

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

MICROSOFT CORPORATION,

Plaintiff,

v.

DOES 1-6,

Defendants.

Case No. \_\_\_\_\_

**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 .....1

STATEMENT OF FACTS .....3

    Lumma Malware .....3

    Disruption and Adaptation of the Lumma C2 Infrastructure.....5

ARGUMENT .....6

    I. The Court Has Jurisdiction.....6

    II. The Record Supports a Temporary Restraining Order and Preliminary  
        Injunctive Relief.....8

        A. Microsoft is Likely to Succeed on the Merits of Its Claims .....8

        B. Defendants’ Conduct Causes Irreparable Harm .....14

        C. The Balance of Equities Strongly Favors Injunctive Relief.....15

        D. The Public Interest Favors an Injunction.....16

        E. The Bond from *Lumma I* Is Sufficient Security for the TRO/PI.....17

    III. The All Writs Act Authorizes the Court to Direct Third Parties to  
        Perform Acts Necessary to Avoid Frustration of the Requested Relief .....18

    IV. An *Ex Parte* TRO that Remains Sealed for a Limited Time is the Only  
        Effective Means of Relief .....21

CONCLUSION.....23

## INTRODUCTION

This case involves a group of DOE Defendants 1-6 (“DOES” or “Defendants”) who are already before the Court as “Infrastructure Provider Defendants” in *Microsoft v. Does 1-10*, N.D.GA Case No.” 1:25-cv-02695-MHC (“*Lumma I*”). Both this case and *Lumma I* involve Defendants’ distribution and use of malicious software commonly known as the LummaStealer or LummaC2 malware (“Lumma”). Defendants’ exploitation of Lumma depends on use of internet domains, including several domains that were the subject of the Court’s previous injunction order in *Lumma I*. In response to successful disruption of their Lumma command and control infrastructure under the Court’s prior preliminary injunction, Defendants have now set up new internet domains in order to continue their ongoing violations of law. Accordingly, Microsoft moves for emergency *ex parte* relief of the same type granted in *Lumma I* regarding Defendants new command and control domains.<sup>1</sup> Specifically, 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;

---

<sup>1</sup> Microsoft believes that this Application is ripe for adjudication on the papers given the related relief granted in *Lumma I*. To the extent the Court requires live testimony or has technical questions, Microsoft’s lead counsel and principal fact witness can be available by phone or video conference on short notice, as they are unable to travel to the District this week due to logistical problems caused by ongoing FAA flight cancelations and their professional and personal obligations.

(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.

Because prior notice to Defendants of Microsoft's motion would provide Defendants to move their infrastructure to new domains before Microsoft can obtain effective relief from the Court, Microsoft seeks relief *ex parte* and has moved to temporarily seal this action until after execution of the Court's orders. 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 fruitless the relief requested in this Application. *Ex parte* relief is not uncommon when disabling an online command and control infrastructure used by unidentified defendants for illegal operations and cybercrime schemes.<sup>2</sup>

If Microsoft's requests for relief are granted, Microsoft will work with its private and public partners to disable the Defendants new infrastructure in a carefully

---

<sup>2</sup> See, e.g., *Microsoft Corp. v. Does 1-10*, No. 1:25-CV-2695-MHC, slip op. ECF #15 (N.D. Ga. May 15, 2025); *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.); *Sophos v. John Does 1-2*, Case No. 1:20-cv-00502 (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.).

timed and coordinated manner that should prevent 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.

### **STATEMENT OF FACTS**

Plaintiff Microsoft Corp. is a leading provider of technology products and services, including computer software, Internet services, and email services. DOES 1-6 are associated with creating, distributing, operating, and selling Lumma malware and associated services as part of a Lumma Malware Enterprise. Declaration of Derek Richardson, ¶¶ 4-10. In general, the Lumma Malware 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 in furtherance of financial crimes.

DOES 1-6 are natural persons believed to reside outside the United States, potentially in Russia. Richardson Decl. ¶ 4. DOES 1-6 provide infrastructure and related services to end users. Among other things, DOES 1-6 provide internet domains that act as C2 infrastructure for Lumma. Richardson Decl. ¶¶ 4-10.

### **Lumma Malware**

Lumma is an information stealer designed to collect data stored in browsers, including session tokens and cookies, saved passwords and input form data, credit

card information, and cryptocurrency wallets. Richardson Decl. ¶ 24. 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. Richardson Decl. ¶ 24. Defendants use various additional types of social engineering technics to infect victim computers. *Id.* ¶¶ 25-26.

Lumma is specifically designed to attack Microsoft's software and customers. Richardson Decl. ¶ 29. Lumma's designers created purpose-built code for bypassing Microsoft antivirus protections. *Id.* ¶ 30. 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. ¶ 37.

