IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

MICROSOFT CORPORATION, Plaintiff, v. DOES 1-10, Defendants.	Case No. 1:25-CV-2695-MHC **FILED UNDER SEAL**

BRIEF IN SUPPORT OF APPLICATION OF MICROSOFT CORPORATION FOR AN EMERGENCY *EX PARTE* ORDER FOR TEMPORARY RESTRAINING ORDER, PRELIMINARY INJUNCTION, AND RELATED RELIEF

TABLE OF CONTENTS

INTRODUCTION

Plaintiff Microsoft Corp. ("Microsoft") moves for emergency *ex parte* relief pursuant to Federal Rule of Civil Procedure 65; the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the Lanham Act (15 U.S.C. §§ 1125); the Copyright Act; the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962(c)); and the All Writs Act (28 U.S.C. § 1651). Microsoft's requested relief is necessary for the investigation, abatement, and remediation of Defendants' use of Microsoft's copyrighted software, trademarks, and customer's computers to distribute and exploit malware designed to steal information from Microsoft customers and use that stolen information to commit financial crimes.

Because prior notice to Defendants of Microsoft's motion would provide Defendants with an opportunity to destroy, move, conceal, or otherwise make inaccessible certain instrumentalities used to obtain unauthorized access into Microsoft software and computer systems and evidence of their unlawful activities, Microsoft seeks relief *ex parte* and has moved to temporarily seal this action until after execution of the Court's orders. *See, e.g., Microsoft Corp. v. Malikov*, No. 1:22-cv-1328-MHC, 2022 WL 1742862 (N.D. Ga. Apr. 8, 2022); *Microsoft Corp. v. Does 1-51,* No. 1:17-CV-4566, 2017 WL 10087886 (N.D. Ga. Nov. 17, 2017) (both cases granting *ex parte* relief in action that was sealed until execution of the court's orders).

Defendants are a group of natural persons engaged in a malicious scheme to distribute and exploit malware targeting Microsoft customers. Specifically, this action targets the most widely distributed data-stealing malware family in the world, commonly known as Lumma, LummaStealer, or LummaC2 malware ("Lumma"). Lumma malware has been linked with a wide range of cybercrimes such as ransomware, financial fraud, and even nation state-initiated activities. Defendants are the creators, distributors, operators, and purchasers of Lumma and associated services, and they act in a concerted and cooperative manner to monetize Lumma and leverage infected computers for their own unlawful purposes. Together, Defendants form and contribute to the conduct of an ongoing criminal enterprise ("Lumma Enterprise") that is harming Microsoft, its customers, and the public at large.

Accordingly, Microsoft respectfully requests:

> (1) an order directing Defendants, their service providers, and/or those acting in concert therewith to preserve evidence related to, and to cease from using or permitting to be used the infrastructure identified in Microsoft's Proposed TRO to operate the Lumma;
>
> (2) an order enjoining Defendants from further violations of the CFAA, Lanham Act, Copyright Act, and RICO Act; and
>
> (3) an order directing Defendants to show cause why they should not be preliminarily enjoined from the violations of law described in this motion and Microsoft's Complaint.

Ex parte relief is essential. Notice to Defendants would provide them with an opportunity to destroy, move, conceal, or otherwise make inaccessible

the instrumentalities they use to direct the operation and the evidence of their unlawful activity. Defendants can easily redirect infected user computers away from the currently used (and identified) command and control infrastructure if they learn of the impending action. Giving Defendants that opportunity would render further prosecution of this lawsuit fruitless. This type of requested *ex parte* relief is not uncommon when disabling an online command and control infrastructure used by unidentified defendants for illegal operations and cybercrime schemes. Courts in numerous cases involving the type of cybercrime at issue here have granted such relief.[1]

If Microsoft's requests for relief are granted, Microsoft will work with its private and public partners to disable the Lumma Enterprise's core infrastructure in a carefully timed and coordinated manner that should prevent

[1] *See, e.g., Microsoft Corp. v. Malikov*, No. 1:22-cv-1328-MHC, 2022 WL 1742862 (N.D. Ga. Apr. 8, 2022) (Cohen, J.); *Microsoft Corp. v. Does 1-51*, No. 1:17-CV-4566, 2017 WL 10087886 (N.D. Ga. Nov. 17, 2017) (Cohen, J.); *Microsoft v. John Does 1-2*, Case No. 1:19-cv-00716-ABJ (D.C. 2019) (Berman-Jackson, J.*); Microsoft v. John Does 1-2*, Case No. 1:19-cv-01582 (E.D. Va. 2019) (O'Grady, J.); *Sophos v. John Does 1-2*, Case No. 1:20-cv-00502 (E.D. Va. 2020) (O'Grady, J.); *Microsoft v. John Does 1-2*, Case No. 1:20-cv-00730 (E.D. Va. 2020) (O'Grady, J.); *DXC Technology Company v. John Does 1-2*, Case No. 1:20-cv-00814 (E.D. Va. 2020) (Alston, J.); *Microsoft and FS-ISAC v. John Does 1-2*, Case No. 1:20-cv-1171 (E.D. Va. 2020) (Trenga, J.); *Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.); *Microsoft v. John Does 1-82 et al*., Case No. 3:13-CV-00319-GCM (W.D.N.C.) (Mullen, J.); *Microsoft Corporation v. John Does 1-8 et al*., Case No. A13-cv-1014-SS (W.D. Tex. 2013) (Sparks, J.); *Microsoft Corp v. John Does 1-5*, Case No. 1:15-cv06565-JBW-LB (E.D.N.Y) (Bloom, J.).

Defendants from regaining control over infected computers. As soon as the requested relief is effected, Microsoft will then act promptly and diligently to provide notice to Defendants by serving them with all papers in this action via all known means of contacting them. Microsoft will also act promptly to unseal this action and will publish the papers in this case to facilitate notice.

STATEMENT OF FACTS

Plaintiff Microsoft Corp. is a corporation duly organized and existing under the laws of the State of Washington, having its headquarters and principal place of business in Redmond, Washington. Microsoft is a leading provider of technology products and services, including computer software, Internet services, websites, and email services.

DOES 1-10 are associated with creating, distributing, operating, and selling Lumma and associated services and are participants in the conduct of a malware-as-a-service enterprise referred to in Microsoft's Complaint as the Lumma Enterprise. Declaration of Derek Richardson, ¶¶ 4-11. In general, the Luma Enterprise is characterized by Defendants' collective efforts to use social engineering techniques designed to trick users into infecting their computers with Lumma malware, to control infected computers through command and control ("C2") infrastructure, and using infected computers and C2 infrastructure to steal data and monetize Lumma-related services in furtherance of financial crimes. Lumma is the most widely

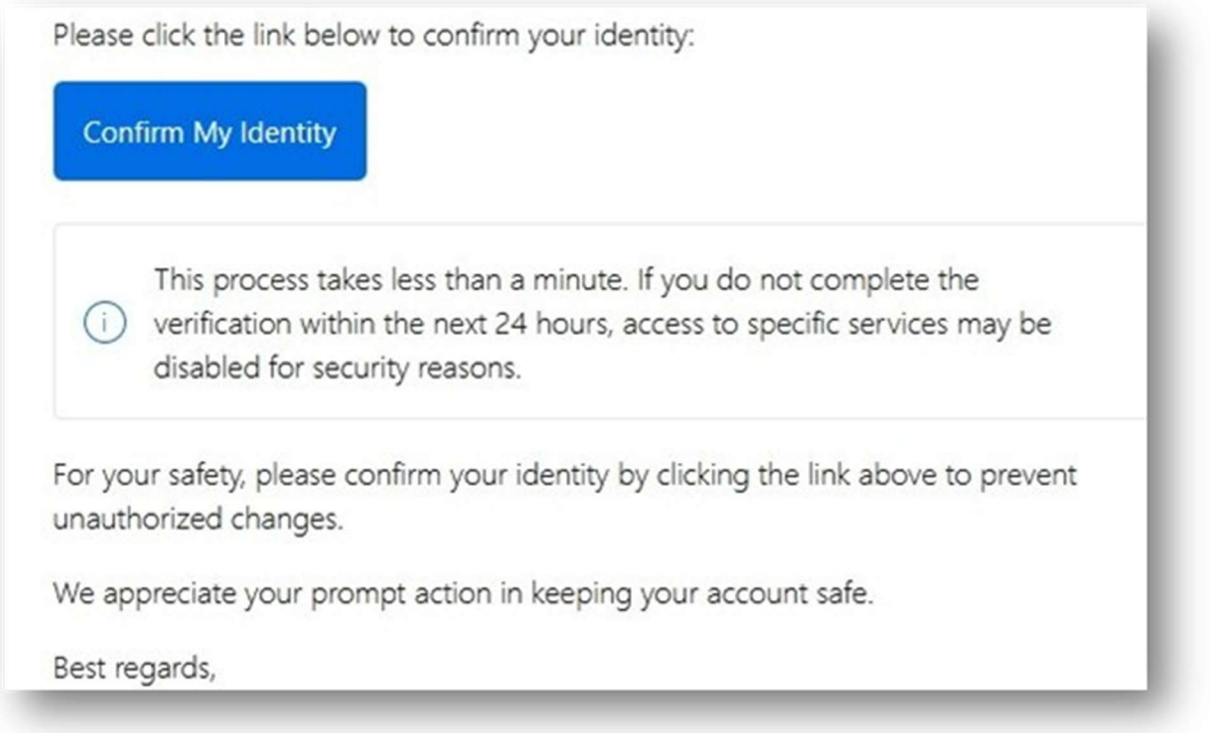
distributed information stealer in the world. Richardson Decl. ¶ 28; Declaration of Jakub Tomanek ¶13. Defendants appear to be focused on theft of credentials associated with crypto currency accounts.

