any additional comments. Mason Decl. ¶ 44.

After the source completed the Google Form, SamCodeSign requested payment via Bitcoin. *Id.* ¶ 45. Using the wallet address provided, Microsoft traced associated financial transactions and identified payments between Vanilla Tempest Defendants and another wallet linked to SamCodeSign. *Id.* ¶¶ 61–64.

Following payment, SamCodeSign provided the source with instructions to access a virtual machine, including the username, password, and IP address, as well as directions for completing the code signing process. *Id.* ¶ 46. A DCU investigator logged into the virtual machine using these credentials and successfully signed a file with a certificate controlled by Fox Tempest Defendants. *Id.* ¶¶ 48–57. While remotely accessing the machine, the DCU investigator collected information on the Microsoft Azure tenant and subscription used by Fox Tempest Defendants to facilitate the code signing process—specifically, the TenantID and Subscription ID visible during the Azure authentication process on the virtual machine. *Id.* ¶ 58. DCU was also able to identify more than 149 virtual machines hosted by Cloudzy in connection with Fox Tempest Defendants' operations. *Id.* ¶ 26. Microsoft has assessed with high confidence that the virtual machines associated with the IP addresses attached in **Appendix B** to the Complaint have been used by the Certificate Abuse Enterprise. *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. *Univ. of Texas v. Camenisch*, 451 U.S. 390, 395 (1981). To be eligible for the requested injunctive relief, a Plaintiff must demonstrate that (1) it is likely to succeed on the merits, (2) it is likely to suffer irreparable harm, (3) the balance of hardships tips

in its favor, and (4) the injunction is in the public interest. *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008)); *UBS Fin. Servs., Inc. v. W Va. Univ. Hosps., Inc.*, 660 F.3d 643, 648 (2d Cir. 2011). In the Second Circuit, this standard is flexible, and preliminary equitable relief is warranted when the moving party demonstrates that "sufficiently serious questions going to the merits to make them a fair ground for litigation and [that the] balance of hardships tip[s] decidedly toward the party requesting the preliminary relief[,]", so long as the other two elements are also met. *UBS Fin. Servs., Inc.*, 660 F.3d at 648. This matter requires injunctive relief. With each day that Defendants' criminal enterprise continues to operate, Microsoft, its customers, and the general public suffer irreparable harm.

## IV. PLAINTIFF'S REQUESTED RELIEF IS WARRANTED

### A. Plaintiff Is Likely to Succeed on the Merits.

Microsoft is likely to succeed on the merits of its claim or, at the very least, has raised serious questions going to the merits of its claims such that a temporary restraining order and a preliminary injunction should be granted. Microsoft alleges the following statutory and common law claims: conspiracy to damage protected computers and trafficking in passwords, in violation of the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(b) & § 1030(a)(6); racketeering and conspiracy to engage in racketeering, in violation of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(c)–(d); trademark infringement, false designation of origin, and trademark dilution in violation of the Lanham Act, 15 U.S.C. §§ 1114(1), 1125(a) & 1125(c); and breach of contract, trespass to chattels, and unjust enrichment. Though early in the proceedings, the record contains ample evidence supporting the elements of each claim and the likelihood of success on the merits weighs in favor of granting injunctive relief.

### 1. Defendants Violate the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq*.

The Computer Fraud and Abuse Act ("CFAA") prohibits computer crimes such as the ones described here. *See, e.g.*, *Univ. Sports Publ'ns Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 384 (S.D.N.Y. 2010) (concluding that the CFAA's language and legislative history show that Congress intended it to proscribe hacking); *In re Doubleclick Privacy Litig.*, 154 F. Supp. 2d 497, 525 n.34 (S.D.N.Y. 2001) (describing "the damage Congress sought to punish and remedy in the CFAA—namely, damage to computer systems and electronic information by hackers"). Among other things, the CFAA makes illegal conduct that (1) "conspires to commit or attempts to commit an offense under subsection (a) of this section[,]" 18 U.S.C. § 1030(b), such as "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer[,]" 18 U.S.C. § 1030(a)(5)(A); and (2) "knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if . . . such trafficking affects interstate or foreign commerce[,]" 18 U.S.C. § 1030(a)(6). The CFAA provides a private right of action, so that any person "who suffers damages or loss by reason of violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

Based on the information contained in the Mason Declaration, Plaintiff is very likely to prove at trial that the Certificate Abuse Enterprise functions to enable cybercriminals like the Vanilla Tempest Defendants to more effectively lure Microsoft customers and other members of the public into downloading and executing malware on their systems, which enables the theft of information, encryption and destruction of data, and extortion of money. The Fox Tempest

Defendants enable this scheme through their fraud on the Microsoft code signing service, are enriched through their sale of fraudulently obtained certificates to the Vanilla Tempest Defendants (knowing and intending that the certificates would be used to facilitate computer fraud and abuse), and profit from the Vanilla Tempest Defendants' hacking operations, as they return to purchase additional certificates for further hacking operations.

**a. Defendants Conspire to Damage a Computer without Authorization in Violation of Section 1030(b).**

Fox Tempest Defendants conspired with Vanilla Tempest Defendants to violate Section 1030(a)(5)(A) by knowingly providing fraudulently obtained code signing certificates with the knowledge that such certificates would be used to sign malware for deployment onto protected computers, including those belonging to Microsoft and its customers. Mason Decl. ¶¶ 12–15. Fox Tempest Defendants marketed their code signing service to cybercriminals, sold certificates knowing they would be used to sign malware, and provided technical support and infrastructure to facilitate the deployment of signed malware. *Id.* ¶¶ 13–14, 22–29. Vanilla Tempest Defendants in turn conspired with Fox Tempest Defendants by purchasing the code signing certificates, using those certificates to sign malware, and deploying the signed malware onto the protected computers of Microsoft and its customers. *Id.* ¶¶ 15, 30–41.

As a result of the conspiracy and the overt acts taken in furtherance thereof, Defendants intentionally caused damage without authorization to protected computers in the United States. *Id.* ¶¶ 40, 67. The malware deployed by Defendants caused damage by collecting system information, stealing credentials, executing unauthorized commands, downloading additional malware, and deploying ransomware that encrypted victims' files and rendered their computers unusable. *Id.* ¶¶ 32, 34, 37. "The CFAA was designed to prohibit the type of unauthorized access and fraudulent conduct facilitated by malware and botnet activity." *Microsoft Corp. v. Does 1–2*, 2021

WL 4755518, at *7 (E.D.N.Y. May 28, 2021), *report and recommendation adopted*, 2021 WL 4260665 (E.D.N.Y. Sept. 20, 2021) (holding that Microsoft was damaged under the CFAA by Defendants' "illicit activities . . . delivering ransomware, enabling attacks against other computers, and stealing online account . . . and other personal identifying information.") (citation omitted); *see also Google LLC v. Starovikov*, 2021 WL 6754263, at *2 (S.D.N.Y. Dec. 16, 2021) (finding cause to issue a preliminary injunction for violation of the CFAA, *inter alia*, where Defendant "infect[ed computers] with malware . . . to obtain information such as account credentials and URL history, which they . . . then sold to others").