Analysis of Lumma shows that the malware targets several types of victim information including user's files, credentials from browsers (login data like username, passwords and credit card numbers), crypto wallets and extensions, and data associated with VPN, FTP, and email applications. Richardson Decl. ¶ 32. For example, if Microsoft's 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.*

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

### **Disruption and Adaptation of the 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. These C2 servers are associated with specific domains that are either hardcoded into the Lumma malware or provided through third party communications tools. Microsoft refers to these domains as C2 domains. Microsoft initially identified over 2,300 hardcoded C2 domains used by Defendants. Many of those domains have now been disabled or abandoned as a result of *Lumma I*’s preliminary injunction order and related work by Microsoft and its partners. Richardson Decl.¶ 43.

The Court’s prior orders in *Lumma I* caused Defendants to lose the ability to control or communicate with victim computers via C2 domains that were seized pursuant to the court orders, voluntarily taken down as the result of action by Microsoft or its partners, or abandoned by Defendants. Richardson Decl.¶ 43.

However, Defendants set up new C2 domains after they learned of this case and attempted to circumvent the efforts of Microsoft and law enforcement by moving certain infrastructure and by releasing new versions of the Lumma malware containing lists of new C2 domains. Richardson Decl.¶ 43. Nevertheless, there are at least several new active C2 domains that can be disrupted via action with U.S.-based ISPs.

Microsoft believes it will be able to disable numerous command-and-control domains through domain abuse channels, industry partner cooperation, and orders providing for preliminary injunctive relief of the type issued in *Lumma I*. Microsoft also believes it will be able to help victims and remediate infected computers by obtaining control over the C2 domains at issue in this motion. However, Microsoft will not be able to achieve effective relief if Defendants are given prior notice of Microsoft's ex parte application because Defendants will likely release new malware versions pointing to a new set of C2 domains before any TRO can be given effect.

## **ARGUMENT**

### **I. THE COURT HAS JURISDICTION**

The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises under federal statutes. 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); *United States v. Auernheimer*, 748 F.3d 525, 533 (3d Cir. 2014); Richardson Decl. ¶ 11.

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 (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; (ii) abusing the infrastructures of companies like Cloudflare, Verisign, and other ISPs 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; and (v) contracting with and abusing the services of U.S.-based Registrars. Richardson

Decl. ¶ 12. Accordingly, 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); 18 U.S.C. § 1965.

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

“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).

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

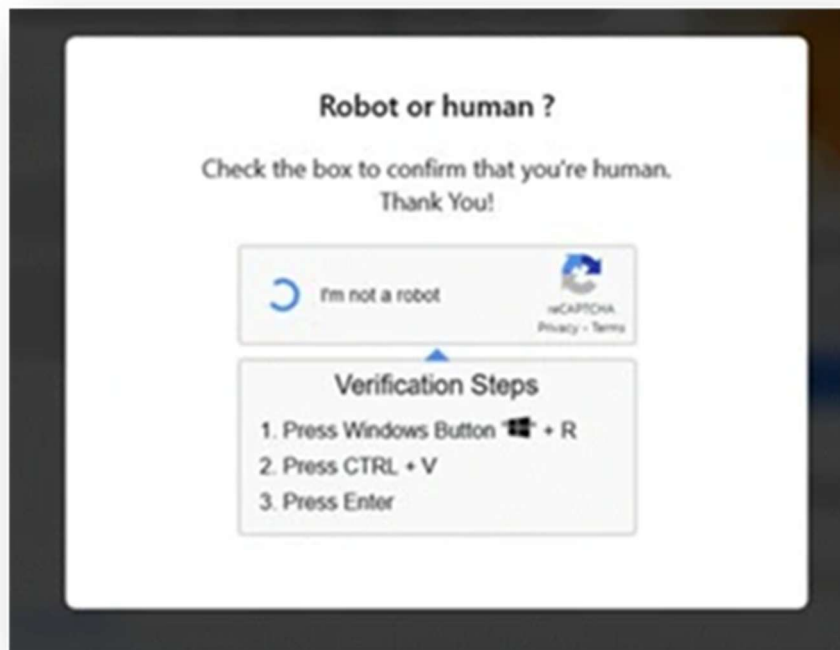
Microsoft’s evidence shows it will be able to establish the elements of each of its claims. The evidence in support of Microsoft’s TRO application is based on the diligent work of experienced investigators and is supported by substantial empirical evidence and forensic documentation.

**CFAA Claim.** 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. See, e.g., *Big Rock Sports, LLC v. AcuSport Corp.*, 2011 U.S. Dist. LEXIS 110995, \*3 (E.D.N.C. Sept. 26, 2011). Microsoft has evidence to support 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). Third, Defendants’ conduct has caused harm to Microsoft exceeding \$5,000, including substantial time spent by Microsoft personnel such as Mr. Richardson. *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) (expenses for legal counsel, cybersecurity consulting, and employees’ time).