DOE 1 is a natural person who resides outside the United States (possibly Russia) and is associated with an online persona known as "Shamel." Richardson Decl. ¶ 5. DOE 2 is a natural person responsible for procuring and operating Cloudflare infrastructure used by Defendants to carry out their scheme. Id. ¶ 6. DOE 3 is a natural person responsible for procuring and operating numerous malicious internet domains used as command and control domains for the Lumma. Id. ¶ 7. Defendant DOE 4 is a natural person responsible for procuring and operating Telegram infrastructure used by Defendants to carry out their scheme. Id. ¶ 8. Defendant DOE 5 is a natural person responsible for procuring and operating Steam infrastructure used by Defendants to carry out their scheme. Id. ¶ 9. DOE 6 is a natural person involved in advertising, selling, and distributing Lumma services. Id. ¶ 10. DOES 7-10 are natural persons who are end users of the malicious services and infrastructure provided by DOES 1-6. Id. ¶ 11.

Lumma Infection Vectors

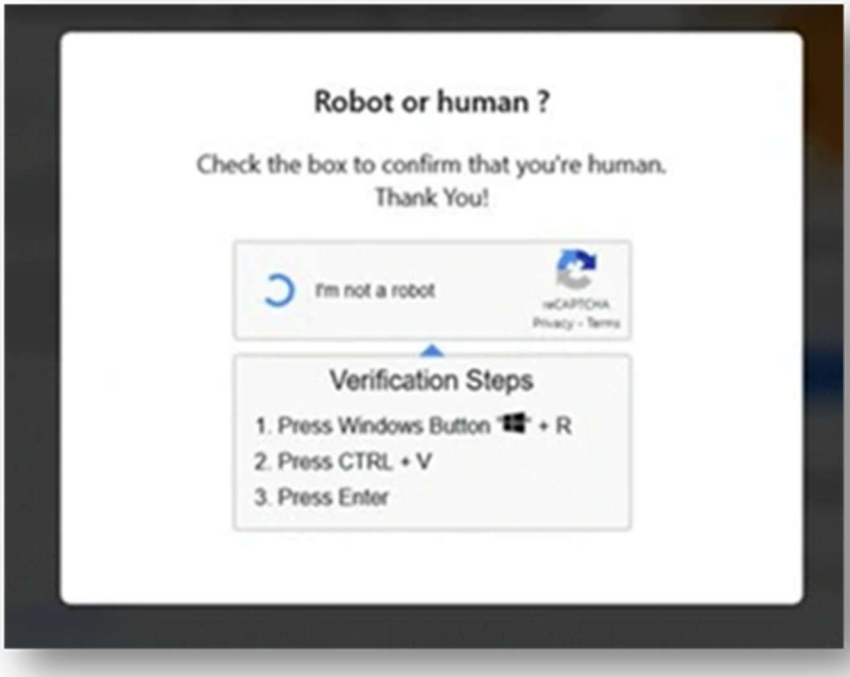
In December 2024, Microsoft Threat Intelligence identified a phishing campaign ("Storm-1865") impersonating an online travel agency and targeting organizations in the hospitality industry. The Storm-1865 phishing campaign uses a

social engineering technique called "ClickFix" to deliver multiple credential-stealing malware in order to conduct financial fraud and theft. Richardson Decl. ¶¶ 21-22. In the ClickFix technique, a threat actor attempts to take advantage of human problem-solving tendencies by displaying fake error messages or prompts that instruct target users to fix issues by copying, pasting, and launching commands that eventually result in the download of malware. This need for user interaction could allow an attack to slip through conventional and automated security features. Id. ¶ 22. An example of a Storm-1865 phishing email observed by Microsoft is depicted below in **Figure 1.**



Another Storm-1865 phishing email observed by Microsoft shows use of a fake CAPTCHA (Completely Automated Public Turing test to tell Computers and

Humans Apart) screen designed to trick users into thinking they are performing Microsoft Windows functions to verify they are human, as show below in **Figure 2.**



Among the types of credential-stealing malware identified during investigation of the Storm-1865 phishing campaign are various files associated with the Lumma malware. Lumma is an information stealer designed to collect data stored in browsers, including session tokens and cookies—which can include multi-factor authentication ("MFA") claims—saved passwords and input form data, credit card information, and cryptocurrency wallets. Richardson Decl. ¶ 25; Declaration of Igor Aronov ¶ 5; Tomanek Decl. ¶ 10. Typically, the goal of Lumma operators is to monetize stolen information collected by selling the data on infostealer marketplaces

or conducting further exploitation for various purposes. Lumma has reportedly been sold on underground forums since 2022 as a malware-as-a-service ("MaaS"), with multiple versions being released by the developers in an attempt to improve its capabilities. Richardson Decl. ¶ 25. Defendants use various additional types of social engineering technics to infect victim computers. Id. ¶¶ 31-34. Due in part to Defendants' sophisticated obfuscation tactics and social engineering efforts, Lumma is currently the most widely distributed malware in the world. Richardson Decl. ¶ 28.

Lumma Malware Characteristics

Lumma is specifically designed to attack Microsoft's software and customers. The malware is designed for injection into legitimate Windows processes and leverages low level Microsoft APIs. Richardson Decl. ¶ 30. Lumma's designers took special care to create purpose-built code for bypassing Microsoft antivirus protections. Lumma attempts to install a driver and terminate services related to various Microsoft security products. Lumma also attempts to delete registry keys related to various Microsoft security products. At least Defendant DOE 1 used Microsoft's Windows software development kit ("Windows SDK") to create the versions of Lumma used in Defendants scheme. Id. ¶ 31. The Windows SDK provides the headers, libraries, metadata, samples, and tools for building Windows applications. In order to access the SDK, DOE 1 needed to indicate their assent to

the terms of Microsoft's Windows SDK License Agreement, which provides that the license Microsoft grants is conditioned on the user's promise to include distributable code in malicious, deceptive, or unlawful programs. Id.

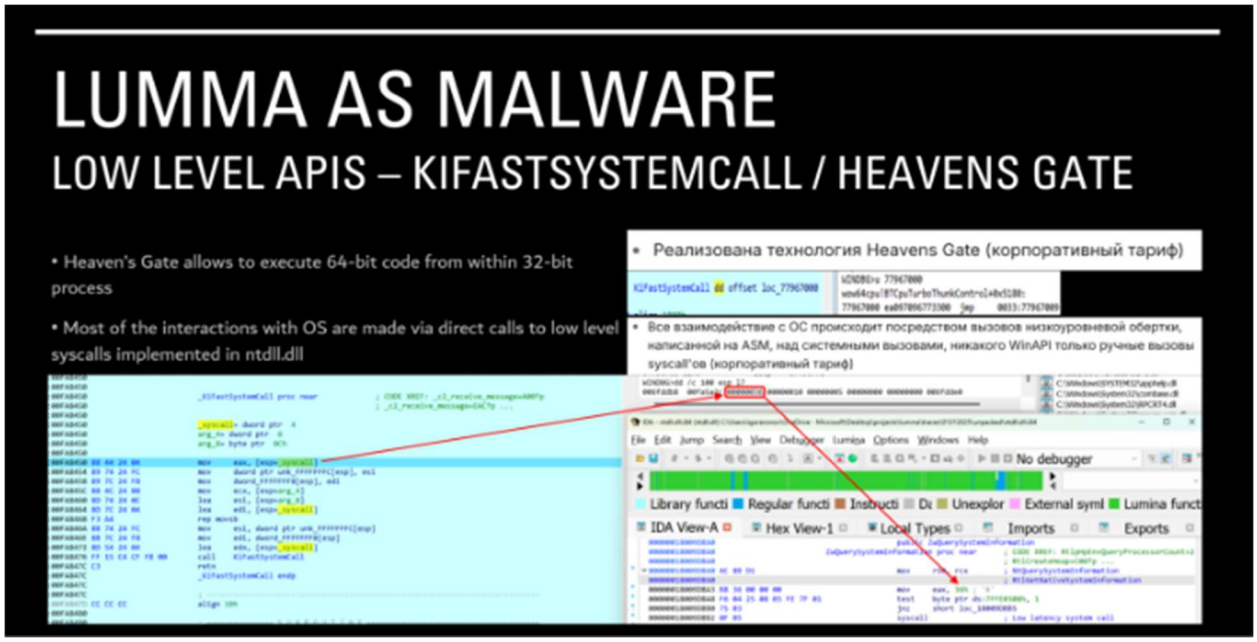
Once a Windows user's computer is infected with Lumma, that computer becomes a "client" in the Defendants' malicious network. Defendants network also includes servers responsible for sending commands to and receiving data from infected computers. These servers are referred to as "command and control" or C2 servers. Richardson Decl.¶ 38. In addition, Defendants utilize Cloudflare proxy server infrastructure to facilitate data exfiltration and to obfuscate the location of Defendants C2 servers. **Figure 3** below provides a high- level depiction of the architecture employed for the Lumma botnet by Defendants.