**b. Defendants Knowingly and with Intent to Defraud Traffick Passwords or Similar Information in Violation of Section 1030(a)(6).**

Microsoft's code signing certificates constitute "password[s] or similar information" within the meaning of Section 1030(a)(6) because, like passwords, when presented to a computer's authorization mechanisms, they enable the Vanilla Tempest Defendants' malware to bypass security controls that would otherwise prevent unauthorized access to the computer, thus allowing the malware to run as if it were legitimate and authorized. Mason Decl. ¶¶ 5–7, 33. This interpretation is supported by the Senate Report accompanying the CFAA that observed "that a 'password' may actually be comprised of a set of instructions or directions for gaining access to a computer and [that the Committee] intends that the word 'password' be construed broadly enough to encompass both single words and longer more detailed explanations on how to access others' computers." S. Rep. No. 99-432, at 13 (1986). Courts, too. have acknowledged a broad scope of what constitutes "passwords or similar information" under the statute. *See, e.g.*, *Mobile Active Def., Inc. v. Los Angeles Unified Sch. Dist.*, 2016 WL 7444876, at *7 (C.D. Cal. Apr. 6, 2016) (finding that "a top secret, confidentially held URL" is "information similar to a password" under Section 1030(a)(6)). This understanding of "similar information" aligns with the Supreme Court's

commentary in *Van Buren v. United States* that "the CFAA's prohibition on password trafficking . . . contemplates a 'specific type of authorization—that is, authentication,' which turns on whether a user's credentials allow him to proceed past a computer's access gate[.]" 593 U.S. 374, 390 n.9 (2021) (citing Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act*, 84 Geo. Wash. L. Rev. 1442, 1470 (2016)). In practice, Microsoft's code signing certificate functions as an authentication badge, one that Fox Tempest Defendants fraudulently obtain and sell to Vanilla Tempest Defendants to affix upon their malware, which thereby gains access to the computers running Microsoft's operating system. Mason Decl. ¶¶ 6–7, 33.

That Fox Tempest Defendants trafficked these code signing certificates knowingly and with intent to defraud is evidenced by the sophisticated infrastructure they designed to serve their criminal enterprise. *Id.* ¶¶ 22–29. Through the use of Telegram, Google Forms, and managed Google Sheets, Fox Tempest Defendants solicited cybercriminals to purchase their fraudulently obtained certificates. *Id.* ¶¶ 28–29. Through cryptocurrency wallets, Fox Tempest Defendants collected difficult-to-trace payments. *Id.* ¶¶ 61–64. And through the signspace.cloud domain and virtual machines hosted by third parties, Fox Tempest Defendants provided cybercriminals with the resources to access and sign malware using Microsoft's code signing certificates. *Id.* ¶¶ 23–26. Moreover, Fox Tempest Defendants even acknowledged in their messages with Microsoft's source that the purpose of this infrastructure was to prevent detection of their fraudulent activities. *Id.* ¶ 27 (SamCodeSign admitted that Fox Tempest Defendants designed their operations to avoid "visible fraud"). Fox Tempest Defendants' trafficking affected interstate or foreign commerce because the certificates were used to sign malware that was deployed on protected computers throughout the United States. *Id.* ¶¶ 40, 65–66.

**c. Microsoft's Aggregated Losses Exceeds the CFAA's Statutory Requirement.**

Microsoft is permitted under the CFAA to bring this civil claim, because Microsoft has incurred during a one-year period a loss aggregating at least $5,000 as a result of Defendants' conduct. *Id.* ¶ 72. The CFAA defines loss as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *JBCHoldings NY, LLC v. Pakter*, 931 F. Supp. 2d 514, 523–24 (S.D.N.Y. 2013) (citing 18 U.S.C. § 1030(e)(11)). Microsoft's damages include the costs associated with "investigating and remedying damage to a computer, or a cost incurred because the computer's service was interrupted[.]" *Nexans Wires S.A. v. Sark-USA, Inc.*, 166 F. App'x 559, 563 (2d Cir. 2006). Further, the CFAA permits Microsoft to aggregate multiple intrusions or violations to meet the $5,000 statutory threshold. *Microsoft Corp. v. Does 1–2*, 2025 WL 2933087, at *8 (E.D.N.Y. Aug. 6, 2025), *report and recommendation adopted*, 2025 WL 2588793 (E.D.N.Y. Sept. 8, 2025) (holding plaintiffs "have alleged a loss well in excess of $5,000" where they "describe in detail the significant resources expended in conducting thorough investigations to identify [multiple] cracked versions of Cobalt Strike[,]" infecting "[a]t least 1.5 million computers").

To date, Defendants' malware has impacted the services of thousands of computers belonging to Microsoft and Microsoft's customers. Mason Decl. ¶¶ 40, 65–67. As at least one circuit has held, "[i]ndividuals other than the computer's owner may be proximately harmed by unauthorized access, particularly if they have rights to data stored on it." *Theofel v. Farey-Jones*, 359 F.3d 1066, 1078 (9th Cir. 2004). Microsoft retains the intellectual property rights associated with Microsoft Windows, which runs on its customers' computers and, therefore, is proximately

harmed by Defendants' deployment of malware onto them. *Id.* ¶ 69; *see WhatsApp Inc. v. NSO Grp. Techs., Ltd.*, 472 F. Supp. 3d 649, 683 & n.9 (N.D. Cal. 2020) (holding WhatsApp Inc. properly alleged injury by defendant's access to a third party's device under the CFAA because plaintiff "alleged rights to at least some data on users' devices."). As a result of Defendants' conduct, Microsoft has spent more than $1,500,000 investigating Defendants' illegal activities, revoking fraudulently obtained certificates, and remediating the damage caused by Defendants to Microsoft and its customers. Mason Decl. ¶ 72. Accordingly, Microsoft is likely to succeed on the merits of its CFAA claims.

**2. Defendants Violate the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962 *et seq.***

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 section 1962 of this chapter and may sue therefor in any appropriate United States district court and shall recover threefold the damages he sustains and the cost of the suit, including a reasonable attorney's fee[.]" 18 U.S.C. § l964(c). And this Court has "jurisdiction to prevent and restrain" such violations "by issuing appropriate orders." 18 U.S.C. § 1964(a); *see also Gingras v. Think Fin., Inc.*, 922 F.3d 112, 124 (2d Cir. 2019) ("binding Circuit precedent compels [the Court] to hold that RICO authorizes private rights of action for injunctive relief"); *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 available under RICO is intended to be broad enough to do all that is necessary") (internal quotation marks omitted); *Trane Co. v. O'Connor Sec.,* 718 F.2d 26, 29 (2d Cir. 1983) (preliminary injunction is 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 numerous predicate acts of fraud and related activity in connection with violating 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).

**a. 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, 944–45 (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.* at 946.

Defendants' racketeering enterprise has existed since June 2025, when Fox Tempest and Vanilla Tempest Defendants conspired to, and did, form an associated-in-fact racketeering enterprise with the common purpose of fraudulently obtaining, uploading, and selling access to Microsoft's code signing certificates, as well as deploying malware signed with such certificates to exploit victims by stealing their information and extorting them for financial gain. Mason Decl. ¶¶ 4, 11–12. The relationships between Fox Tempest Defendants and Vanilla Tempest Defendants are systematic and ongoing, allowing them to collectively pursue their criminal purpose as the Certificate Abuse Enterprise. *Id.* ¶ 41.

Fox Tempest Defendants and Vanilla Tempest Defendants each have specialized and indispensable roles in the Certificate Abuse Enterprise, on which the success and furtherance of the Certificate Abuse Enterprise is entirely dependent. *Id.* Fox Tempest Defendants and Vanilla Tempest Defendants leverage each other's criminal expertise and support to: (1) fraudulently obtain code signing certificates from Microsoft's Artifact Signing service through identity fraud and misrepresentation, (2) sell and distribute those certificates to known cybercriminals, (3) sign and deploy malware onto the computers of unsuspecting Microsoft customers and other members of the public, (4) gain unauthorized access to victims' computers, and (5) engage in further malicious activities, including exfiltrating sensitive personal and financial information, deploying ransomware, and extorting victims for financial gain. *Id.* ¶¶ 12–16, 30–41. Though Fox Tempest Defendants originated the scheme to fraudulently obtain Microsoft's code signing certificates, Vanilla Tempest Defendants joined the conspiracy when they purchased the certificates and began using them to conduct ransomware attacks. *Id.* ¶¶ 15, 31; *see 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 MSaaS business model with the sale and malicious deployment of Microsoft's code signing certificates at the core of the operation and will continue to do so absent the injunctive relief. Mason Decl. ¶¶ 73–74, 77.

