

Exhibit 12

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X	:	
MICROSOFT CORPORATION,	:	
	:	
Plaintiff,	:	Case No. 23 Civ. 10685 (PAE)
-against-	:	
	:	
DUONG DINH TU,	:	
LINH VAN NGUYEN, and	:	
TAI VAN NGUYEN,	:	<u>REQUEST TO FILE UNDER SEAL</u>
	:	
Defendants.	:	
-----X	:	

**MICROSOFT’S MOTION FOR AN *EX PARTE* SUPPLEMENTAL
PRELIMINARY INJUNCTION ORDER**

Pursuant to Federal Rule of Civil Procedure 65, Plaintiff Microsoft Corporation (“Microsoft”) files this motion for an *ex parte* supplemental preliminary injunction order (the “Motion”). Plaintiff seeks to enjoin Defendants from their ongoing (1) violations of the Lanham Act (15 U.S.C. §§ 1114 *et seq.*, 1125(a), (c)), (2) violations of the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962), (3) tortious interference with Microsoft’s business relationships with its customers, (4) conversion of Microsoft’s property, (5) trespass to Microsoft’s chattels, and (6) unjust enrichment at Microsoft’s expense.

As set forth in Plaintiff’s Memorandum of Law, as well as the Declaration of Jason Lyons in support of the Motion, evidence shows that Defendants are continuing to market and sell tools for fraudulently obtaining Microsoft accounts and other criminal services (Defendants’ “Fraudulent Enterprise”) in a manner comparable to that described in Plaintiff’s Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause (ECF No. 12), now through a new Internet domain known as “rockcaptcha.com” (the “RockCAPTCHA Website”).

Accordingly, Plaintiff requests an order directing the RockCAPTCHA Website's (1) registry operator to change the registrar of record for the domain to Plaintiff's registrar of choice, which will then change the registrant of the domain to Plaintiff, and to take reasonable steps to work with Plaintiff to ensure the transfer of the domain; and (2) hosting service provider to disable all services provided thereto. It is imperative that this action be effectuated on an *ex parte* basis, shielded from anyone associated with the Fraudulent Enterprise, until it is complete. If Defendants are alerted to these efforts prior to completion, there is substantial risk they will relocate the infrastructure to an alternative domain or domains, thwarting this attempt to stop the Fraudulent Enterprise.

Microsoft respectfully requests that this Court grant its Motion.

Dated: July 23, 2024
New York, New York

CAHILL GORDON & REINDEL LLP

By: 

Brian T. Markley
Samson A. Enzer
Jason Rozbruch
32 Old Slip
New York, New York 10005

MICROSOFT CORPORATION
Sean Farrell
One Microsoft Way
Redmond, Washington 98052

Counsel for Plaintiff Microsoft Corporation

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X
MICROSOFT CORPORATION, :
 :
 :
 Plaintiff, : Case No. 23 Civ. 10685 (PAE)
 -against- :
 :
 :
 DUONG DINH TU, :
 LINH VAN NGUYEN, and :
 TAI VAN NGUYEN, : **REQUEST TO FILE UNDER SEAL**
 :
 Defendants. :
-----X

DECLARATION OF JASON LYONS IN SUPPORT OF
MICROSOFT’S MOTION FOR AN *EX PARTE* SUPPLEMENTAL
PRELIMINARY INJUNCTION ORDER

I, Jason Lyons, declare as follows:

1. I am a Principal Manager of Investigations in the Digital Crimes Unit (“DCU”) Cybercrime Enforcement Team at Microsoft Corporation (“Microsoft”). I respectfully submit this declaration in support of Microsoft’s motion for an *ex parte* supplemental preliminary injunction order in the above-captioned case.

2. In my role at Microsoft, I assess technological security threats to Microsoft and the impact of such threats on Microsoft’s business and customers. Among my responsibilities are protecting Microsoft’s online service assets from network-based attacks. I also participate in the investigation of malware¹ and court-authorized countermeasures to neutralize and disrupt malware. For example, I have personally investigated and assisted in the court-authorized

¹ Malware is malicious software that is designed specifically to disrupt, damage, or gain unauthorized access to a computer system.

takedown of several families of malware or botnets while at Microsoft, including the malware families and botnets known as Ramnit, ZeroAccess, Dorkbot, and Necurs.

3. Before joining Microsoft, I held cybersecurity-related positions for Xerox and Affiliated Computer Services (“ACS”), and in those roles I provided in-court testimony in connection with a temporary restraining order application concerning the misappropriation of ACS’s intellectual property. Prior to entering the private sector, from 1998 to 2005, I served as a Counterintelligence Special Agent in the United States Army. My duties as a Counterintelligence Special Agent included investigating and combating cyber-attacks against the United States. I obtained certifications in counterintelligence, digital forensics, computer crime investigations, and digital media collection from the United States Department of Defense.