Microsoft analyzed Lumma malware using a combination of reverse engineering techniques, including dynamic and static reverse engineering methodologies. Declaration of Roedlio Fiñones ¶ 5. Lumma's source code is heavily

obfuscated, which indicates an attempt by the authors of the malware to make it difficult for Microsoft and other security researchers to understand its functions. Id. ¶ 6. Analysis of Lumma shows that the malware targets several types of victim information including user's files (documents from under %userprofiles%), credentials from browsers (login data like username, passwords and credit card numbers, search histories, web data, user and network cookies), crypto wallets and extensions, two factor authentication web browser extensions, and data associated with VPN, FTP, and email applications. For example, if Edge browser is open and Lumma attempts to steal browser cookies, it will terminate processes related to Edge and will restart the process with specific command line as if it attempts to debug it. Id. ¶ 10.

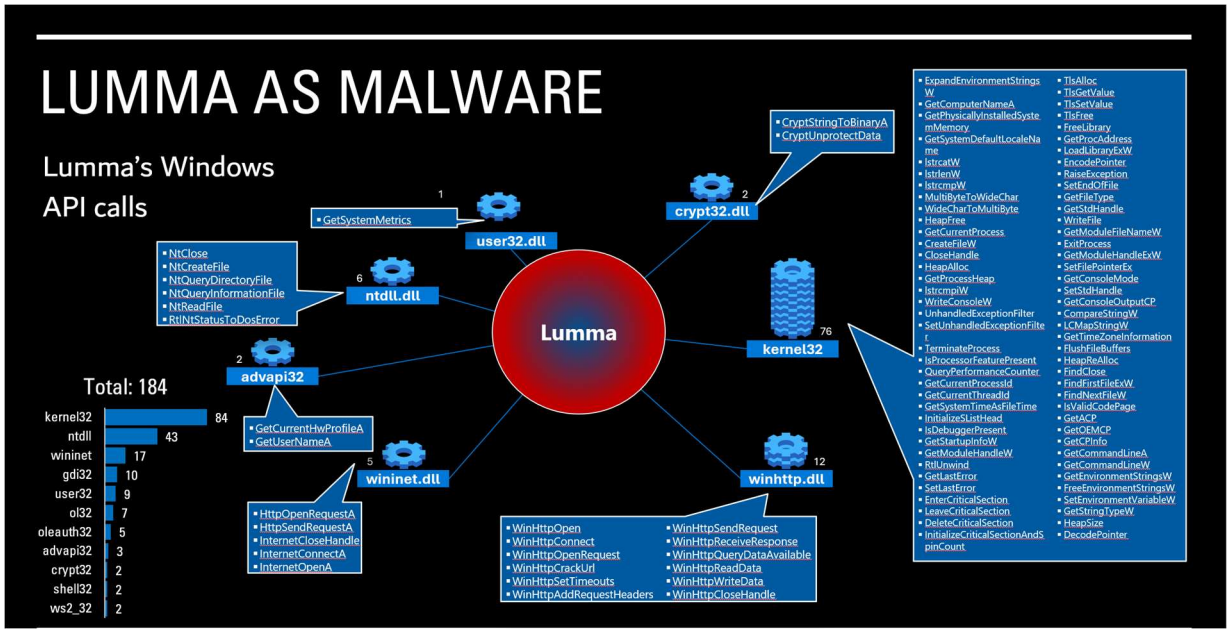
Lumma also makes use of something commonly known as the "Heavens Gate" technique. This technique is designed to exploit a feature in operating systems that allows the transition from a 32-bit mode to a 64-bit mode during execution of certain software. The Heavens Gate technique enables malware to evade detection by security software designed to monitor only 32-bit processes. Most of Lumma's interactions with Windows take place via direct calls to low level APIs. Id. ¶ 11. Lumma is designed to bypass Microsoft antivirus products. The malware attempts to install a driver that is used by a malicious loader program to deliver/download Lumma and other malware modules. Lumma malware also attempts to terminate

services related to Microsoft Security Products. The snapshot **Figure 4** below shows the execution flow.



Id.

Lumma malware makes at least 184 Windows API calls during the course of its operation. Windows APIs are APIs created by Microsoft that can be used to facilitate communications between the Windows operating system and third party software applications. Id. ¶ 12. **Figure 5** below provides a graphical display of the APIs and number of calls observed during Microsoft's investigation:



Id. The APIs depicted in Figure 5 belong to Microsoft and are subject to copyright protection. Id. ¶ 13.

Lumma C2 Infrastructure

Lumma causes infected computers to reach out to command and control ("C2") servers. These C2 servers transmit information about data stealer capabilities, can instruct the infected computer to download and execute additional plugins/modules and malware, and can run malware from disk, or directly in memory. For example, C2 servers can download a clipboard stealing module or coin miners that collect data exfiltrated from the victim's computer's web browser sessions. These C2 servers are associated with specific domains that are either hardcoded into the Lumma malware or provided through malicious Telegram and

Steam accounts. Microsoft refers to these domains as C2 domains. Aronov Decl. ¶ 6.

Instructions regarding which victim credentials to steal are specified in the configuration file retrieved from C2 servers. The stealer configuration file is divided into several parts, some pertaining to the target list of apps for cryptocurrency wallets and extensions, others pertaining to the list of applications and configuration details for browsers, user file's locations, and other applications. Id. ¶ 7.

The distribution infrastructure supporting Lumma is flexible and adaptable. Operators continually refine their techniques, rotating malicious domains, exploiting ad networks, and leveraging legitimate cloud services to evade detection and maintain operational continuity. This infrastructure enables Defendants to maximize the success of their campaigns while complicating efforts to trace or dismantle their activities. Id. ¶ 9. Lumma maintains robust C2 infrastructure, using a combination of hardcoded Tier 1 C2s that are regularly updated and reordered, and two types of intermediate/extended C2s hosted as Steam and Telegram profiles, which also point to the Tier 1 C2s. To further hide the real C2 servers, all the C2 servers are hiding behind a Cloudflare proxy. In addition, Lumma employs domain obfuscation techniques that demonstrate Defendants technical sophistication. Tier 1 C2s and Telegram C2 (if present) will be encrypted using ChaCha20, Steam C2 is encrypted using simple variation of XOR encoding. Id. ¶ 10.

Microsoft has identified over 2,300 hardcoded command-and-control domains. Microsoft has identified 3 Steam and 92 Telegram accounts used to point to backup C2 domains. Aronov Decl. ¶ 11. Microsoft has confirmed that, as of the date of this declaration, approximately 1,500 of these domains remain active. Richardson Decl.¶ 43.

Lumma Marketing and Distribution

Lumma is currently the most widely distributed malware in the world. Between March 16, 2025 to May 2, 2025, Microsoft observed approximately 331,000 infected and encountered Windows computers. Richardson Decl. ¶ 28. **Figure 6** below provides a heatmap of Lumma infections in the U.S.

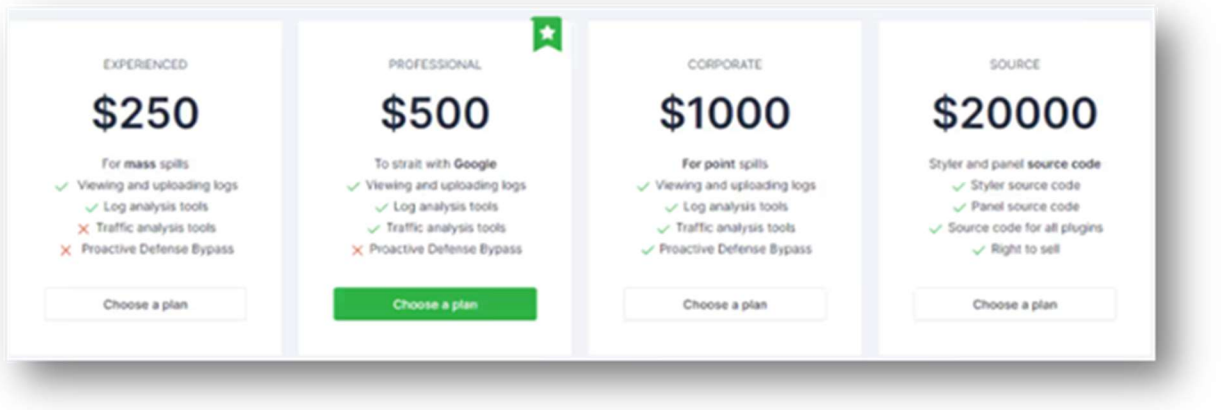
Id.

The creators, distributors, and operators of the Lumma malware are characterized by a high degree of sophistication and commercial organization.

According to an IBM study, Lumma is the most actively advertised information stealer on the dark web by a wide margin. Richardson Decl. ¶ 29. Lumma even has its own logo that is used in connection with efforts to monetize the malware, as depicted below in **Figure 7**.

Id.

Marketplace Defendants (DOES 6-7) provide a marketplace for Lumma that provides pricing tiers up to $20,000 depending on the type of criminal use case desired. Richardson Decl. ¶ 42. DOES 8-10 are consumers in this marketplace and have engaged in at least one transaction for services or data provided by the Lumma malware and Infrastructure Defendants. Id. **Figure 8** below is a screenshot of the Lumma malware marketplace website.



Id.