Both the purpose of the Racketeering Enterprise and the relationship between Fox Tempest Defendants and Vanilla Tempest Defendants are proven by: (1) the dissemination of fraudulently obtained Microsoft code signing certificates; (2) the subsequent development and operation of the enterprise's internet infrastructure to proliferate ransomware attacks; and (3) the Defendants'

respective and interrelated roles in the sale, operation of, and profiting from the certificate selling scheme to further Defendants' common financial interests. *Boyle,* 556 U.S. at 947 (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.") (internal quotation marks omitted).

**b. 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. Nw. 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). Defendants have conspired to conduct and have conducted and participated in the operations of the Racketeering Enterprise through a continuous pattern of racketeering activity. Each predicate act is related to and in furtherance of the common unlawful purpose shared by the members of the Racketeering Enterprise. These acts are ongoing and will continue until this Court grants Microsoft's request for a temporary restraining order.

Defendants' racketeering acts include persistent violations of the Computer Fraud and Abuse Act, including Section 1030(a)(5)(A), which is incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(G) and 18 U.S.C. § 2332b(g)(5)(B). Section 1030(a)(5)(A) prohibits the knowing transmission of a program, information, code, or command that intentionally causes damage without authorization to a protected computer. A "protected computer" is a computer "used in or affecting interstate or foreign commerce or communication." *See United States v. Gasperini*, 2017 WL 2399693, at *3 (E.D.N.Y. June 1, 2017). This definition encompasses any

computer with an internet connection. *See United States v. Yücel*, 97 F. Supp. 3d 413, 418–19 (S.D.N.Y. 2015) (collecting cases and observing "widespread agreement in the case law" that "protected computer" includes any internet-connected computer). Each of the victims' computers that Defendants attempted to infiltrate through the MSaaS scheme meets the definition of a protected computer. These computers were then damaged within the meaning of the CFAA by Defendants' fraudulent—and therefore unauthorized—access. *See Sewell v. Bernardin*, 795 F.3d 337, 340 (2d Cir. 2015) (holding "damage" is "defined as 'any impairment to the integrity or availability of data, a program, a system, or information.'") (quoting 18 U.S.C. § 1030(e)(8)). Impacted customers have experienced substantial financial, reputational, and emotional harm, including the theft of sensitive business, personal, and financial information, the theft of credentials that can be used for further intrusions, the deployment of ransomware that encrypts their files and renders their computers unusable, extortion by Vanilla Tempest Defendants, and significant operational downtime. Mason Decl. ¶¶ 15, 37, 67.

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

*Existence of a scheme to defraud.* Defendants' modus operandi is to defraud Microsoft with the express aim of deploying malware onto the computers of Microsoft's end users. Mason Decl. ¶¶ 4, 16. Fox Tempest Defendants commit fraud by faking their credentials and other information to obtain Microsoft's code signing certificates; Vanila Tempest Defendants commit

fraud by using Microsoft's code signing certificates to pass their malware off as legitimate Microsoft programs to gain entry and access to their victims' computers. *Id.* ¶¶ 17, 21, 32–37.

*Knowing participation in scheme.* Defendants' knowledge is clear from the structure and operation of their scheme. *Id.* ¶¶ 16, 27. Defendants knowingly provide false identification information to circumvent Microsoft's entity and identity validation requirements to fraudulently obtain and sell Microsoft's code signing certificates. *Id.* ¶ 21. The certificates then allow Defendants to bypass the controls in the Windows operating system, which would otherwise flag or block Defendants' malware. *Id.* ¶¶ 6–7, 33. The interdependent steps of this process shows that Defendants' actions are knowing and intentional. *Id.* ¶ 41.

*Use of wire communication in interstate commerce to further the scheme.* Defendants operate through infrastructure spanning multiple countries—including servers in Germany, Estonia, and the United States—and use wire communications, including Telegram messaging and the internet, to market, sell, and deliver fraudulently obtained code signing certificates to customers located across the United States and globally. *Id.* ¶ 28. The Vanilla Tempest Defendants subsequently distribute signed malware to victims located across the United States through malvertising, SEO poisoning, and deceptive download pages. *Id.* ¶¶ 9, 35–36. These wire transmissions resulted not only in defrauding victims into downloading malware onto their computers, but also allowed Defendants to receive monetary benefits through the sale of the fraudulently obtained code signing certificates.

**c. Microsoft's Injury Is a Direct Result of Defendants' Racketeering Activity.**

Microsoft has been directly harmed as a result of Defendants' conduct. *Id.* ¶¶ 67–72. Microsoft has suffered damage to its brands and reputation, customers have been deceived and defrauded, and Microsoft has incurred significant damages and costs to investigate and remediate

the harm caused by Defendants. *Id.* In October 2025 alone, Microsoft investigated and revoked more than 200 certificates that Vanilla Tempest Defendants fraudulently obtained and used to perpetrate attacks. *Id.* ¶ 38. As such, "there [is] a direct relationship between [the] injury and [Defendants'] injurious conduct" and "the RICO violation was the but-for (or transactional) cause of injury." *UFCW Local 1776 v. Eli Lilly & Co.*, 620 F.3d 121, 132 (2d Cir. 2010) (citing *Holmes v. Sec. Investor Prot. Corp.*, 503 U.S. 258, 268 (1992)). As such, Microsoft is likely to succeed on the merits of its RICO claim.

**3. Defendants' Conduct Violates the Lanham Act.**

Microsoft has valid, incontestable U.S. trademark registrations for "Microsoft" and "Microsoft Teams," which are unmistakable identifiers of Microsoft's high-quality, effective, and trusted products and services. *See* Compl. App. A. "The purpose of trademark law is to protect the public from confusion as to the source of goods and to protect the trademark holder from misappropriation of its mark." *Fourth Toro Family Ltd. P'ship v. PV Bakery, Inc.*, 88 F. Supp. 2d 188, 195 (S.D.N.Y. 2000) (citing *Sterling Drug, Inc. v. Bayer AG*, 14 F.3d 733, 740 (2d Cir. 1987)). Defendants' willful and knowing misuse of Microsoft's trademarks subverts the fundamental purpose of trademark use, by misleading consumers about the safety and origin of Vanilla Tempest Defendants' and cybercriminals' malware. Microsoft is well known in the world as a leading computer company with excellent products and product safety. Indeed, "it is beyond dispute that the general public regularly interacts with Microsoft and Windows operating systems." *Microsoft Corp.*, 2025 WL 2933087, at *8. A consumer's ability to trust the hallmark quality, security, and reliability of the Microsoft brand is precisely what trademark law seeks to protect. As the Second Circuit held, "[t]he core purpose of trademark law is to prevent competitors from copying those aspects of a product [that] afford[] consumers a low-cost means of identifying the source of goods[.]") *Wallace Int'l Silversmiths, Inc. v. Godinger Silver Art Co.*, 916 F.2d 76, 78 (2d Cir.

1990), *cert. denied*, 499 U.S. 976 (1991). Indeed, the Lanham Act authorizes a Court to issue injunctive relief "according to the principles of equity and upon such terms as the court may deem reasonable," to prevent violations of trademark law. 15 U.S.C. § 1116(a). As such, Defendants' enterprise of fraudulently obtaining and affixing Microsoft's code signing certificates to malware to deceive consumers familiar with the "Microsoft" or "Microsoft Teams" trademark constitutes willful trademark infringement, false designation of origin, and trademark dilution, all with a devastating impact on the consuming public.