4. In connection with Plaintiff’s December 2023 motion for an emergency *ex parte* temporary restraining order and order to show cause (“TRO Motion”), I was involved in investigating the structure and function of an online criminal enterprise—referred to herein as the “Fraudulent Enterprise” (or the “Enterprise”)—that is in the business of using fraud and deception to breach Microsoft’s security systems, opening Microsoft accounts in the names of fictitious users, and then selling these fraudulent Microsoft accounts to cybercriminals for use in a wide variety of internet-based crimes. The Fraudulent Enterprise has caused, and continues to cause, substantial damage to Microsoft and other parties, which, if permitted to continue, will compound over time.

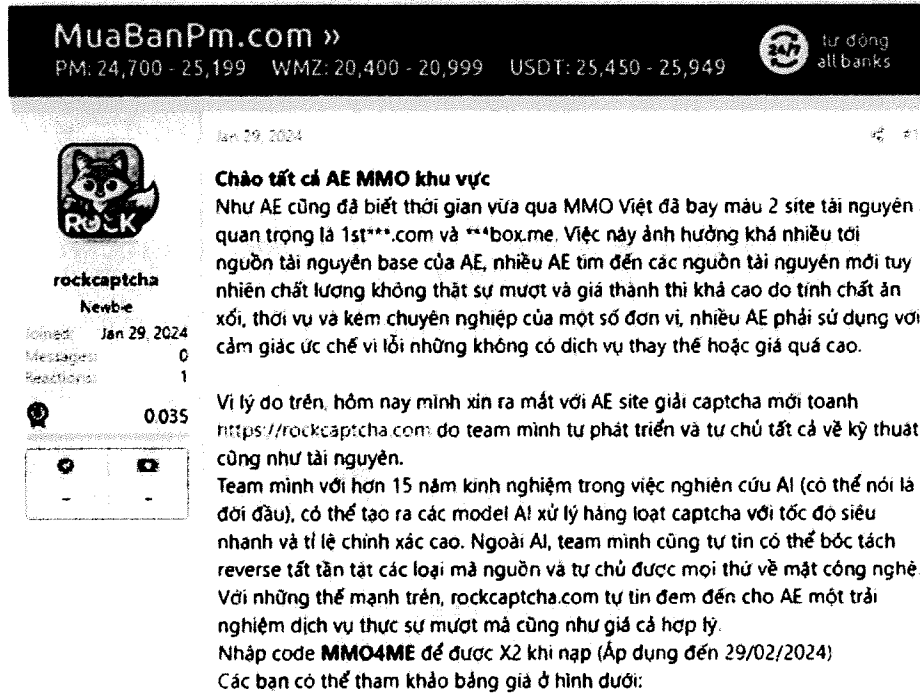
5. I make this declaration based upon my personal knowledge, and upon information and belief from my review of documents and evidence collected during Microsoft’s investigation of the Fraudulent Enterprise.

6. On December 12, 2023, Microsoft worked with third-party registry operators and service providers to execute this Court's Temporary Restraining Order ("TRO"). While the fraudulent activity attributable to the Fraudulent Enterprise ceased following the TRO, I and other Microsoft investigators have recently discovered that Defendants reconstituted their unlawful infrastructure under a new domain, "rockcaptcha.com" (the "RockCAPTCHA Website"), and are again engaging in the same fraudulent conduct prohibited by the TRO. To investigate and identify this new infrastructure and domain, I and other Microsoft investigators used the same investigative methods described in connection with my previous declaration in support of the TRO Motion.

7. Using those same investigative methods, I discovered, on an internet forum that I know is commonly used for the sale of tools used for cybercrime, the blog post reflected in Figure 1. The post, when roughly translated into English,² states, "recently . . . ha[ve] lost two important resource sites, 1st***.com and ***box.me. . . . For the above reason, today I would like to launch . . . the brand new captcha solving site <https://rockcaptcha.com> developed by my team[.]" I understand the post's references to "1st***.com" and "****box.me" to be referring to 1stcaptcha.com and hotmailbox.me, which were the websites targeted by our initial infrastructure disruption effort in this matter. Based on my experience and these investigative methods, which include internal tools available to me at Microsoft, I have concluded that the Defendants are both the authors of this post and the creators of the RockCAPTCHA Website.

² The post is publicly available in Vietnamese at the following link: <https://mmo4me.com/threads/rockcaptcha-com-giai-captcha-twitter-hotmail-recaptcha-toc-do-ban-tho-gia-sieu-re.475942/> (Jan. 29, 2024).