Remediation Strategy

Microsoft believes it will be able to disable approximately 500 command-and-control domains through domain abuse channels and industry partner cooperation. For the remaining domains and infrastructure used by Defendants, Microsoft seeks injunctive relief that will allow Microsoft to seize the domains in order to preserve evidence and prevent their continued use by Defendants. Richardson Decl. ¶ 45.

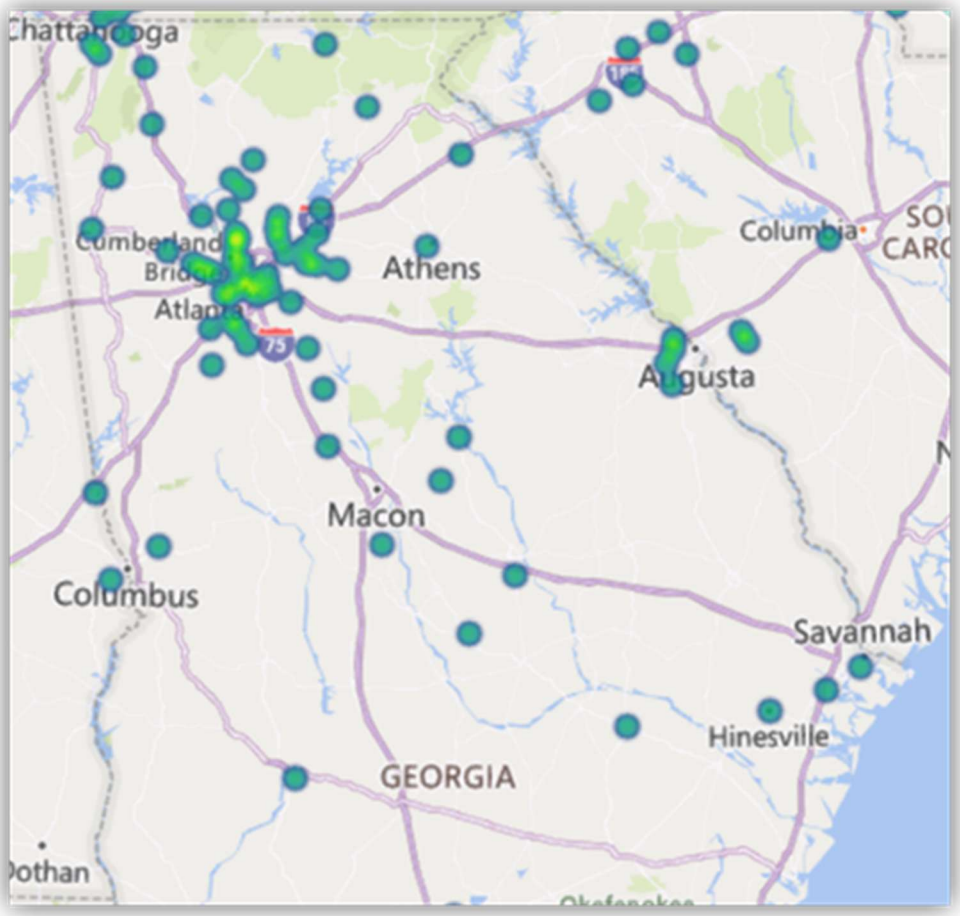
ARGUMENT

I. THE COURT HAS JURISDICTION OVER THIS ACTION AND EACH DEFENDANT

The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises out of Defendants' violation of the CFAA (18 U.S.C. § 1030), the Lanham Act (15 U.S.C. §1125(a), (c)), the Copyright Act (17 U.S.C. § 101), and the Racketeer Influence and Corrupt Organizations Act (18 U.S.C. § 1962(c)).

The Court has jurisdiction over Defendants because in carrying out the

conduct described in this Complaint, Defendants have availed themselves of the privilege of conducting business in Georgia. *See, e.g., Diamond Crystal Brands, Inc. v. Food Movers Int'l*, 593 F.3d 1249, 1267 (11th Cir. 2010). Defendants have intentionally infected, communicated with, and extracted data from Windows computers in Georgia and have thus directed the acts complained toward the State, its residents, and this judicial district. *See, e.g., Skyhop Techs., Inc. v. Narra*, 58 F.4th 1211, 1228 (11th Cir. 2023) ("SkyHop's CFAA claim arises from Indyzen's communications into Florida"); *United States v. Auernheimer*, 748 F.3d 525, 533 (3d Cir. 2014) (Venue would be proper in any district where the CFAA violation occurred, or wherever any of the acts in furtherance of the conspiracy took place."). There are currently at least 532 Lumma-infected machines in Georgia associated with the Lumma Enterprise. Richardson Decl. ¶ 12. These infected computers are actively sending data from user machines in Georgia to C2 servers controlled by one or more DOE defendants. The data Defendants are stealing, distributing, and selling from Georgia-based computers include IP address information which shows Defendants that the computers are located in Georgia. *Id*. Between March and May 2, 2025 Microsoft observed Lumma on several hundred Windows computers in the state of Georgia. Lumma infections in the State of Georgia are depicted in **Figure 9** below.



Id.

Defendants have acted at all times relevant with knowledge that their acts would cause harm through computers located in Georgia thereby injuring Plaintiff, its customers, and others in in the United States.

In addition to their contacts with Georgia, Defendants also have sufficient national contacts with the United States as a whole to subject each Defendant to the Court's jurisdiction consistent with requirements of due process. *See, e.g., Charter Oil Co. v. Cotton (In re Charter Oil Co.),* 189 B.R. 527, 530 (Bankr. M.D. Fla. 1995)

("The national contacts analysis requires that defendants have national contacts with the United States, not the State').

Defendants intentionally availed themselves of the privilege of doing business in the United States by engaging in the following activities: (i) fraudulently gaining access to Microsoft's Windows SDK and WDK, which required one or more Defendants to affirmatively enter into license agreements with Microsoft by misrepresenting that they would not use Microsoft's materials for illegal purposes; (ii) Abusing the infrastructures of companies like Cloudflare, Verisign, and other ISPs located in the U.S.; (iii) Victimizing users and computers located throughout the U.S.; (iv) Obtaining code from, and posting code to, U.S.-based source code repository providers; (v) Contracting with and abusing the services of at least nine U.S.-based Registrars in order to purchase, register and control at least 664 command and control domains; (vi) Contracting with and abusing the services of U.S.-based Valve Corporation to distribute command and control domains through its Steam service. Richardson Decl. ¶ 13.

Accordingly, to the extent Defendants do not have sufficient contacts with Georgia alone to support jurisdiction and venue in this Court, each Defendant is subject to jurisdiction based on their national contacts with the United States and are thus subject to national service of process and jurisdiction is proper in this Court. *Gen. Cigar Holdings, Inc. v. Altadis, S.A.*, 205 F. Supp. 2d 1335, 1340 (S.D. Fla.

2002) ("personal jurisdiction is proper in any district, so long as sufficient national contacts have been established."); 18 U.S.C. § 1965.

II. THE RECORD SUPPORTS A TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTIVE RELIEF

The fundamental purposes of temporary restraining orders and preliminary injunctions are 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. *See, e.g., United States v. State of Ala*., 791 F.2d 1450, 1459 (11th Cir. 1986). "Parties seeking a preliminary injunction must demonstrate that (1) they are likely to succeed on the merits, (2) they are likely to suffer irreparable harm, (3) the balance of hardships tips in their favor, and (4) the injunction is in the public interest." *Winter v. Natural Res. Def. Council, Inc*., 555 U.S. 7, 20 (2008).

This matter presents a quintessential case for injunctive relief. Defendants' conduct causes irreparable harm to Microsoft because Defendants are breaking Microsoft's software, causing malicious misuse of Microsoft's copyrighted materials, using Microsoft's trademarks to deceive victims, and stealing sensitive data from victim computers in order to facilitate financial crimes. Each of these is a distinct and cognizable form of irreparable harm. *See, e.g., Fla. Atl. Univ. Bd. of Trs. v. Parsont*, 465 F. Supp. 3d 1279 (S.D. Fla. 2020) (granting preliminary injunction because "federal courts around the country agree that the interference with an entity's control of its computer systems constitutes irreparable injury"); *Metro-Goldwyn-*

Mayer, Inc. v. Showcase Atlanta Co-op. Prods., Inc., 479 F. Supp. 351 (N.D. Ga. 1979) (granting preliminary injunction re copyright infringement); *Boulan S. Beach Master Ass'n, Inc. v. Think Props., LLC*, 617 F. App'x 931 (11th Cir. 2015) (unpublished) (plaintiff who pled that trademark misuse caused confusion and damage to its brand entitled to injunction). Every day that passes gives Defendants an opportunity to infect more computers and cause more damage. Unless the requested relief is granted, Defendants will very likely continue to use the Lumma malware to intercept and gain access to the contents of communications transmitted through the computers and infrastructure of Microsoft and its users, including access to the passwords, personal identifying information, sensitive financial information, or personal health information contained in such communications causing irreparable harm.

A. Microsoft is Likely to Succeed on the Merits of Its Claims

Microsoft's evidence shows it will be able to establish the elements of each of its claims. The evidence in support of Microsoft's TRO application is based on the diligent work of experienced investigators and is supported by substantial empirical evidence and forensic documentation. Given the strength of Microsoft's evidence, the likelihood of success on the merits weighs heavily in favor of granting injunctive relief.