**a. Defendants Commit Willful Trademark Infringement under 15 U.S.C § 1114(1)..**

A defendant commits trademark infringement under Section 32 of the Lanham Act, 15 U.S.C. § 1114(1)(a), when they "(1) without consent, (2) use[] in commerce, (3) a reproduction, copy or colorable imitation of plaintiff's registered mark, as part of the sale or distribution of goods or services and (4) that such a use is likely to cause confusion." *Gruner + Jahr USA Publ'g v. Meredith Corp.*, 991 F.2d 1072, 1075 (2d Cir. 1993). Microsoft never consented to Defendants' use of its trademarks: Defendants use the Microsoft®-branded certificates to sign and distribute malware; Vanilla Tempest Defendants further disguise their malware as legitimate Microsoft Teams software, going as far as creating a fraudulent installer files named "MSTeamsSetup.exe" and hosting them on intentionally misleading domains such as "teams-download[.]buzz," "teams-install[.]run," and "teams-download[.]top." Mason Decl. ¶ 36. These sham download pages mimic legitimate Microsoft Teams websites and display Microsoft's trademarks, "Microsoft" and "Microsoft Teams." *Id.* This conduct causes consumer confusion as to the origin, sponsorship, or approval of the malware, which has both the outward appearance of a legitimate "Microsoft Teams" product, and is signed to imply that none other than "Microsoft" endorses the safety of the program.

The Second Circuit's eight-factor test for assessing likelihood of confusion[2] overwhelmingly favors Microsoft. Regarding the first factor, Microsoft's mark is "presumed to be strong by virtue of being registered." *Juul Labs, Inc. v. EZ Deli Grocery Corp I*, 2022 WL 1085406, at *5 (E.D.N.Y. Feb. 10, 2022), *report and recommendation adopted*, 2022 WL 819152 (E.D.N.Y. Mar. 18, 2022). Regarding the second factor, the marks are identical, as is shown by Figure 3 to the declaration of Mr. Mason filed in support of this application for temporary restraining order. Because the Defendants deliberately design their malware download pages to appear identical to Microsoft's legitimate Microsoft Teams download page, the third factor favors Microsoft in light of these bad faith actions of the Defendants, even though Defendants' malware does not technically approximate Microsoft's product. The fourth factor likewise "is irrelevant here given that Defendants have created counterfeit versions of [Microsoft's] marks and consumers are not purchasing them in any marketplace." *Microsoft Corp.*, 2025 WL 2933087, at *7. As to the fifth factor, it is "black letter law that actual confusion need not be shown to prevail under the Lanham Act, since actual confusion is very difficult to prove and the Act requires only a likelihood of confusion as to source." *Guthrie Healthcare Sys. v. ContextMedia, Inc.*, 826 F.3d 27, 45 (2d Cir. 2016). The fact that more than 200 certificates have been used by Vanilla Tempest Defendants in fake Microsoft Teams setup files and that these numbers contribute to the thousands of machines in the United States alone that have been impacted by malware signed with fraudulent certificates clearly demonstrates actual consumer confusion. Mason Decl. ¶¶ 38–40. The imitative

[2] The elements of this test are: "(1) strength of the trademark; (2) similarity of the marks; (3) proximity of the products and their competitiveness with one another; (4) evidence that the senior user may 'bridge the gap' by developing a product for sale in the market of the alleged infringer's product; (5) evidence of actual consumer confusion; (6) evidence that the imitative mark was adopted in bad faith; (7) respective quality of the products; and (8) sophistication of consumers in the relevant market." *Starbucks Corp. v. Wolfe's Borough Coffee, Inc.*, 588 F.3d 97, 115 (2d Cir. 2009) (citing *Polaroid Corp. v. Polarad Elecs. Corp.*, 287 F.2d 492 (2d Cir. 1961)).

marks were adopted in bad faith, satisfying factor six, because Defendants have used them to disguise harmful malware as legitimate Microsoft products. Factor seven tips in Microsoft's favor, because the quality of Microsoft's legitimate version of Microsoft Teams is obviously what consumers are seeking, rather than malware that "enables malicious cyber actors to gather system information, extract credentials, issue commands, deploy additional malware (including ransomware), and ensure ongoing access to infected [computers.]" Mason Decl. ¶ 32. As for factor eight, the sophistication of consumers in the relevant market, even those sophisticated consumers that compose Microsoft's global consumer base face difficulty contending with Defendants' sophisticated efforts to subvert a "critical trust mechanism in modern computing operating systems by obtaining and misusing valid signing certificates to mask dangerous malware as trusted software." *Id.* ¶ 8.

Ultimately, the "application of the *Polaroid* [eight-factor] test is 'not mechanical, but rather, focuses on the ultimate question of whether, looking at the products in their totality, consumers are likely to be confused.'" *Starbucks Corp.*, 588 F.3d at 115 (quoting *Star Indus., Inc. v. Bacardi & Co.*, 412 F.3d 373, 384 (2d Cir. 2005)). Vanilla Tempest Defendants' conduct clearly causes consumer confusion, because their deception relies and trades upon the extensive goodwill and reputation that Microsoft has built with its consumer base through years of providing excellent services and products, thus infringing upon Microsoft's trademarks in violation of the Lanham Act.

Fox Tempest Defendants are also contributorily liable for the acts of trademark infringement committed by Vanilla Tempest Defendants. "To state a claim for contributory trademark infringement, a plaintiff must allege that defendant either (1) intentionally induced another to infringe a trademark or (2) continued to supply its product or service to one whom it

knew or had reason to know was engaging in trademark infringement." *King Spider LLC v. 884886 CH Store*, 2024 WL 3184674, at *1 (S.D.N.Y. June 26, 2024) (quoting *Lopez v. Bonanza.com, Inc.*, 2019 WL 5199431, at *14 (S.D.N.Y. Sept. 30, 2019)). Where "a plaintiff alleges a service provider's contributory liability, it is required to allege that said service provider had more than a general knowledge or reason to know that its service is being used to [infringe a trademark], and sufficient control over infringing activity to merit liability." *Id. (*quoting *Lopez*, 2019 WL 5199431, at *14).

Fox Tempest Defendants intentionally invite bad actors to purchase their product, namely, fraudulently obtained Microsoft code signing certificates. Vendors of valid products can directly obtain such certificates from Microsoft itself, but the Fox Tempest Defendants are clearly aware that their clients and collaborators cannot do the same. Fox Tempest Defendants thus "had more than a general knowledge or reason to know" its services would be used to engage in trademark infringement. Indeed, their entire business model centers around helping criminals bypass the security features built into the Windows operating system by equipping their malware with fraudulently obtained certificates. In fact, when Fox Tempest Defendants moved their infrastructure from signspace.cloud to Cloudzy, the latter was preferable "so there won't be [*i.e.*, to mask] visible fraud." Mason Decl. ¶ 27 (SameCodeSign, a Fox Tempest Defendant, explaining their preference for using Remote Desktop Protocol over a website). As such, Fox Tempest Defendants' conduct, at the very least, clearly constitutes contributory trademark infringement.

**b. Defendants Commit Willful False Designation of Origin under 15 U.S.C. § 1125(a).**

"[I]t is well settled that the standards for false designation of origin claims under Section 43(a) of the Lanham Act (15 U.S.C. § 1125) are the same as for trademark infringement claims under Section 32 (15 U.S.C. § 1114)." *Twentieth Century Fox Film Corp. v. Marvel Enters.,*

*Inc.*, 220 F. Supp. 2d 289, 297 (S.D.N.Y 2002); *see also Morningside Grp. Ltd. v. Morningside Cap. Grp., L.L.C.*, 182 F.3d 133, 137 (2d Cir. 1999) (To establish a claim of false designation of origin, a plaintiff must establish that "it has a valid mark entitled to protection and that the defendant's use of it is likely to cause confusion."). Accordingly, for the same reasons as above for trademark infringement, Defendants in tandem have willfully committed false designation of origin by fraudulently obtaining and using Microsoft-branded certificates to sign malware. By distributing malware disguised as legitimate Microsoft products, Defendants deliberately create an association between Microsoft and the malware, causing significant consumer confusion by suggesting Microsoft approves or sponsors a malicious program that appears to be a legitimate "Microsoft Teams" product. *See Microsoft Corp. v. AGA Sols., Inc.*, 589 F. Supp. 2d 195, 203 (E.D.N.Y. 2008) (granting summary judgment to Microsoft because "[t]he same facts that establish that [Plaintiffs] violated section 32 of the Lanham Act establish that they violated section 43(a) by falsely designating the origin of the software they sold").