**Trademark Claims.** 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.” The Lanham Act also 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. Further, 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, e.g., 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); *Hotmail Corp. v. Van\$ Money Pie, Inc.*, 1998 U.S. Dist.

LEXIS 10729, \*12-13 (N.D. Cal. 1998) (copying the Hotmail trademarks in “e-mail return addresses” constituted false designation of origin). In addition, Defendants cause Lumma to inject malicious code into legitimate Windows processes, 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); *Microsoft Corp. v. Doe*, 2021 U.S. Dist. LEXIS 101862, at \*13-14 (E.D.N.Y. May 28, 2021).

**Copyright Claims.** 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). Here, as in prior cases supporting injunctive relief, “Defendants copied hundreds of lines of Microsoft’s Declaring Code” after having “had access to the code through the SDK toolkit.” *Microsoft Corp. v. Does*, 2021 U.S. Dist. LEXIS 258143, at \*9, \*13-15 (E.D. Va. Aug. 12, 2021). 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 and such reproduction is copyright infringement.

**RICO Claims.** 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), 18 U.S.C. § 1029 (access device fraud), 18 U.S.C. § 2320 (trademark counterfeiting), and 18 U.S.C. § 2319 (criminal copyright infringement). 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. § 1964(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).

Defendants 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. This Enterprise has caused harm to Microsoft and its

customers as discussed above and below. Defendants have conducted the affairs of the Enterprise through a coordinated and continuous pattern of illegal by repeatedly violating the federal wire fraud statute (18 U.S.C. § 1343), engaging in access device fraud (18 U.S.C. § 1029), trademark counterfeiting (18 U.S.C. §2320) and violating the criminal copyright statute (18 U.S.C. § 2319). First, 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”). Second, 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. *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). Third, Defendants have distributed counterfeit Microsoft trademarks as described on pages 9 and 10 above. Fourth, Defendants have engaged in a pattern of criminal copyright infringement. “Section 2319 criminalizes violations of 17 U.S.C. § 506(a),” while “17 U.S.C. § 506(a)(1), in turn, makes liable those ‘who infringe[] a copyright

willfully . . . (1) for purposes of commercial advantage or private financial gain.” *Stewart v. Wachowski*, No. CV 03-2873 MMM (VBKx), 2005 U.S. Dist. LEXIS 46703, at \*14-15 (C.D. Cal. June 13, 2005).

**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.” *E.g.*, *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); *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). Second, 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); *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.”). 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 its copyright rights. *See, e.g., Compulife Software Inc. v. Newman*, 959 F.3d 1288 (11th Cir. 2020).

Lastly, as a practical matter, Defendants are causing harm that is unlikely to ever be compensated by monetary payment because Defendants are elusive cybercriminals. *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.'").

**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 interest 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).

**E. The Bond from *Lumma I* Is Sufficient Security for the TRO/PI**

Rule 65(c) requires movant “give[] security in an amount that the court considers proper to pay the costs and damages sustained by any party found to have been wrongfully enjoined or restrained.” “[I]t is well-established that ‘the amount of security required by the rule is a matter within the discretion of the trial court ...[, and] the court may elect to require no security at all.’” *BellSouth Telecommunications, Inc. v. MCIMetro Access Transmission Servs., LLC*, 425 F.3d 964, 971 (11th Cir. 2005) (quoting *City of Atlanta v. Metro. Atlanta Rapid Transit Auth.*, 636 F.2d 1084, 1094 (5th Cir. Feb. 13, 1981)).<sup>3</sup> In *Lumma I*, the Court approved and Microsoft posted a bond of \$25,000 as security. *See Microsoft Corp. v. Does 1-10*, No. 1:25-CV-2695-MHC (N.D. Ga. May 15, 2025) (“*Lumma I*”) at

---

<sup>3</sup> Decisions of the Fifth Circuit prior to October 1, 1981 have been adopted as “binding as precedent in the Eleventh Circuit.” *Bonner v. City of Prichard*, 661 F.2d 1206, 1207 (11th Cir. 1981) (en banc).

Dkt. Entry dated 6/12/2025 (receipt #100019912). This \$25,000 bond should also be held as security in the instant case.

**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, Local 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 their infrastructure and associated artifacts before Microsoft can obtain discovery and before the TRO can have any remedial effects. Richardson

Decl. ¶ 45. *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 relief and order this action to remain sealed for a limited period of time necessary to effect the Court’s orders.

Dated: November 12, 2025    Respectfully submitted,

/s/ Joshua D. Curry

Joshua D. Curry (Georgia Bar No. 117378)  
Jonathan D. Goins (Georgia Bar No. 738593)  
Abigail Van Horn (Georgia Bar No. 253790)

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  
abigail.vanhorn@lewisbrisbois.com

ROBERT L. URIARTE (*Pro Hac Vice*  
forthcoming)  
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

*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: November 12, 2025     /s/Joshua D. Curry