FIGURE 1

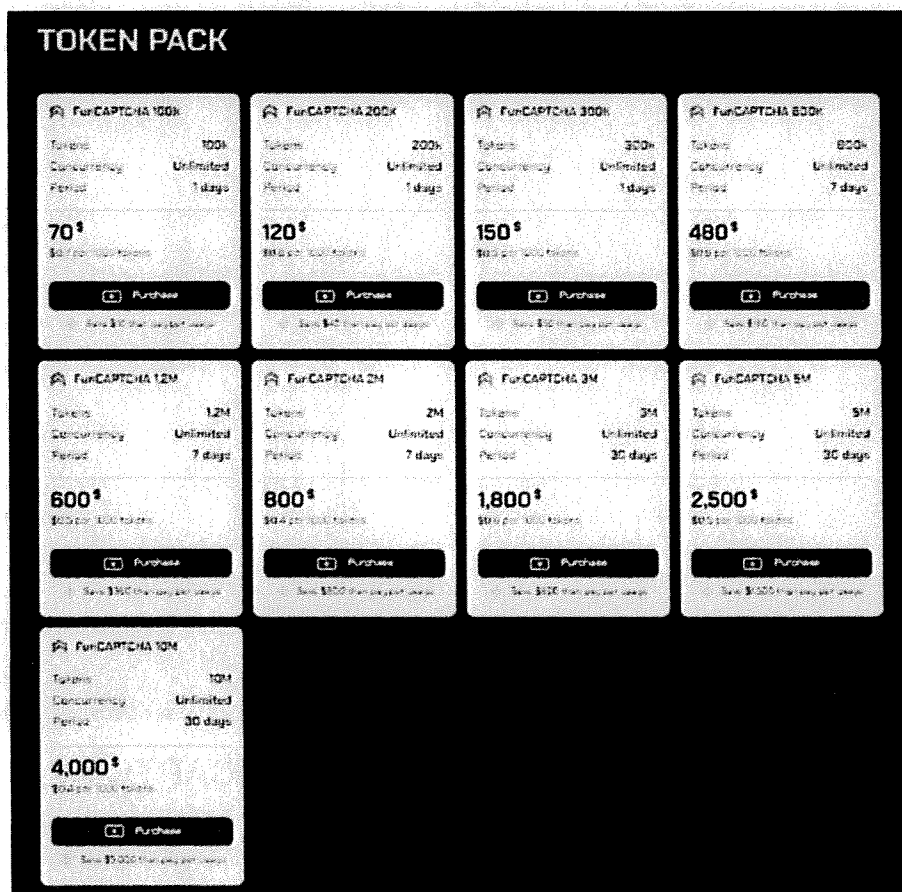


8. The RockCAPTCHA Website targets Microsoft by offering services specifically designed to defeat the CAPTCHA security measures of Arkose Labs, which are employed by Microsoft as described in the original TRO Motion. Below at Figures 2 and 3 are screenshots of portions of the RockCAPTCHA Website.

FIGURE 2

	PAY PER USAGE	Price/1000	Speed	Valid rate
☆	reCAPTCHA Token V2	\$ 0.30	10 seconds	99%
☆	reCAPTCHA Token V3	\$ 0.30	2 seconds	99.8%
☆	reCAPTCHA V2 Enterprise	\$ 0.30	16 seconds	99%
☆	reCAPTCHA V3 Enterprise	\$ 0.30	4 seconds	99%
☆	reCAPTCHA Recognition	\$ 0.18	0.5 second	99%
☆	FunCAPTCHA Token	\$ 0.80	1 seconds	100%
☆	Image to Text	\$ 0.30	1 second	95%

FIGURE 3



9. Moreover, a video titled “RockCAPTCHA Extension to Bypass FunCAPTCHA,” which is publicly available at <https://www.youtube.com/watch?v=JLulSoca3wg>, and which was posted by the YouTube channel, @ROCKCAPTCHA, on April 4, 2024, demonstrates that the services provided by the RockCAPTCHA Website are intended to be used for Microsoft Outlook in particular. The video’s description states, “[t]his video will guide you on how to set up the Rock CAPTCHA Extension to bypass Fun CAPTCHA on the Outlook/Hotmail [] creation page.” A screenshot of the portion of the video dedicated to explaining how to defeat Microsoft’s CAPTCHA security measures can be seen below at Figure 4. This video also demonstrates that Defendants make unauthorized use of Microsoft’s registered trademark. A zoomed-in side-by-side comparison of the screenshot below with Microsoft’s trademark is depicted in Figure 5.