**c. Defendants Commit Willful Trademark Dilution under 15 U.S.C. § 1125(c).**

Dilution by tarnishment is an "association arising from the similarity between a mark or trade name and a famous mark that harms the reputation of the famous mark." 15 U.S.C. § 1125(c)(2)(C). This form of dilution "generally arises when the plaintiff's trademark is linked to products of shoddy quality, or is portrayed in an unwholesome or unsavory context likely to evoke unflattering thoughts about the owner's product." *Tiffany (NJ) Inc. v. eBay, Inc.*, 600 F.3d 93, 111 (2d Cir. 2010) (quoting *Deere & Co. v. MTD Prods., Inc.*, 41 F.3d 39, 43 (2d Cir. 1994)). Microsoft's trademarks have been tarnished by Defendants' unauthorized use of them in conjunction with proliferating malware disguised as Microsoft Teams. "When products attributed to Microsoft are used in connection with cybercrime, customers will mistakenly believe Microsoft

is responsible for the attack. Customers subjected to the negative effects of Defendants' activities sometimes incorrectly believe Microsoft is the source of the problem and thus will incorrectly attribute these problems to Microsoft and associate these problems with Microsoft's products and services." Mason Decl. ¶ 71. Further, Defendants use Microsoft's trademarks "in commerce" as part of their commercial enterprise to trade upon the extensive consumer goodwill, reputation, and fame of goods and services associated with "Microsoft" and "Microsoft Teams." 15 U.S.C. § 1125(c)(1). As the owner of the famous "Microsoft" and "Microsoft Teams" marks, Microsoft is likely to succeed on the merits of this claim and "shall be entitled to an injunction against another person" who uses the mark in a way "that is likely to cause dilution by blurring or dilution by tarnishment of the famous mark…." *Id.*

**4. Defendants' Conduct Violates New York Law**.

**a. Breach of Contract (Fox Tempest Defendants)**

"The essential elements of a cause of action to recover damages for breach of contract are (1) the existence of an enforceable contract, (2) the plaintiff's performance pursuant to that contract, (3) the defendant's breach of the contract, and (4) damages resulting from that breach." *Nassau Operating Co., LLC v. DeSimone*, 206 A.D.3d 920, 926 (2d Dep't 2022).

Microsoft's Terms of Use for Artifact Signing ("Terms of Use") is an enforceable contract that governs the access and use of Microsoft's Artifact Signing service. Fox Tempest Defendants accepted and became bound by Microsoft's Terms of Use when they created tenants and accessed the Artifact Signing service. Mason Decl. ¶ 18. The Terms of Use is available and incorporated into the Complaint as **Exhibit 1**.

Under the Terms of Use, users make a series of representations and warranties to Microsoft and to any party who may rely on a certificate issued to them. Users represent and warrant that "all the Submitted Information and all representations [user] makes to Microsoft in any Services

[including Artifact Signing] applications are accurate." Terms of Use § 2(b). Further, "the Submitted Information (including the email address of [user's] personnel who submitted such information, if applicable) has not been and will not be used for any unlawful purpose." *Id.* "[I]f the Submitted Information or the representations [the user] made to Microsoft in any Services application changed or is no longer valid[,]" the user is bound to "inform Microsoft[.]" *Id.* Critically, users agree to "use the Services exclusively for authorized and legal purposes consistent with this [Terms of Use.]" *Id.*

Users must agree to use Artifact Signing in accordance with the Code of Conduct, which specifically prohibits users from "us[ing] 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; (iii) help others send unsolicited bulk email, postings, or instant messages; (iv) publicly display inappropriate images; (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 …." *Id*. § 2(g).

Fox Tempest Defendants materially breached the Terms of Use by, among other things: (1) submitting false and fraudulent information to Microsoft in connection with the service, including fake identifying information and fraudulent business registration documents; (2) using the service for unlawful purposes, including to facilitate the sale of code signing certificates to cybercriminals; (3) engaging in illegal activity, false or misleading activity, and activity that harms Microsoft and others; (4) enabling access to the service by unauthorized third parties; and (5) failing to investigate malicious activity they had awareness of.

As a result of Fox Tempest Defendants' breach of contract, Microsoft incurred damages including but not limited to reputational harm and the costs of investigating Fox Tempest Defendants' activities and revoking fraudulently obtained certificates. Mason Decl. ¶¶ 68, 72.

Accordingly, all the elements of a breach of contract are met and Microsoft is likely to succeed on the merits of this claim.

**b. Trespass to Chattels (Fox Tempest Defendants)**

Under New York law, a "trespass to chattel occurs when a party intentionally damages or interferes with the use of property belonging to another." *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 437 (2d Cir. 2004). "Traditionally, courts have drawn a distinction between interference by dispossession, which does not require a showing of actual damages, and interference by unauthorized use or intermeddling which requires a showing of actual damages." *Fischkoff v. Iovance Biotherapeutics, Inc.*, 339 F. Supp. 3d 408, 416 (S.D.N.Y. 2018). "Interference with information stored on a computer may give rise to trespass to chattel if plaintiff is dispossessed of the information or the information is impaired as to its condition, quality or value." *Hecht v. Components Int'l, Inc.*, 22 Misc. 3d 360, 370 (N.Y. Sup. Ct., Nassau Cnty. 2008).

Fox Tempest Defendants trespassed upon Microsoft's computer systems when they accessed without authorization, and exceeded their authorized access to, Microsoft's Artifact Signing service, a proprietary Microsoft cloud-based code signing platform, and created more than 580 Microsoft tenants using false identifying information and otherwise acted in violation of the Terms of Use described above. Mason Decl. ¶¶ 17, 21. As a result of their unauthorized access and use of the service, Fox Tempest Defendants obtained code signing certificates to which they were not entitled. *Id.*; Compl. ¶ 139. Similar to *Register.com, Inc. v. Verio, Inc.*, where the Second Circuit affirmed the district court's preliminary injunction enjoining the defendant from using a search robot to access the plaintiff company's computer systems without authorization, Fox Tempest Defendants' unauthorized access harmed Microsoft's systems by "consuming the computer systems' capacity." *Register.com, Inc.*, 356 F.3d at 438; Compl. ¶ 141 ("John Does 1–2 consumed Microsoft's computing resources without authorization by fraudulently accessing the

Artifact Signing service and utilizing Microsoft's cloud infrastructure to generate code signing certificates."). As the Second Circuit held, "computer systems are valuable resources of finite capacity [and the] unauthorized use of such systems depletes the capacity available to authorized end-users[.]" *Register.com, Inc.*, 356 F.3d at 438; *cf. Sch. of Visual Arts v. Kuprewicz,* 3 Misc. 3d 278, 281–82 (N.Y. Sup. Ct., N.Y. Cnty. 2003) (trespass action viable where there are allegations of "depleted hard disk space, drained processing power, [or when the conduct] adversely affected other system resources"). Accordingly, Microsoft is likely to succeed in its trespass to chattels claim.

**c. Unjust Enrichment (Vanilla Tempest Defendants)**

Unjust enrichment is "a New York common law quasi-contract cause of action requiring the plaintiff to establish: (1) that the defendant benefitted; (2) at the plaintiff's expense; and (3) that equity and good conscience require restitution." *Myun-Uk Choi v. Tower Rsch. Cap. LLC*, 890 F.3d 60, 69 (2d Cir. 2018).