1. Microsoft's Evidence Shows Defendants' Violations of the CFAA

Congress enacted the Computer Fraud and Abuse Act (the "CFAA") specifically to address computer crime. *See, e.g., Univ. Sports Pub. 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 (S.D.N.Y. 2001) (noting that activity that "Congress sought to punish and remedy in the CFAA -- namely, damage to computer systems and electronic information by hackers"); *Big Rock Sports, LLC v. AcuSport Corp*., 2011 U.S. Dist. LEXIS 110995, *3 (E.D.N.C. Sept. 26, 2011). "Any computer with Internet access [is] subject [to] the statute's protection." *Id*. *Inter alia*, the CFAA penalizes a party that intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage. 18 U.S.C. § 1030(a)(5)(C).

A "protected computer" is a computer "used in interstate or foreign commerce or communication." *See, e.g.,* United States v. Gasperini, 2017 WL 2399693, at *3 (E.D.N.Y. June 1, 2017); *SecureInfo Corp. v. Telos Corp*., 387 F. Supp. 2d 593, 608 (E.D. Va. 2005). This definition encompasses any computer with an internet connection. See United States v. Yücel, 97 F. Supp. 3d 413 (S.D.N.Y. 2015) (collecting cases and noting "widespread agreement in the case law" that "protected computer" includes any internet-connected computer). "The phrase 'exceeds

authorized access' means 'to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter.'" *JBCHoldings NY, LLC v. Pakter*, 931 F. Supp. 2d 514, 523 (S.D.N.Y. 2013) (citing 18 U.S.C. § 1030(e)(6)). In order to prosecute a civil claim under the CFAA, a plaintiff must demonstrate loss or damage in excess of $5,000. The CFAA defines loss as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Sprint Nextel Corp. v. Simple Cell, Inc*., 2013 U.S. Dist. LEXIS 99580, 21 (D. Md. July 17, 2013) (citing 18 U.S.C. § 1030(e)(8)). "Damage. . . means any impairment to the integrity or availability of data, a program, a system, or information." *Id*. (citing 18 U.S.C. § 1030(e)(11)). "The Fourth Circuit has recognized that this 'broadly worded provision plainly contemplates consequential damages' such as 'costs incurred as part of the response to a CFAA violation, including the investigation of an offense.'" *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009). The CFAA permits plaintiffs to aggregate multiple intrusions or violations for the purpose of meeting the $5,000 statutory threshold. *See Nexans Wires S.A. v. Sark-USA, Inc*., 319 F. Supp. 2d 468, 473

(S.D.N.Y. 2004), aff'd, 166 F. App'x 559 (2d Cir. 2006); *Sprint Nextel Corp*., 2013 U.S. Dist. LEXIS 99580, 21 (citations omitted).

In sum, in order to prevail on their CFAA claim, Microsoft must establish that Defendants (1) accessed a protected computer; (2) without authorization; (3) resulting in loss or damage in excess of $5,000. The Richardson, Finones, and Aronov Declarations establish that Defendants' conduct satisfies each of these elements. First, the computers that run Microsoft's network infrastructure are protected computers. *See* 18 U.S.C. § 1030(e)(2)(B) (defining "protected computer" as a computer "used in interstate or foreign commerce or communication").

Second, each protected computer has been accessed without authorization: Defendants use social engineering to trick users into installing malicious files, and those files then bypass Microsoft security tools to gain unauthorized access to victims' computers and data. *See, e.g., Microsoft Corp. v. Malikov*, No. 1:22-cv-1328-MHC, 2022 WL 1742862 at *4 (N.D. Ga. Apr. 8, 2022) (finding Microsoft's and Microsoft's partners and customers computers to be protected computers); *Microsoft Corp. v. Does 1-51,* No. 1:17-CV-4566, 2017 WL 10087886 at *4 (N.D. Ga. Nov. 17, 2017) (finding Microsoft's and Microsoft's customers computers to be protected computers); *Volk v. Zeanah,* No. 608CV094, 2010 U.S. Dist. LEXIS 5621, at *4 (S.D. Ga. Jan. 25, 2010) ("The CFAA is meant to reduce hacking of computer systems/networks"); *Schwartz v. ADP, Inc.,* No. 2:21-cv-283-SPC-MRM, 2021 U.S.

Dist. LEXIS 231613, at *3 (M.D. Fla. Dec. 3, 2021) ("The CFAA punishes computer hacking")*; Microsoft Corp. v. Does*, Civil Action No. 1:22cv607 (LMB/WEF), 2024 U.S. Dist. LEXIS 76088, at *26-27 (E.D. Va. Jan. 10, 2024) (collecting cases).

Third, Defendants' conduct has caused harm to Microsoft exceeding $5,000, including substantial time spent by Microsoft personnel such as Messrs. Richardson, Finones, and Aronov. Microsoft has also incurred attorneys' fees investigating and remediating Defendants conduct. The substantial economic and human cost devoted to investigating and remediating Defendants' conduct amounts to well over $5,000 in harm. *See, e.g., Benessere Inv. Grp., LLC v. Swider,* No. 24-CV-21104-RAR, 2024 U.S. Dist. LEXIS 198469, at *16 n.6 (S.D. Fla. Oct. 31, 2024); *GSP Fin. Servs., LLC v. Harrison*, No. GJH-18-2307, 2021 U.S. Dist. LEXIS 16341, at *21 (D. Md. Jan. 28, 2021) ("The Court finds the expenses for legal counsel, cybersecurity consulting, and employees' time are reasonably foreseeable and necessary losses associated with investigating and remedying the harm caused by Defendant's actions.").

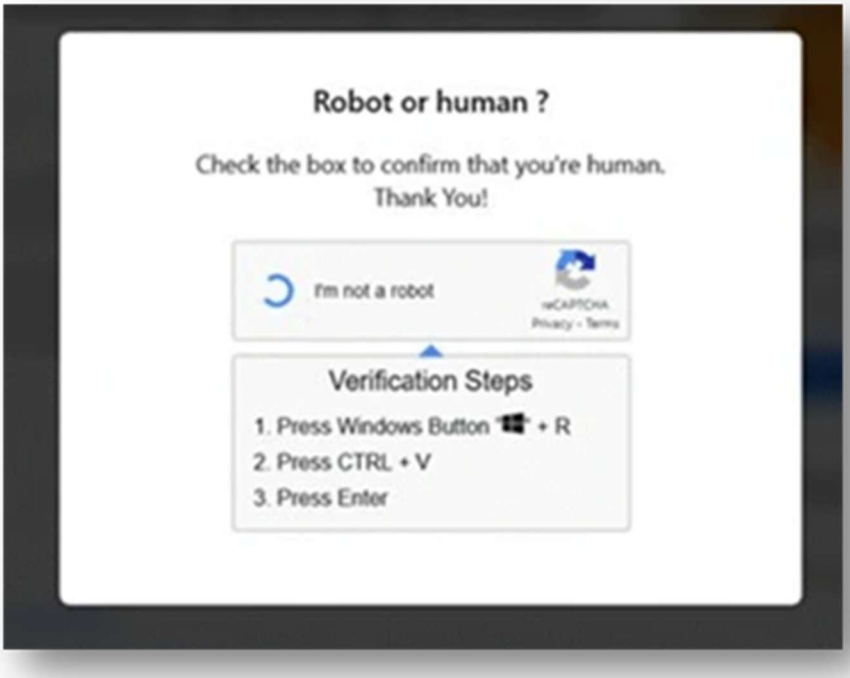
2. Defendants' Conduct Violates the Lanham Act

Section 1125(c) of the Lanham Act prohibits use of registered marks that are "likely to cause dilution by blurring or dilution by tarnishment of the famous mark." Defendants are actively tarnishing Microsoft's marks by corrupting Microsoft's products and using its Windows, Edge, and Microsoft marks in connection with

those corrupted products. Defendants' conduct also constitutes false designation of origin under section 1125(a), which prohibits use of a registered mark that:

> is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person.

15 U.S.C. § 1125(a)(1)(A). In carrying out their criminal activity, Defendants rely on the misleading and false uses of Plaintiffs' trademarks. Defendants' social engineering campaigns leverage Microsoft's trademarks and logos to make it look like the messages are legitimate communications from Microsoft, as shown in the example image below.



Richardson Decl. ¶ 23. Such misuse of Microsoft's trademarks is a clear violation of Lanham Act and Microsoft is likely to succeed on the merits. *See Garden & Gun, LLC v. Twodalgals, LLC*, 2008 U.S. Dist. LEXIS 79982 (W.D.N.C. 2008) (granting preliminary injunction against misleading use of trademarks under Section 1125(a)); *IHOP Corp*., 2008 U.S. Dist. LEXIS 112056 at *1-3 (same; granting TRO); *Am. Online v. IMS*, 24 F. Supp. 2d 548, 551-552 (E.D. Va. 1998) (misuse of trademark in e-mail headers violated §1125(a); also constituted trademark "dilution" under §1125(c)); *Brookfield Commc'ns*., 174 F. 3d at 1066-67 (entering preliminary injunction under Lanham Act §1125(a) for infringement of trademark in software and website code); *Hotmail Corp. v. Van$ Money Pie, Inc*., 1998 U.S. Dist. LEXIS 10729, *12-13 (N.D. Cal. 1998) (granting preliminary injunction; copying the Hotmail trademarks in "e-mail return addresses" constituted false designation of origin; also constituted trademark "dilution" under §1125(c)).