FIGURE 4

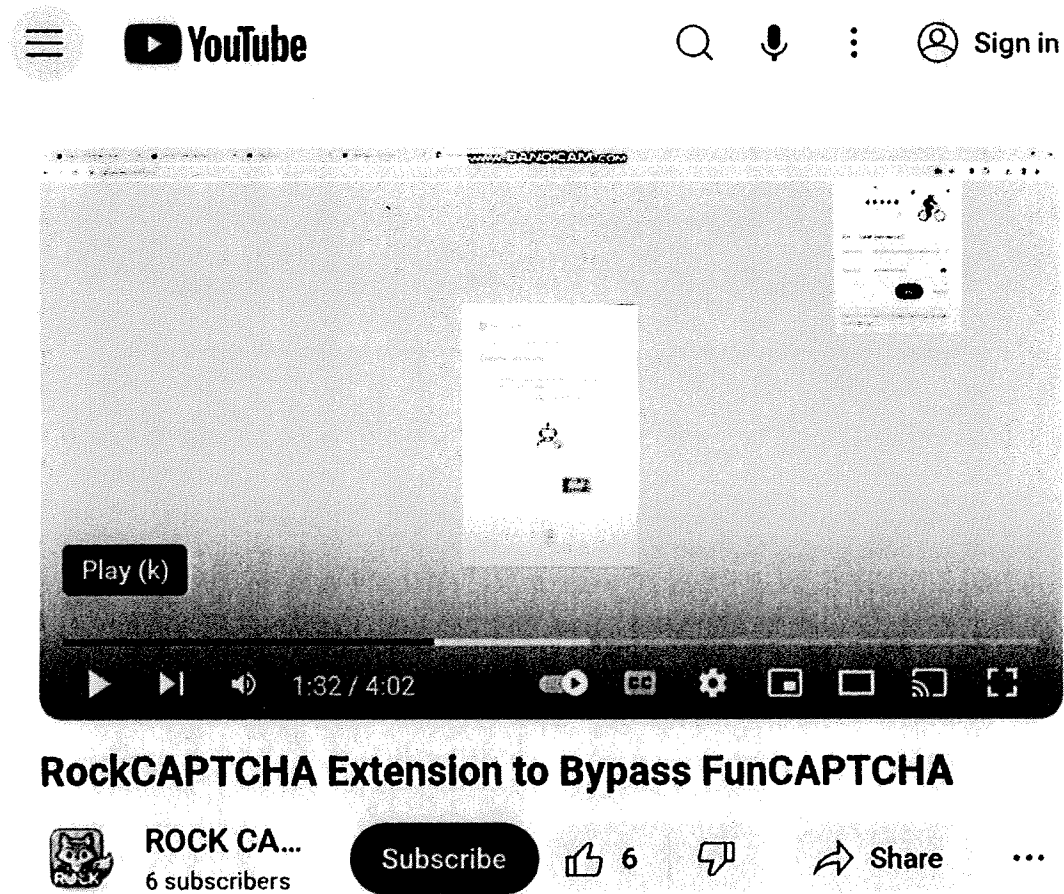


FIGURE 5



10. As reflected below in Figures 6 and 7, Defendants are also actively marketing the RockCAPTCHA Website through the Facebook page, "RockCaptcha," which is publicly available at https://www.facebook.com/people/RockCaptcha/61557799251236/?_rdr. The RockCaptcha Facebook page was created on March 21, 2024.