Unjust enrichment "contemplates 'an obligation imposed by equity to prevent injustice, in the absence of an actual agreement between the parties.'" *Georgia Malone & Co. v. Rieder*, 19 N.Y.3d 511, 516 (2012) (citation omitted). Vanilla Tempest Defendants, though not party to the Terms of Use that governs the use of Microsoft's Artifact Signing service, nevertheless benefited at Microsoft's expense by illegally obtaining Microsoft's code signing certificates through Fox Tempest Defendants, their partners in Certificate Abuse Enterprise. Mason Decl. ¶¶ 15, 31. Vanilla Tempest Defendants were aware of their actions and of the benefit they derived from their unauthorized use of Microsoft's code signing certificates, which they exploited to sign malware and conduct ransomware attacks on Microsoft's customers. *Id.* ¶¶ 15, 32–37. Equity and good conscience require Vanilla Tempest Defendants to disgorge the profits they unjustly reaped from their malfeasance, including through ransomware and extortion payments. *Id.* ¶¶ 15, 37, 64. The

facts here present precisely one of those "unusual situations when, though the defendant has not breached a contract nor committed a recognized tort, circumstances create an equitable obligation running from the defendant to the plaintiff," and Microsoft is therefore likely to succeed on the merits of this claim. *Corsello v. Verizon N.Y., Inc.*, 18 N.Y.3d 777, 790 (2012).

**B. Defendants Cause Irreparable Harm.**

It is well established in this Circuit that consumer confusion and injury to business goodwill constitute irreparable harm. *See Tom Doherty Assocs. v. Saban Entm't, Inc.*, 60 F.3d 27, 37–38 (2d Cir. 1995) (recognizing that the loss of prospective business or goodwill supports a finding of irreparable harm); *Broker Genius, Inc. v. Volpone*, 313 F. Supp. 3d 484, 496 (S.D.N.Y. 2018) (same). Defendants' actions have inflicted direct and severe harm on Microsoft in this manner.

First, by creating more than 580 fraudulent Artifact Signing tenants using false information, Fox Tempest Defendants have undermined the integrity of Microsoft's Artifact Signing service and damaged Microsoft's reputation and the goodwill of its associated trademarks. Mason Decl. ¶¶ 68–69. The Artifact Signing service is designed to provide a secure, verified chain of trust between software developers, Microsoft, and end users. *Id.* ¶¶ 5, 17. Defendants knowingly circumvented verification procedures by creating accounts with false identifying information and then used the resulting certificates to sign malware in violation of the Artifact Signing service's Terms of Use. *Id.* ¶¶ 17, 21. This conduct deceives Microsoft customers into believing that malicious software is legitimate and trustworthy, thereby harming the value of Microsoft's Artifact Signing service and damaging the goodwill associated with its trademarks. *Id.* ¶¶ 70–71.

Second, Vanilla Tempest Defendants' conduct has caused similar reputational harm through their abuse of Microsoft's brands more broadly. *Id.* ¶¶ 68–71. John Does 3–4 leveraged falsely named Microsoft Teams setup files hosted on domains designed to mimic Microsoft's registered marks and domains. *Id.* ¶ 36. Similar to the abuse of the Artifact Signing service, when

Microsoft customers download what they believe to be legitimate Microsoft software and instead receive malware, those customers associate the resulting harm with Microsoft and its products, causing further damage to Microsoft's brands and the goodwill associated therewith. *Id.* ¶ 71.

Microsoft has expended significant resources to investigate the abuse of its Artifact Signing service, identify the fraudulent tenants created by Fox Tempest Defendants, revoke the certificates used to sign malware, and implement additional safeguards to prevent future abuse. *Id.* ¶ 72. Additionally, Microsoft has investigated and worked to remediate the damages caused by the abuse of its Microsoft Teams brand. *Id.* ¶¶ 38, 70, 72. In October 2025 alone, Microsoft investigated and revoked more than 200 certificates that John Does 3–4 fraudulently obtained and used to perpetrate attacks. *Id.* ¶ 38. Microsoft has expended significant resources—more than $1,500,000—to investigate and track the Defendants' illegal activities and to counter and remediate the damage caused by Defendants to Microsoft and its customers. *Id.* ¶ 72.

Defendants' actions have also inflicted direct and severe harm on Microsoft and Microsoft's customers. *Id.* ¶ 67. To date, Microsoft has identified thousands of machines in the United States, including machines owned by Microsoft, that have been impacted by malware signed with certificates originating from the fraudulent tenants created by Fox Tempest Defendants. *Id.* ¶¶ 40, 67. Impacted customers have experienced substantial harm, including the theft of sensitive business, personal, and financial information, the theft of credentials that can be used for further intrusions, the deployment of ransomware that encrypts their files and renders their computers unusable, the extortion by Vanilla Tempest Defendants, and significant operational downtime. *Id.* ¶¶ 15, 37, 67.

These injuries are sufficient in and of themselves to constitute irreparable harm. In addition, Defendants have caused and may continue to cause monetary harm for which Microsoft will not

be compensated—even after final judgment—because Defendants are elusive cybercriminals against whom Microsoft is unlikely to enforce a judgment. *Cf. CRP/Extell Parcel I, L.P. v. Cuomo*, 394 F. App'x 779, 781 (2d Cir. 2010) ("[W]e have held that a finding of irreparable harm may lie in connection with an action for money damages where the claim involves an obligation owed by an insolvent or a party on the brink of insolvency.").

**C. Balance of Equities Strongly Favors Injunctive Relief.**

Because Defendants have no legitimate interest in committing cybercrime in violation of U.S. laws, Defendants will suffer no harm to any legitimate interest should a temporary restraining order and preliminary injunction be issued. Rather, the balance of equities in this situation tip sharply in favor of granting an injunction to prevent Defendants from continuing their illegal scheme to defraud customers and injure Microsoft. *See, e.g.*, *N. Atl. Operating Co., Inc. v. Evergreen Distribs., LLC*, 2013 WL 5603602, at *13 (E.D.N.Y. Sept. 27, 2013) ("Where '[t]he only hardship to Defendant from [an] injunction would be to prevent him from engaging in further illegal activity, [] the balance clearly weighs in Plaintiffs' favor.'" (quoting *DISH Network L.L.C. v. DelVechhio*, 831 F. Supp. 2d 595, 601–02 (W.D.N.Y. 2011)). The irreparable harm suffered by Microsoft, its customers, and the general public and the real possibility of continued harm substantially outweighs Defendants' interests in continuing their criminal enterprise.

**D. Public Interest Favors Injunctive Relief.**

An injunction here can only serve the public interest. Each day, Defendants sell illegally obtained certificates to allow more bad actors to defraud members of the public and steal more information from the accounts and computers of innocent victims. Public interest is served by enforcing statutes specifically designed to protect the public, such as the CFAA, RICO, and the Lanham Act. *FXDirectDealer, LLC v. Abadi*, 2012 WL 1155139, at *8 (S.D.N.Y. Apr. 5, 2012) (holding that public interest weighed in favor of an injunction to enforce CFAA); *Google LLC*,

2021 WL 6754263, at *4 (holding "the public interest is clearly served by enforcing statutes designed to protect the public, such as RICO"); *Juicy Couture, Inc. v. Bella Int'l Ltd.*, 930 F. Supp. 2d 489, 505 (S.D.N.Y. 2013) (holding the grant of a preliminary injunction under the Lanham Act would not disserve the public interest, where there was a strong interest in preventing public confusion over parties' competing trademarks).

Numerous federal courts have granted requests for injunctive relief to disable the instrumentalities of cybercrime, such as those used by Defendants here. *See, supra* note 1. The same result is warranted here.

## V. THE ALL WRITS ACT AUTHORIZES THE COURTS TO DIRECT A THIRD PARTY TO PERFORM THE NECESSARY ACTS TO AVOID FRUSTRATION OF THE REQUESTED RELIEF.