In addition, Defendants cause Lumma to inject malicious code into legitimate Windows processes, Finones Decl. ¶ 7, resulting in counterfeit versions of Microsoft's products that users falsely believe to be genuine. *See, e.g., Microsoft Corp. v. Tierra Comput., Inc*., 184 F. Supp. 2d 1329, 1333 (N.D. Ga. 2001) ("Defendants used counterfeit marks in the sale of the infringing software packages"). *Audi AG v. Shokan Coachworks, Inc*., 592 F. Supp. 2d 246, 279 (N.D.N.Y. 2008) (holding that the use of the plaintiffs' marks in the defendants'

email addresses created a likelihood of consumer confusion); *Microsoft Corp. v. Doe*, 2021 U.S. Dist. LEXIS 101862, at *13-14 (E.D.N.Y. May 28, 2021) ("[malware] does not intend to just compete with the Windows operating system, it intends to hide itself within the system to take over and replace it without the user's knowledge," and "[i]n the eyes of the user, [malware] becomes Microsoft, but it is not Microsoft at all. Nor is the user aware that [malware] is manipulating their devices to commit cybercrimes."); *see also Kuklachev v. Gelfinan*, 629 F. Supp. 2d 236,258 (E.D.N.Y. 2008) (entering preliminary injunction under Lanham Act for infringement of trademarks where confusion was likely to result from use of plaintiffs' name and images in connection with defendants' advertisements); *Broolqield Commc'ns. v. W. Coast Entm 't Corp*., 174 F.3d 1036, 1066-1067 (9th Cir. 1999) (entering preliminary injunction under Lanham Act for infringement of trademark in software and website code).

Defendants' activity warrant injunctive relief. *See, e.g., CJ Prods. LLC v. Snuggly Plushez LLC*, 809 F. Supp. 2d 127, 147-48 (E.D.N.Y. 2011) (entering a preliminary injunction under the Lanham Act § 1125(a) for infringement of trademark on a website); *Brookfield Commc'ns.*, 174 F. 3d at 1066-67 (entering preliminary injunction under Lanham Act § 1125(a) for infringement of trademark in software and website code); *Hotmail Corp. v. Van$ Money Pie, Inc*., 47 U.S.P.Q.2d (BNA) 1020,1024, 1025- 26 (N.D. Cal. 1998) (granting preliminary

injunction; copying the Hotmail trademarks in "e-mail return addresses" constituted false designation of origin); *Am. Online v. IMS*, 24 F. Supp. 2d 548, 551-552 (E.D. Va. 1998) (misuse of trademark in e-mail headers violated §1125(a)); *Microsoft Corp. v. Doe*, 2021 U.S. Dist. LEXIS 101862, at *13-14 (E.D.N.Y. May 28, 2021) ("[malware] does not intend to just compete with the Windows operating system, it intends to hide itself within the system to take over and replace it without the user's knowledge," and "[i]n the eyes of the user, [malware] becomes Microsoft, but it is not Microsoft at all. Nor is the user aware that [malware] is manipulating their devices to commit cybercrimes.").

The Lanham Act further provides that the owner of a famous, distinctive mark "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...." 15 U.S.C. § 1125(c). Here, Defendants' misuse of Plaintiffs' famous marks in connection with malicious conduct aimed at Plaintiffs' customers and the public dilutes the famous marks by tarnishment and by blurring consumers' associations with the marks. This is another clear violation of the Lanham Act, and Plaintiffs are likely to succeed on the merits. *See, e.g., Hamzik v. Zale Corp*., 2007 U.S. Dist. LEXIS 28981 (N.D.N.Y. April 18, 2007); *Hotmail Corp.*, 47 U.S.P.Q.2d at 1024, 1025-26; (spam e-mail with purported "from" addresses including plaintiff's trademarks constituted dilution); Am. Online, 24 F. Supp. 2d at 552

(same).

3. Defendants' Copyright Infringement

A certificate of registration from the U.S. Copyright Office is prima facie evidence of a copyright's validity. *See Glennon v. Rosenblum*, 325 F. Supp. 3d 1255, 1263 (N.D. Ala. 2018). The copyright certificate to Microsoft's Declaring Code constitutes prima facie evidence of the validity of the copyright. *See* 17 U.S.C. § 410(c) (2000); 4 Melville Nimmer & David Nimmer, Nimmer on Copyright § 13.01[A], at 13-7(2002); *see also Oracle Am., Inc. v. Google Inc*., 750 F.3d 1339, 1358 (Fed. Cir. 2014) (holding that Oracle's structure, sequence, and organization of its declaring code in Java was copyrightable). Microsoft has a registration for the APIs reproduced by Defendants. Finones Decl. ¶ 13; Complaint, Attachment 1.

Previous courts adjudicating similar claims by Microsoft to the claims presented here found protectable "[t]he code, called the 'Declaring Code,' … used to develop applications for Windows and enables applications to call and invoke pre-packaged functionality in libraries contained within the operating systems." *Microsoft Corp. v. Does*, 2021 U.S. Dist. LEXIS 258143, at *9 (E.D. Va. Aug. 12, 2021). Here, as in prior cases, "Defendants copied hundreds of lines of Microsoft's Declaring Code" after having "had access to the code through the SDK toolkit." Id. at *13-15. This "copying was unauthorized because the SDK License explicitly prohibits use of the Declaring Code in malicious software." Id. The Lumma malware

reproduces without authorization a substantial number of lines of code from Microsoft's copyrighted software. Fiñones Decl.¶ 13. Such reproduction is copyright infringement.

4. Defendants' Conduct Violates the RICO Act

Section 1962(c) of the RICO Act provides that:

> It shall be unlawful for 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 or collection of unlawful debt.

18 U.S.C. § 1962(c). Pursuant to this statute, to succeed on a civil RICO claim, a private RICO plaintiff must allege "(1) conduct (2) of an enterprise (3) through a pattern (4) of racketeering activity." *Viridis Corp. v. TCA Glob. Credit Master Fund, LP*, 155 F. Supp. 3d 1344, 1354 (S.D. Fla. 2015) (citation omitted). "Racketeering activity" includes any act violative of several specific federal statutes, including 18 U.S.C. § 1343 (wire fraud) and 18 U.S.C. § 1029 (access device fraud). 18 U.S.C. § 1961(1). A civil RICO plaintiff must also show that multiple acts of racketeering "(5) caused (6) injury to the business or property of the plaintiff." *Cisneros v. Petland, Inc*., 972 F.3d 1204, 1211 (11th Cir. 2020).

"Any person injured in his business or property by reason of a violation of" either of these provisions is entitled to recovery, 18 U.S.C. § l 964(c), and this court has "jurisdiction to prevent and restrain" such violations "by issuing appropriate

orders." 18 U.S.C. 1964(a). *See also* Absolute Activist Value Master Fund Ltd. v. Devine, No. 215CV328FTM29MRM, 2016 WL 1572388 at *4 (M.D. Fla. Apr. 19, 2016) (finding TRO to be proper equitable relief for private litigants in a civil federal RICO action); *United States v. Carson*, 52 F.3d 1173, 1181-82 (2d Cir. 1995) ("the jurisdictional powers in § 1964(a) serve the goal of foreclosing future violations," and "the equitable relief under RICO is intended to be broad enough to do all that is necessary"); *Trane Co. v. O'Connor Sec.*, 718 F.2d 26, 29 (2d Cir. 1983) (preliminary injunction proper under RICO where plaintiff establishes "a likelihood of irreparable harm").

Defendants are members of an ongoing association-in-fact enterprise. They are participants in the conduct of a malware-as-a-service enterprise referred to in Microsoft's Complaint as the Lumma Enterprise. Richardson Decl. ¶ 4. The creators, distributors, and operators of the Lumma malware are characterized by a high degree of sophistication and commercial organization. According to an IBM study, Lumma is the most actively advertised information stealer on the dark web by a wide margin. Lumma even has its own logo that is used in connection with efforts to monetize the malware. Id. ¶ 29.

The Defendants can be grouped into two general categories of actors. A first group of actors, DOES 1-6 ("Infrastructure Provider Defendants"), provide and control software and infrastructure needed to infect victim computers, exfiltrate

stolen data, distribute that data to other participants in Defendants' malicious enterprise, and provide a marketplace for Defendants services and/or stolen data obtained from operation of the Lumma malware. A second group of actors, DOES 7-10 ("End User Defendants"), is comprised of Lumma end users who pay Infrastructure Provider Defendants and/or Distributor Defendants for their malicious services and stolen data. End User Defendants use Lumma and stolen data to carry out financial theft. Richardson Decl. ¶¶ 34-36. DOES 8-10 are consumers in this marketplace and have engaged in at least one transaction for services or data provided by the Lumma malware and Infrastructure Defendants. Id. ¶ 42.

Defendants have conducted the affairs of the Enterprise through a coordinated and continuous pattern of illegal activity in order to achieve their common unlawful purposes. Defendants have engaged in racketeering by violating the federal wire fraud (18 U.S.C. § 1343) and access device fraud (18 U.S.C. § 1029) statutes.

Wire Fraud (18 U.S.C. § 1343). Defendants have violated the federal wire fraud statute by using the Internet to distribute malware, steal data, and engage in financial fraud. *See, e.g., United States v. Azari*, No. 19-cr-610 (JGK), 2024 U.S. Dist. LEXIS 165416, at *1 (S.D.N.Y. Sep. 10, 2024); *United States v. 113 Virtual Currency Accounts*, Civil Action No. 20-606, 2020 U.S. Dist. LEXIS 142015, at *2 (D.D.C. Aug. 4, 2020) ("the hacking and theft of virtual currencies in violation of 18 U.S.C. § 1343").