FIGURE 6

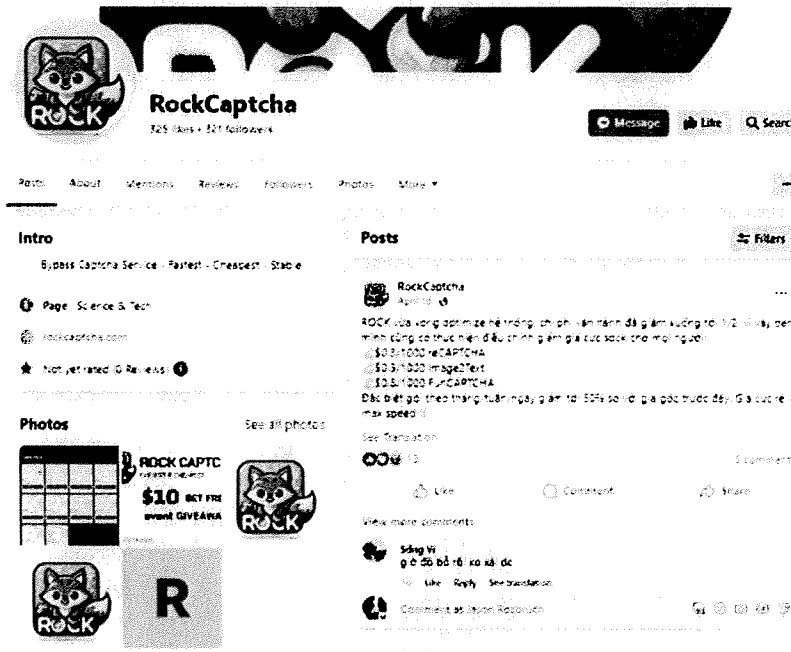
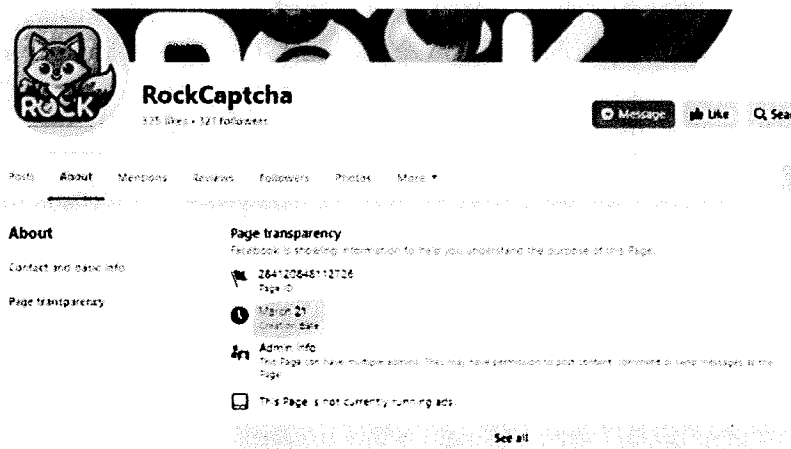


FIGURE 7



11. This conduct gives rise to the same harm to Microsoft that was described in detail in my December 5, 2023 Declaration (ECF No. 15).

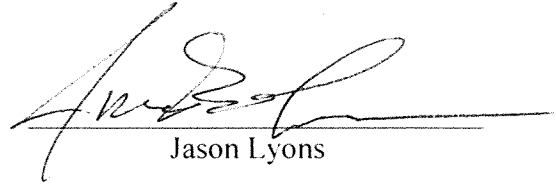
12. Through this lawsuit, Microsoft is requesting judicial authorization to direct VeriSign, Inc., the registry operator for .com domain names, including rockcaptcha.com, and Vultr, the RockCAPTCHA Website’s hosting provider, to take specific actions that would disrupt

this scheme. It is critical that these actions be shielded from anyone associated with the Enterprise—including the Defendants named in this action—until complete. If Defendants become aware of these efforts prior to their completion, there is a substantial risk that Defendants will relocate the infrastructure to alternative domains prior to the effectuation of this Court’s Order, and these efforts to stop the Fraudulent Enterprise will be thwarted. The actions set forth in the Proposed *Ex Parte* Supplemental Preliminary Injunction Order (“Proposed Order”) will be carried out immediately upon entry and will prevent Defendants from operating the RockCAPTCHA Website, which directly supports their Fraudulent Enterprise. Although the Defendants have already demonstrated an ability to reconstitute their malicious infrastructure following Microsoft’s disruption efforts, their new, reconstituted websites operate on a much lesser scale, with far fewer customers. I believe based on my experience that additional, unannounced disruptions of these illicit operations will further frustrate Defendants’ efforts to maintain and add customers, weaken their credibility in the marketplace, and ultimately cause the Fraudulent Enterprise to fail.

13. I believe that the steps described in the Proposed Order are appropriate and necessary to suspend the ongoing harm caused by the Fraudulent Enterprise on Microsoft, its consumers, and the public.

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

Executed on this 17 day of July, 2024 in Redmond, WA.


Jason Lyons

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X
MICROSOFT CORPORATION, :
 :
 : Plaintiff, : Case No. 23 Civ. 10685 (PAE)
 :
 -against- :
 :
 : DUONG DINH TU, :
 : LINH VAN NGUYEN, and :
 : TAI VAN NGUYEN, : **REQUEST TO FILE UNDER SEAL**
 :
 : Defendants. :
-----X

DECLARATION OF JASON ROZBRUCH IN SUPPORT OF
PLAINTIFF MICROSOFT'S MOTION FOR AN *EX PARTE* SUPPLEMENTAL
PRELIMINARY INJUNCTION ORDER

I, Jason Rozbruch, declare as follows:

1. I am an attorney with the law firm of Cahill Gordon & Reindel LLP and am counsel for Plaintiff Microsoft Corporation ("Microsoft") in the above-captioned action. I make this declaration in support of Microsoft's Motion for an *Ex Parte* Supplemental Preliminary Injunction Order, to put copies of certain documents before the Court that are referenced in Microsoft's motion papers.