To effectuate the TRO, Microsoft's Proposed Order requires the reasonable cooperation of third-party registrar GoDaddy and virtual machine provider Cloudzy, whose infrastructures Defendants rely on to further their schemes. Mason Decl. ¶¶ 24, 26, 73. GoDaddy and Cloudzy are the primary entities identified thus far in the United States that can disable the signspace.cloud and virtual machine infrastructure and their cooperation is therefore essential to the effective execution of injunctive relief. *Id.* ¶¶ 73–74.

Microsoft respectfully requests that the Court direct GoDaddy and Cloudzy to reasonably cooperate with the execution of the temporary restraining order 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 held that narrow direction to third parties is sometimes necessary to effect the implementation of a court order and such direction 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. N.Y. Tel. Co*., 434 U.S. 159, 174 (1977) (citations omitted); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, at *30 (Jan. 6, 2014) (invoking All Writs act and granting relief similar to that requested here).

There are three threshold requirements to invoking the All Writs Act: (1) issuance of the writ must be "in aid of" the issuing court's jurisdiction; (2) the type of writ requested must be "necessary or appropriate" to provide such aid to the issuing court's jurisdiction; and (3) the issuance of the writ must be "agreeable to the usages and principals of law." *In re Apple, Inc.*, 149 F. Supp. 3d 341, 350–51 (E.D.N.Y. 2016). Microsoft has met these threshold factors.

*First*, this action is commenced under various federal statutes—the Lanham Act, the Computer Fraud and Abuse Act, and the Racketeer Influenced and Corrupt Organizations Act. Thus, this Court "unquestionably has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331, and, therefore, has jurisdiction to issue the requested [All Writs Act] Order." *United Spinal Ass'n v. Bd. of Elections in City of N.Y.*, 2017 WL 8683672, at *5 (S.D.N.Y. Oct. 11, 2017), *report and recommendation adopted*, 2018 WL 1582231 (S.D.N.Y. Mar. 27, 2018).

*Second*, the writ requested is "necessary or appropriate" here. As the Supreme Court stated in *New York Telephone* "'[u]nless appropriately confined by Congress, a federal court may avail itself of all auxiliary writs as aids in the performance of its duties." *N.Y. Tel. Co.*, 434 U.S. at 172–73 (citing *Adams v. United States ex rel. McCann*, 317 U.S. 269, 273 (1942)). The requested writ is necessary here because GoDaddy's signspace.cloud domain and Cloudzy's virtual machines form the lynchpin of Defendants' Certificate Abuse Enterprise by hosting and providing access to Microsoft's code signing certificates. An order enjoining the Defendants here without an order directed to the domain registrar and the host of the virtual machines identified in **Appendix B** will

leave Microsoft without relief, because there is good reason to believe the Defendants themselves, as yet beyond the reach of this Court and knowingly engaged in criminal conduct, will not themselves disable their own infrastructure or turn evidence of their crimes over to Microsoft. *See Microsoft Corp. v. Fridi*, No. 1:26-cv-01603 (S.D.N.Y. Feb. 26, 2026) (Cote, J.) (Dkt. 31) (granting a temporary restraining order with respect to third parties to seize the instrumentalities of Defendants' criminal enterprise); *Microsoft Corp. v. Ogundipe*, No. 1:25-cv-07111 (S.D.N.Y. Aug. 27, 2025) (Rakoff, J.) (Dkt. 21) (same).

*Third*, the issuance of a temporary restraining order under present circumstances also satisfies three additional factors that courts typically consider in exercising their All Writs Act authority, namely that "(1) the third party must be closely connected with the underlying controversy…; (2) the order must not adversely affect the basic interests of the third party or impose an undue burden; (3) the assistance of the third party must be absolutely necessary." *United States v. Hall*, 583 F. Supp. 717, 719 (E.D. Va. 1984) (citing *N.Y. Tel. Co.*, 434 U.S. at 174-77); *see also In re Apple, Inc.*, 149 F. Supp. 3d at 344 (reciting similar three factors). As discussed, GoDaddy and Cloudzy are closely connected with the underlying controversy because Defendants exploit GoDaddy's domain registration services and Cloudzy's virtual machine offerings to host and further their criminal enterprise. Mason Decl. ¶¶ 24, 26. The Proposed Order requires only minimal assistance from GoDaddy and Cloudzy in executing the TRO, namely the transfer of control and access of the domain, signspace.cloud, and virtual machines contemplated in **Appendix B**. GoDaddy and Cloudzy both manage the control and access of their respective services in the ordinary course of their businesses.

Further, the Proposed Order shall be implemented with the least degree of interference with the normal operations of GoDaddy and Cloudzy and will not deprive the GoDaddy or Cloudzy of

any tangible or significant property interests. If GoDaddy or Cloudzy wishes to bring an issue to the attention of the Court, Microsoft will inform the Court immediately. Further, GoDaddy and Cloudzy will have an opportunity to be heard at the preliminary injunction hearing, which the Federal Rules of Civil Procedure require to be held shortly after the execution of the Proposed Order. Fed. R. Civ. P. 65(b).

The narrow directions contemplated in the Proposed Order satisfy Due Process and are necessary to effectuate the relief requested, without which Defendants will continue to irreparably harm Microsoft, its customers, and the general public. The Proposed Order is also in line with similar relief ordered by federal courts across multiple jurisdictions under the All Writs Act. *See supra* fn. 1. "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[.]" *In re Baldwin-United Corp*., 770 F.2d 328, 338–39 (2d Cir. 1985). The exercise of that authority is appropriate here.

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

The requested temporary restraining order must issue *ex parte* to be effective. Defendants are technically sophisticated actors who would quickly relocate their infrastructure if given advance notice. Rule 65 of the Federal Rules of Civil Procedure permits an *ex parte* temporary restraining order 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) (recognizing *ex parte* temporary restraining orders are "necessary in certain circumstances").

If notice is given prior to issuance of a temporary restraining order, Defendants would likely dismantle their current infrastructure and establish alternate systems before any temporary

restraining order could have effect, rendering any remedial measures futile. Courts consistently grant *ex parte* relief in such circumstances. *See, e.g., In re Vuitton Et Fils S.A.*, 606 F.2d 1, 2–5 (2d Cir. 1979) (holding that notice prior to issuing TRO was not necessary where notice would "serve only to render fruitless further prosecution of the action" and the plaintiff's prior experience demonstrated that notifying any single member of the enterprise would prompt the relocation of contraband); *AT&T Broadband v. Tech Commc'ns, Inc.*, 381 F.3d 1309, 1319–20 (11th Cir. 2004) (affirming *ex parte* search and seizure order to seize contraband technical equipment, given evidence that in the past defendants and persons similarly situated had routinely secreted or destroyed evidence once notified of legal proceedings); *see also Microsoft Corp. v. Fridi*, No. 1:26-cv-01603 (S.D.N.Y. Feb. 26, 2026) (Dkt. 31) (Cote, J.*)* (granting *ex parte* TRO against cybercriminal phishing-as-a-service operation where advance notice would enable defendants to destroy, move, hide, or conceal the infrastructure and evidence at issue); Declaration of Adam Hickey ISO *Ex Parte* TRO Application ("Hickey Decl.") ¶ 7; Hickey Decl. Ex. 6.

Microsoft has observed in prior actions that cybercriminals routinely change or relocate infrastructure once it becomes publicly known that action will be taken. For example, when Microsoft has sought to other criminal operations, operators have attempted to move command and control infrastructure to new IP addresses, delete files from seized host servers, and activate dormant domains to maintain control over infected devices. *See, e.g.*, *Microsoft Corp. v. John Does 1–5*, No. 1:15-cv-06565 (E.D.N.Y. Nov. 23, 2015) (Dkt. 12) ("Dorkbot Botnet"); *Microsoft Corp. v. John Does 1–8*, No. 1:13-CV-1014 (W.D. Tex. Nov. 25, 2013) (Dkt. 17) ("ZeroAccess Botnet"); *Microsoft Corp. v. John Does 1–11*, No. 2:11-cv-00222 (W.D. Wa. Mar. 9, 2011) (Dkt. 19) ("Rustock Botnet"). Hickey Decl. ¶ 6. Defendants here have already taken steps to obfuscate their identities, including operating through hosting providers in multiple countries and using aliases.