Access Device Fraud (18 U.S.C. § 1029). Whoever "knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that that period," is guilty of violating 18 U.S.C. § 1029 "if the offense affects interstate or foreign commerce." 18 U.S.C. § 1029(a)(2). An "access device" includes "any … code, account number, electronic serial number, mobile identification number [or] personal identification number … that can be used, alone or in conjunction with another access device, to obtain money … or any other thing of value, or that can be used to initiate a transfer of funds." 18 U.S.C. § 1029(e)(1). An "unauthorized access device" include "any access device that is lost, stolen ... or obtained with intent to defraud." 18 U.S.C. § 1029(e)(3). Violation of this statute constitutes "racketeering activity." 18 U.S.C. § 1961(1)(B).

Defendants have violated the Access Device Fraud statute by configuring computers to inject malicious code in order to gain access to victim computers without authorization. Fiñones Decl. ¶ 7; Aronov Decl. ¶¶ 5-6. *Synopsys, Inc. v. Ubiquiti Networks, Inc.,* No. 17-cv-00561-WHO, 2017 U.S. Dist. LEXIS 130070, at *38 (N.D. Cal. Aug. 15, 2017) ("using the counterfeit access device…in order to obtain money, goods, services, or any other thing of value" violates 1029). This access device fraud has occurred hundreds of thousands of times.

B. Defendants' Conduct Causes Irreparable Harm

Defendants' conduct causes Microsoft several types of irreparable harm. First, "[n]umerous courts have found that unauthorized access of computers and the acquisition of data in violation of the CFAA constitute irreparable harm." *Chegg, Inc. v. Doe*, No. 22-cv-07326-CRB, 2023 U.S. Dist. LEXIS 200023, at *21-22 (N.D. Cal. Nov. 7, 2023) (collecting cases). This Court and others have found that "there is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, Microsoft's customers, and the Public" under circumstances similar to those presented here. *See Microsoft Corp. v. Does 1-51*, No. 1:17-CV-4566, 2017 WL 10087886 at *2 (N.D. Ga. Nov. 17, 2017); *Microsoft Corp. v. Malikov*, No. 1:22-cv-1328-MHC, 2022 WL 1742862 at *2 (N.D. Ga. Apr. 8, 2022) (same); *see also, e.g., Microsoft Corp. v. Does*, Civil Action No. 1:21-cv-822 RDA/IDD, 2022 U.S. Dist. LEXIS 236135, at *11-12 (E.D. Va. Dec. 27, 2022) (citing *Microsoft Corp. v. Peng Yong* et al., Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (injunction to dismantle botnet command and control servers); and *Microsoft v. Piatti,* et al., Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (injunction [*12] to dismantle botnet command and control servers)); *accord Microsoft Corp. v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va. 2010, Brinkema J.) (similar).

Second, it is well settled that consumer confusion and injury to business goodwill constitute irreparable harm. *See, e.g., Int'l Labor Mgmt. Corp. v. Perez*,

2014 U.S. Dist. LEXIS 57803, 35 (M.D.N.C. Apr. 25, 2014) (damage to "reputation and loss of goodwill constitutes irreparable harm for purposes of injunctive relief") (citing *In Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co*., 22 F.3d 546 (4th Cir. 1994)); *MicroAire Surgical Instruments, LLC v. Arthrex, Inc*., 726 F. Supp. 2d 604, 635 (W.D. Va. 2010) ("The loss of goodwill is a well-recognized basis for finding irreparable harm"). A finding of irreparable harm usually follows a finding of unlawful use of a trademark and a likelihood of confusion. *Ledo Pizza Sys. v. Singh*, 2013 U.S. Dist. LEXIS 146938, 9 (D. Md. Oct. 10, 2013); *Nabisco Brands, Inc. v. Conusa Corp*., 722 F. Supp. 1287, 1290 (M.D.N.C. 1989) ("In the context of a trademark infringement dispute, several courts have held that where likelihood of confusion is established likelihood of success on the merits as well as risk of irreparable harm follow.").

Here, Defendants' conduct tarnishes Microsoft's valuable trademarks, injuring Microsoft's goodwill, creating confusion as to the source of harmful content created or facilitated by Defendants, and damaging the reputation of Microsoft and the public's confidence in Microsoft's robust safety measures. Defendants are also depriving Microsoft of the right to control the use, distribution, and modification of its copyrighted software code. *See, e.g., Compulife Software Inc. v. Newman*, 959 F.3d 1288 (11th Cir. 2020). These injuries are sufficient in and of themselves to constitute irreparable harm.

Lastly, as a practical matter, Defendants are causing harm that is unlikely to ever be compensated by monetary payment—even after final judgment—because Defendants are elusive cybercriminals whom Microsoft is unlikely to be able to enforce judgments against. "[C]ircumstances[] such as insolvency or unsatisfiability of a money judgment, can show irreparable harm." *Khepera-Bey v. Santander Consumer USA, Inc*., 2013 U.S. Dist. LEXIS 87641, 13-14 (D. Md. June 21, 2013); *accord Burns v. Dennis-Lambert Invs., Ltd. P'ship*, 2012 Bankr. LEXIS 1107, 9 (Bankr. M.D.N.C. Mar. 15, 2012) ("a preliminary injunction may be appropriate where 'damages may be unobtainable from the defendant because he may become insolvent before final judgment can be entered.'"); *Rudolph v. Beacon Indep. Living LLC*, 2012 U.S. Dist. LEXIS 7075, 5 (W.D.N.C. Jan. 23, 2012) ("Irreparable harm exists here because of Defendant Beacon's continued occupancy of the Facility without paying any rents, particularly in light of the threat of insolvency by one or more Defendants.").

C. The Balance of Equities Strongly Favors Injunctive Relief

Because Defendants are engaged in an illegal scheme to steal from Microsoft's customers in order to obtain unlawful access to Microsoft's systems, circumvent safety mitigations, and create and disseminate harmful content, the balance of equities clearly tips in favor granting an injunction. *See, e.g., US Airways, Inc. v. US Airline Pilots Ass'n*, 813 F. Supp. 2d 710, 736 (W.D.N.C. 2011); *Pesch v.*

First City Bank of Dallas, 637 F. Supp. 1539, 1543 (N.D. Tex. 1986) (balance of hardships clearly favors injunction where enjoined activity is illegal). On one side of the scales of equity rests the harm to Microsoft, its customers, and the public at large, while on the other side rests no legally cognizable harm to Defendants because an injunction would only require them to cease illegal activities. *US Airways*, 13 F. Supp. 2d at 736.

D. The Public Interest Favors an Injunction

It is clear that an injunction would serve the public interest here. The public has a strong interest in enforcing laws like the CFAA, RICO, Copyright Act, and Lanham Act. *See, e.g., ProFitness Phys. Therapy Ctr. v. Pro-Fit Ortho. And Sports Phys. Therapy P.C.*, 314 F.3d 62, 68 (2d Cir. 2002) (finding a "strong public interesting in preventing public confusion"); *BSN Med., Inc. v. Art Witkowski*, 2008 U.S. Dist. LEXIS 95338, 10 (W.D.N.C. Nov. 21, 2008) ("In a trademark case, the public interest is 'most often a synonym for the right of the public not to be deceived or confused.' . . . the infringer's use damages the public interest.") (citation omitted); *accord Meineke Car Care Ctrs., Inc. v. Bica*, 2011 U.S. Dist. LEXIS 118171, 10 (W.D.N.C. Oct. 12, 2011) (similar); *FXDirectDealer, LLC v. Abadi*, 2012 WL 1155139, at *8 (S.D.N.Y. Apr. 5, 2012) (public interest weighed in favor of injunction to enforce CFAA); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 32 (E.D. Va. Jan. 6, 2014) (public interest weighed in favor of injunction to

enforce CFAA). The public also has a strong interest in disrupting criminal enterprises operating in violation of the RICO Act. *See, e.g., Amazon.com, Inc. v. WDC Holdings LLC*, Civil Action No. 1:20-cv-484, 2020 U.S. Dist. LEXIS 134555, at *31 (E.D. Va. July 28, 2020) (granting injunction to enjoin RICO enterprise conduct). "Microsoft's proposed injunction is tailored to target and disable communication between Defendants" and to disrupt the malicious infrastructure at issue "with the least amount of burden on third party domain registries and the public," which ensures that "the public interest would not be harmed, and likely would be served, by a permanent injunction." *Microsoft Corp. v. Doe*, No. 20-CV-1217 (LDH) (RER), 2021 U.S. Dist. LEXIS 101862, at *28 (E.D.N.Y. May 28, 2021).

III. THE ALL WRITS ACT AUTHORIZES THE COURT TO DIRECT THIRD PARTIES TO PERFORM ACTS NECESSARY TO AVOID FRUSTRATION OF THE REQUESTED RELIEF

Microsoft's Proposed Order directs that the third-party service providers whose infrastructure Defendants rely on to reasonably cooperate to effectuate the order. Microsoft's proposed order also directs such entities to preserve evidence of Defendants' conduct. Microsoft has been working with private and public partners regarding remediation of Defendants misconduct, and several third-party entities are inclined to assist in removing illegal and abusive accounts from their respective services. Microsoft has observed voluntary third-party compliance with orders like

the one it seeks here in several past cases, which makes sense because it is in most companies' interests to reduce the amount of cybercrime carried out on their platforms.