2. Attached hereto as Exhibit 1 is a true and correct copy of the Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause, entered by this Court in the above-captioned action on December 7, 2023.

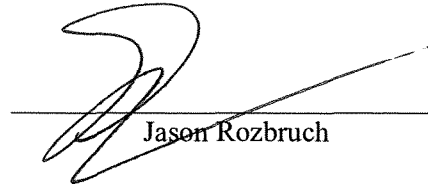
3. Attached hereto as Exhibit 2 is a true and correct copy of the June 16, 2023 Order Granting *Ex Parte* Motion to Supplement the Preliminary Injunction (ECF No. 24) in the matter of *Microsoft Corp. v. John Does 1-2*, No. 1:23-cv-02447 (E.D.N.Y. 2023).

4. Attached hereto as Exhibit 3 is a true and correct copy of the December 6, 2016 Supplemental Preliminary Injunction Order (ECF No. 49) in the matter of *Microsoft Corp. v. John Does 1-2*, No. 1:16-cv-00993 (E.D. Va. 2016).

5. Attached hereto as Exhibit 4 is a true and correct copy of the May 22, 2019 Supplemental Injunction Order (ECF No. 21) in the matter of *Microsoft Corp. v. John Does 1-2*, No. 1:19-cv-00716 (D.D.C. 2019).

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

Executed on this 23 day of July, 2024 in New York, New York.



Jason Rozbruch

Exhibit 1

JUDGE FALLA

23 CV 10685

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X
MICROSOFT CORPORATION, :
: :
Plaintiff, : Case No.
-against- : :
: :
DUONG DINH TU, :
LINH VAN NGUYEN, and :
TAI VAN NGUYEN, : **REQUEST TO FILE UNDER SEAL**
: :
Defendants. :
-----X

~~[PROPOSED]~~ ^g **EMERGENCY EX PARTE TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE**

Plaintiff Microsoft Corp. (“Microsoft”) has filed a Complaint for injunctive and other relief for (1) violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962; (2) trademark infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.*; (3) false designation of origin, federal false advertising, and federal unfair competition under the Lanham Act, 15 U.S.C. § 1125(a); (4) trademark dilution under the Lanham Act, 15 U.S.C. § 1125(c); (5) tortious interference with business relationships; (6) conversion; (7) trespass to chattels; and (8) unjust enrichment. Plaintiff has also moved *ex parte* for an emergency temporary restraining order pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(d) (the Lanham Act) and 28 U.S.C. § 1651(a) (the All Writs Act), and an order to show cause why a preliminary injunction should not be granted.

I. FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiff's Motion for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause Regarding Preliminary Injunction ("TRO Motion"), the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint adequately states claims upon which relief may be granted against Defendants for (1) violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962; (2) trademark infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.*; (3) false designation of origin, federal false advertising, and federal unfair competition under the Lanham Act, 15 U.S.C. § 1125(a); (4) trademark dilution under the Lanham Act, 15 U.S.C. § 1125(c); (5) tortious interference with business relationships; (6) conversion; (7) trespass to Chattels; and (8) unjust enrichment.

2. Microsoft owns the following registered trademarks: (1) Outlook launch icon mark, (2) Outlook word mark, and (3) Hotmail word mark. Copies of the trademark registrations for the Microsoft marks are attached as **Appendix B** to the Complaint.

3. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that constitute (1) violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962; (2) trademark infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.*; (3) false designation of origin, federal false advertising, and federal unfair competition under the Lanham Act, 15 U.S.C. § 1125(a); (4) trademark dilution under the Lanham

Act, 15 U.S.C. § 1125(c); (5) tortious interference with business relationships; (6) conversion; (7) trespass to chattels; and (8) unjust enrichment.

4. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from Defendants' ongoing (1) violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962; (2) trademark infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.*; (3) false designation of origin, federal false advertising, and federal unfair competition under the Lanham Act, 15 U.S.C. § 1125(a); (4) trademark dilution under the Lanham Act, 15 U.S.C. § 1125(c); (5) tortious interference with business relationships; (6) conversion; (7) trespass to chattels; and (8) unjust enrichment. The evidence set forth in Plaintiff's TRO Motion and the accompanying declarations and exhibits demonstrates that Plaintiff is likely to prevail on its claims that Defendants have engaged in violations of the foregoing laws, including by participating in the conduct and affairs of a criminal enterprise, hereinafter referred to as the "Fraudulent Enterprise," through a pattern of racketeering activity, by perpetrating an ongoing scheme to use Internet "bots" to hack into and deceive Microsoft's security systems into believing that they are legitimate human consumers of Microsoft services, open Microsoft Outlook email accounts in names of fictitious users, and sell those fraudulent accounts to cybercriminals for use as tools in perpetrating a wide variety of online crimes. There is good cause to believe that if such conduct continues, irreparable harm will occur to Plaintiff and the public, including Plaintiff's customers. There is good cause to believe that the Defendants are engaging, and will continue to engage, in such unlawful actions if not immediately restrained from doing so by Order of this Court.

5. There is 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 of the technological infrastructure used by the Fraudulent Enterprise to carry out its illegal objectives that is hosted at and otherwise operates through the Internet domains listed in **Appendix A**, through (1) VeriSign, Inc., as the manager and operator of 1stcaptcha.com, anycaptcha.com, and nonecaptcha.com; (2) Identity Digital Inc. (formerly Afilias Inc.), as the manager and operator of hotmailbox.me; (3) Cloudflare, Inc., as the service provider of 1stcaptcha.com, anycaptcha.com, nonecaptcha.com, and hotmailbox.me; (4) Cloud South, as the service provider of 1stcaptcha.com, anycaptcha.com, nonecaptcha.com, and hotmailbox.me, and (5) through the following Internet Protocol (“IP”) addressees, which are associated with Defendants’ Fraudulent Enterprise: 104.22.5.58, 104.22.4.58, 172.67.13.19, 104.26.11.230, 172.67.69.233, 172.67.12.153, 154.27.66.194, 154.27.66.246, 172.66.41.15, 172.66.42.241, 188.114.98.229, 104.26.13.192, 172.67.72.186, 104.26.12.192, 188.114.98.229, and 188.114.99.229 (“Defendants’ IP Addresses”), and from the destruction or concealment of other discoverable evidence of Defendants’ misconduct available at those locations if Defendants receive advance notice of this action. Based on the evidence cited in Plaintiff’s TRO Motion and accompanying declarations and exhibits, Plaintiff is likely to be able to prove that: (1) Defendants are engaged in activities that directly violate U.S. law and harm Plaintiff and the public, including Plaintiff’s customers; (2) Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests; (3) Defendants are likely to delete or relocate the Fraudulent Enterprise infrastructure at issue in Plaintiff’s TRO Motion and the harmful, malicious, and trademark-infringing products and services disseminated through Defendants’ IP Addresses and the domains listed in **Appendix A** and to warn their associates engaged in such activities if informed of Plaintiff’s action. Plaintiff’s request for this emergency *ex parte* relief is not the result of any lack of diligence on Plaintiff’s part, but instead is based upon the nature of Defendants’

unlawful conduct and the likelihood that notice of this action before the temporary restraining order sought by Plaintiff can be fully executed risks frustrating the relief sought. Therefore, in accordance with Fed. R. Civ. P. 65(b) and 15 U.S.C. § 1116(d), good cause and the interests of justice require that this Order be granted without prior notice to Defendants, and accordingly Plaintiff is relieved of the duty to provide Defendants with prior notice of Plaintiff's TRO Motion.

6. There is good cause to believe that Defendants have specifically directed their products and services to cybercriminals located in the Southern District of New York. There is also good cause to believe that, in carrying out their Fraudulent Enterprise, Defendants utilize an Internet Service Provider ("ISP") data center located in the Southern District of New York, as well as services provided by third parties located in the Southern District of New York, including payment processors and ISPs.

7. There is good cause to believe that Defendants have engaged in illegal activity using the data centers and/or Internet hosting providers identified in **Appendix A** to host the Hotmailbox and 1stCAPTCHA Websites, which Defendants use to operate and maintain their Fraudulent Enterprise.

8. There is good cause to believe that to immediately halt the injury caused by Defendants, data and evidence at Defendants' IP Addresses must be preserved and held in escrow pending further order of the court, Defendants' computing resources related to such IP addresses must then be disconnected from Defendants' infrastructure, Defendants must be prohibited from accessing Defendants' computer resources related to such IP addresses, and the data and evidence located on those computer resources must be secured and preserved.

9. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in **Appendix A** to this order to host the Hotmailbox and

1stCAPTCHA Websites, which are used to maintain and operate the Defendants' Fraudulent Enterprise. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in **Appendix A** must be immediately transferred to the control of Microsoft where they can be secured and thus made inaccessible to Defendants.