Mason Decl. ¶¶ 22–27. Microsoft has every reason to believe Defendants would take similar evasive action if given notice. *Id.* ¶¶ 76–77; Hickey Decl. ¶ 6. District courts have previously granted *ex parte* relief in cases brought by Microsoft against similarly situated cybercriminal operations. *See supra* fn. 1.

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

**A. Microsoft Will Provide Notice to Defendants by Personal Delivery and through Treaty if Possible.**

Microsoft has identified infrastructure from which Defendants operate, and, pursuant to the TRO, will obtain from relevant domain registries, third-party hosting providers, and service providers any and all physical addresses of Defendants, to the extent those are available or not fictitious. Hickey Decl. ¶¶ 9, 11. Pursuant to Rule 4(e)(2)(A), Microsoft plans to effect formal notice of the preliminary injunction hearing and service of the Complaint by personal delivery of the summons, Microsoft's Complaint, the instant motion and supporting documents, and any Order issued by this Court to such addresses in the United States. *Id.* ¶ 15. If valid physical addresses of Defendants can be identified outside of the United States, Microsoft will notice Defendants and serve process upon them through the Hague Convention or similar treaty-based means pursuant to Fed. R. Civ. P. 4(f)(3). *Id.* ¶¶ 16–17.

**B. Microsoft Will Provide Notice to Defendants by Email, Facsimile, and Mail.**

Microsoft has identified email addresses, mailing addresses, and/or other contact information provided by Defendants in connection with the registration and operation of their infrastructure, and Microsoft will seek to identify additional contact information pursuant to the terms of the requested TRO. *Id.* ¶¶ 11–12. Microsoft 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 Defendants provided to the registrars and registries. *Id.* ¶¶ 12–13. When Defendants registered for domain names, they agreed that notice of disputes regarding hosting could be provided to them by sending complaints to the email, facsimile and mail addresses they provided. *Id.* ¶¶ 30–36. Additionally, Fox Tempest Defendants used email addresses in connection with the creation of their fraudulent Microsoft tenants, and thus have agreed that notice of disputes regarding their use of such services could be provided to them by sending complaints to the contact information they provided. *Id.*. ¶¶ 18–24.

**C. Microsoft Will Provide Notice to Defendants by Publication.**

Microsoft will notify Defendants of the preliminary injunction hearing and the Complaint by publishing the materials on a centrally located, publicly accessible source on the internet. *Id.* ¶ 13.

**D. Microsoft's Proposed Methods of Service Satisfy Due Process.**

The proposed methods of notice and service described above comport with due process, represent reasonable and appropriate means to notify Defendants of this action, and are warranted given the circumstances of this case. Constitutional due process requires only that service of process provide notice "reasonably calculated, under all the circumstances, to apprise interested parties of the pendency of the action and afford them an opportunity to present their objections." *Elsevier, Inc. v. Siew Yee Chew*, 287 F. Supp. 3d 374, 379 (S.D.N.Y. 2018) (citing *Mullane v. Cent. Hanover Bank & Trust Co.*, 339 U.S. 306, 314 (1950)). Microsoft therefore requests that the Court authorize the alternative service methods described above.

Legal notice and service by e-mail, facsimile, mail, and publication satisfies due process because these methods are reasonably calculated under the circumstances to apprise the interested

parties of the TRO, the preliminary injunction hearing, and the lawsuit. Federal Rule of Civil Procedure 4(f)(3) permits service by means not prohibited by international agreement, and courts have repeatedly authorized similar alternative service methods against international defendants who seek to evade accountability. *Microsoft Corp. v. Does 1–18*, 2014 WL 1338677, at *3 (E.D. Va. Apr. 2, 2014) (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 [infrastructure]" and published the same information at the publicly available website www.noticeofpleadings.com) (citing Fed. R. Civ. P. 4(f)(3)); *Payne v. McGettigan's Mgmt. Servs. LLC*, 2019 WL 6647804, at *1 (S.D.N.Y. Nov. 19, 2019) (noting that courts have found various alternative methods of service, including email, appropriate); *Elsevier, Inc.*, 287 F. Supp. 3d at 379–80 (finding that in trademark infringement action, proposed means of service on foreign defendants via email satisfied due process).

Here, the e-mail addresses Defendants provided when registering their infrastructure represent the most reliable means of contact. To activate their Azure subscriptions, Fox Tempest Defendants were required to click on a verification email sent by Microsoft; they also used these e-mail addresses for multi-factor authentication to access their Azure accounts. Mason Decl. ¶ 20. In addition, when Defendants registered for the domain names of their websites, they agreed to provide reliable contact information and agree to accept notice of hosting-related disputes through the contact information, including email, provided by them. Hickey Decl. ¶¶ 30, 34–36. Defendants should anticipate receiving dispute-related communications through these channels, as their agreements with service providers authorize such contact. *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."). E-mail and publication service are therefore both warranted and necessary.

Alternative service is particularly warranted in cases such as this involving internet-based misconduct, carried out by international defendants, causing immediate, irreparable harm. *See, e.g.*, *Rio Props., Inc. v. Rio Int'l. Interlink*, 284 F.3d 1007, 1018 (9th Cir. 2002) ("If any method of communication is reasonably calculated to provide [Defendant operating online] with notice, surely it is email—the method of communication which [Defendant] utilizes and prefers."). *Rio Properties* has been followed in the Second Circuit. *See Payne*, 2019 WL 6647804, at *1; *Elsevier, Inc.*, 287 F. Supp. 3d at 379–80.

Moreover, if Defendants' physical addresses prove fictitious and their actual locations remain unknown, the Hague Convention would not apply, further supporting the appropriateness of alternative service. *Kelly Toys Holdings, LLC. v. Top Dep't Store,* 2022 WL 3701216, at *5 (S.D.N.Y. Aug. 26, 2022) ("the Hague Convention does not apply here, because defendants' physical address was unknown to plaintiffs despite reasonably diligent efforts to learn it").

For these reasons, Microsoft respectfully requests that the Court find the proposed methods of notice and service satisfy Fed. R. Civ. P. 4(f)(3) and due process, and are reasonably calculated to apprise Defendants of this action.

## VII. CONCLUSION

For the reasons set forth herein, Microsoft respectfully requests that this Court grant its Emergency *Ex Parte Application for* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction.

Dated: May 4, 2026

Respectfully submitted,

MAYER BROWN LLP

Adam S. Hickey
David J. Lizmi
MAYER BROWN LLP
1221 Avenue of the Americas
New York, NY 10020
Tel: (212) 506-2500
Fax: (212) 262-1910
Email: *ahickey@mayerbrown.com*
*dlizmi@mayerbrown.com*

Sasha L. Keck
Christina Luk (*pro hac vice forthcoming*)
Aaron J. Futerman (*pro hac vice forthcoming*)
Tanner L. Wilburn (*pro hac vice forthcoming*)
MAYER BROWN LLP
1999 K Street, NW
Washington, DC 20006
Tel: (202) 263-3000
Fax: (202) 263-3300
Email: *skeck@mayerbrown.com*
*cluk@mayerbrown.com*
*afuterman@mayerbrown.com*
*twilburn@mayerbrown.com*

*Attorneys for Plaintiff Microsoft Corporation*

**CERTIFICATION PURSUANT TO LOCAL RULE 7.1(c)**

The total number of words in the foregoing Memorandum of Law, including point headings and footnotes, and excluding the caption, Table of Contents, Table of Authorities, signature block, and certifications is 13,006 words. Concurrently with this Memorandum of Law, Microsoft files a motion for leave to exceed word count.

Adam S. Hickey