In addition to the fact that many third parties are likely to voluntarily comply with orders such as the one Microsoft seeks here, the All Writs Act provides a mechanism for obtaining compliance if needed. The Act provides that a court may issue all writs necessary or appropriate for the administration of justice. 28 U.S.C. § 1651(a). The Supreme Court has recognized that narrow direction to third parties necessary to effect the implementation of a court order is authorized by the All Writs Act:

> The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice, and encompasses even those who have not taken any affirmative action to hinder justice.

United States v. New York Tel. Co., 434 U.S. at 174 (citations omitted) (order to telephone company to assist in implementation of a pen register warrant was authorized under the All Writs Act); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 30 (E.D. Va. Jan. 6, 2014) (invoking All Writs act and granting relief similar to that requested herein); *United States v. X*, 601 F. Supp. 1039, 1042 (D. Md. 1984) (All Writs Act permits the district court to order a third party to provide "nonburdensome technical assistance" in aid of valid warrant); *Moore v.*

Tangipahoa Parish Sch. Bd., 507 Fed. App'x. 389, 396 (5th Cir. 2013) (unpublished) ("The All Writs Act provides 'power to a federal court to issue such commands . . . as may be necessary or appropriate to effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained.'") (citing *New York Tel. Co*., 434 U.S. at 172); *see also In re Application of United States for an Order Authorizing An In-Progress Trace of Wire Commc'ns Over Tel. Facilities*, 616 F.2d 1122, 1129 (9th Cir. 1980) (same; noting of *New York Tel. Co*., "the Court made the commonsense observation that, without the participation of the telephone company, 'there is no conceivable way in which the surveillance authorized could have been successfully accomplished.'" 434 U.S. at 172); *In re Baldwin-United Corp*., 770 F.2d 328, 338-339 (2d Cir. 1985) ("An important feature of the All-Writs Act is its grant of authority to enjoin and bind non-parties to an action when needed to preserve the court's ability to reach or enforce its decision in a case over which it has proper jurisdiction"; "We do not believe that Rule 65 was intended to impose such a limit on the court's authority provided by the All-Writs Act to protect its ability to render a binding judgment."); *Dell Inc*., 2007 U.S. Dist. LEXIS 98676, at *16 (All Writs Act applied in conjunction with trademark seizure under Rule 65 and Lanham Act).

Requiring the third parties whose infrastructure is identified in the proposed TRO is within the Court's power under the all writs act because compliance (1)

requires only minimal assistance from such third parties in executing the order (acts that they would take in the ordinary course of their operations upon receipt of abuse notifications), (2) requires that it be implemented with the least degree of interference with the normal operation of third parties, (3) does not deprive of any tangible or significant property interests and (4) requires Microsoft to compensate for costs, if any, associated with the assistance rendered.

If, in the implementation of the Proposed Order, any third party wishes to bring an issue to the attention of the Court, Microsoft will bring any such issue to the Court's attention immediately. All affected parties will have an opportunity to be heard at the preliminary injunction hearing, which must occur shortly after the execution of the Proposed Order. *See* Fed. R. Civ. P. 65(b)(2). The third-party directions in the Proposed Order are thus narrow, satisfy Due Process, and are necessary to effect the requested relief and ensure that the relief is not rendered fruitless.

IV. AN *EX PARTE* TRO THAT REMAINS SEALED FOR A LIMITED TIME IS THE ONLY EFFECTIVE MEANS OF RELIEF

The Orders Microsoft requests herein must issue *ex parte* for the relief to be effective at all because of the extraordinary factual circumstances here—namely, Defendants' technical sophistication and ability to move their infrastructure and evidence if given advance notice of Microsoft's request for injunctive relief. Rule 65 of the Federal Rules of Civil Procedure permits an *ex parte* TRO where the

moving party sets forth facts that show an immediate and irreparable injury and why notice should not be required. Fed. R. Civ. P. 65(b)(1); *see Granny Goose Foods, Inc. v. Brotherhood of Teamsters & Auto Truck Drivers, Lcal No. 70*, 415 U.S. 423, 438-39 (1974) ("*Ex parte* temporary restraining orders are no doubt necessary in certain circumstances[.]").

If notice is given prior to issuance of a TRO, it is likely that Defendants will be able to relocate (or destroy) their infrastructure and associated artifacts before Microsoft can obtain discovery and before the TRO can have any remedial effects. Richardson Decl. ¶ 46. *Ex parte* relief is appropriate under circumstances such as the instant case, where notice would render the requested relief ineffective. *See, e.g., Microsoft Corp. v. Does 1-51,* No. 1:17-CV-4566, 2017 WL 10087886 at *2 (N.D. Ga. Nov. 17, 2017) (granting an *ex parte* TRO where there was "good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants"); *Microsoft Corp. v. Malikov*, No. 1:22-cv-1328-MHC, 2022 WL 1742862 at *2 (N.D. Ga. Apr. 8, 2022) (same); *AllscriptsMisys, LLC v. Am. Digital Networks, LLC*, 1:10-cv-00111, 2010 U.S. Dist. LEXIS 4450, at *2 (D. Md. Jan. 20, 2010) (granting an *ex parte* TRO where "Defendant may dissipate the funds and/or take action to render it difficult to recover funds ...."); *Crosby v. Petromed, Inc*., 2:09-cv-05055, 2009 U.S. Dist. LEXIS 73419, at *5 (E.D. Wash.

Aug. 6, 2009) (granting *ex parte* TRO as "notice to Defendants of this TRO request could result in further injury or damage to Plaintiffs...."); *AT&T Broadband v. Tech Commc'ns, Inc*. 381 F.3d 1309, 1319-1320 (11th Cir. 2004) (affirming *ex parte* search and seizure order to seize contraband technical equipment, given evidence that in the past defendants and persons similarly situated had secreted evidence once notice given); *Little Tor Auto Center v. Exxon Co*., U.S.A., 822 F. Supp. 141, 143 (S.D.N.Y. 1993) (*ex parte* TRO appropriate where contraband "may be destroyed as soon as notice is given"); *Kelly v. Thompson*, 2010 U.S. Dist. LEXIS 31800, *3 (W.D. Tex. Mar. 31, 2010) (granting *ex parte* TRO without notice where irreparable harm would result if notice were given); *In re Vuitton Et Fils S.A*., 606 F.2d 1, 4-5 (2d Cir. 1979) (per curiam) (holding that notice prior to issuing TRO was not necessary where notice would "serve only to render fruitless further prosecution of the action"; prior experience taught that once one member of the counterfeiting enterprise received notice, contraband would be transferred to another unknown counterfeiter, perpetuating the harm and rendering judicial efforts pointless). Courts have previously found that where, as in the instant case, Defendants' scheme is "in electronic form and subject to quick, easy, untraceable destruction by Defendants," *ex parte* relief is particularly warranted. *Dell, Inc. v. Belgiumdomains, LLC*, 1:07-cv-22674, 2007 U.S. Dist. Lexis 98676, at *5-6 (S.D. Fla. Nov. 21, 2007).

CONCLUSION

For the reasons set forth herein, Microsoft respectfully requests that this Court grant Microsoft the requested injunctive relief and order this action to remained sealed for a limited period of time necessary to effect the Court's orders.

Dated: May 14, 2025

Respectfully submitted,

/s/ Joshua D. Curry
Joshua D. Curry

Joshua D. Curry (Georgia Bar No. 117378)
Jonathan D. Goins (Georgia Bar No. 738593)
LEWIS BRISBOIS BISGAARD & SMITH LLP
600 Peachtree Street NE, Suite 4700
Atlanta, GA 30308
Tel: 404.348.8585
Fax: 404.467.8845
josh.curry@lewisbrisbois.com
jonathan.goins@lewisbrisbois.com

ROBERT L. URIARTE (*Pro Hac Vice*)
ruriarte@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
355 S. Grand Ave.
Ste. 2700
Los Angeles, CA 90017
Telephone: + 1 213 629 2020
Facsimile: + 1 213 612 2499

JACOB M. HEATH (*Pro Hac Vice*)
jheath@orrick.com
ANA M. MENDEZ-VILLAMIL (*Pro Hac Vice*)
amendez-villamil@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
The Orrick Building
405 Howard Street
San Francisco, CA 94105

Telephone: + 1 415 773 5700
Facsimile: + 1 415 773 5759

LAUREN BARON (*Pro Hac Vice*)
lbaron@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019
Telephone: + 1 212 506 5000
Facsimile: + 1 212 506 5151

Of Counsel:

RICHARD BOSCOVICH
rbosco@microsoft.com
MICROSOFT CORPORATION
Microsoft Redwest Building C
5600 148th Ave NE
Redmond, Washington 98052
Telephone: +1 425 704 0867
Facsimile: +1 425 706 7329

Attorneys for Plaintiff
MICROSOFT CORPORATION

CERTIFICATION OF COMPLIANCE

Pursuant to L.R. 7.1(D), N.D. Ga., counsel for Plaintiff hereby certifies that this Motion has been prepared with one of the font and point selections approved by the Court in L.R. 5.1, N.D. Ga.

Dated: May 14, 2025 */s/ Joshua D. Curry*