10. There is good cause to direct third-party Internet registries, registrars, data centers, and hosting providers with a presence in the United States to reasonably assist in the implementation of this Order and refrain from frustrating the implementation and purposes of this Order, pursuant to 28 U.S.C. § 1651(a) (the All Writs Act).

11. There is good cause to believe that if Defendants are provided advance notice of Plaintiff's TRO Motion or this Order, they would move the technological infrastructure supporting their Fraudulent Enterprise, permitting them to continue their misconduct, and would destroy, move, hide, conceal, or otherwise make inaccessible to the Court evidence of their misconduct, the Defendants' infrastructure's activity, the infringing materials, the instrumentalities used to make the infringing materials, and the records evidencing the manufacture and distributing of the infringing materials.

12. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing, and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, satisfy Fed. R. Civ. P. 4(f)(3), and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing, and of this action: (1) personal delivery upon Defendants at any physical addresses in the United States provided to the data centers and Internet hosting providers; (2) personal delivery through the

Hague Convention on Service Abroad or other treaties upon Defendants who provided contact information outside the United States; (3) transmission by e-mail, electronic messaging addresses, facsimile, and mail to the known email and messaging addresses of Defendants and to their contact information provided by Defendants to the domain registrars, registries, data centers, Internet hosting providers, and website providers who host the software code associated with Defendants' IP Addresses or the domains identified in **Appendix A**; and (4) publishing notice to the Defendants on a publicly available Internet website.

13. There is good cause to believe that the harm to Plaintiff of denying the relief requested in their TRO Motion outweighs any harm to any legitimate interests of Defendants and that there is no undue burden to any third party.

II. TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED as follows:

14. Defendants, their representatives, and persons who are in active concert or participation with them are temporarily restrained and enjoined from: making or causing others to make false or misleading representations or omissions to obtain any access to any Microsoft accounts or services; using Internet "bots" to hack into Microsoft's security systems; using Internet "bots" to deceive Microsoft's security systems into believing that they are legitimate human consumers of Microsoft services; creating Microsoft Outlook email accounts in names of fictitious users or otherwise in violation of Microsoft's Services Agreement; selling those fraudulently-procured accounts to cybercriminals for use as tools in perpetrating a wide variety of online crimes;

and otherwise configuring, deploying, operating, or maintaining the Hotmailbox and 1stCAPTCHA Websites.

15. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from infringing or otherwise misappropriating Plaintiff's registered trademarks, as set forth in **Appendix B**.

16. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from using in connection with Defendants' activities any false or deceptive designation, advertisement, representation or description of Defendants' or of their representatives' activities, whether by symbols, words, designs or statements, which would damage or injure Plaintiff or give Defendants an unfair competitive advantage or result in deception of consumers.

IT IS FURTHER ORDERED, pursuant to the All Writs Act:

17. VeriSign, Inc., the manager and operator of the .com registry, shall change the registrar of record for 1stcaptcha.com, anycaptcha.com, and nonecaptcha.com in the .com registry to Plaintiff's registrar of choice, MarkMonitor, Inc., and that MarkMonitor, Inc., shall change the registrant of those domains to Plaintiff;

18. Identity Digital, (formerly Afilias Inc.), the manager and operator of the .me registry, shall change the registrar of record for hotmailbox.me in the .me registry to Plaintiff's registrar of choice, MarkMonitor, Inc., and that MarkMonitor, Inc., shall change the registrant of those domains to Plaintiff;

19. Cloudflare, Inc. and Cloud South, the service providers of 1stcaptcha.com, anycaptcha.com, nonecaptcha.com, and hotmailbox.me, shall (1) preserve the computers, servers, electronic data storage devices, software, data, or media assigned to or otherwise associated with

Defendants' IP Addresses and the domains listed in **Appendix A**; (2) preserve all evidence of any kind related to the content, data, software or accounts associated with such IP addresses, domains, and such computer hardware; (3) completely disable the computers, servers, electronic data storage devices, software, data, or media assigned to or otherwise associated with Defendants' use of Defendants' IP Addresses and the domains listed in **Appendix A** and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives, and all other persons, except as otherwise ordered herein; (4) completely, and until further order of this Court, suspend all services to Defendants or Defendants' representatives or resellers associated with Defendants' IP Addresses and the domains listed in **Appendix A**; and (5) isolate and disable any content and software associated with the Defendants hosted at Defendants' IP Addresses in a manner that does not impact any content or software not associated with Defendants' IP Addresses. In determining the method and mechanism to disable content and software associated with the Defendants, the relevant data centers and/or hosting providers shall reasonably confer with Plaintiff's counsel, Brian T. Markley, Cahill Gordon & Reindel LLP, 32 Old Slip, 19th Floor, New York, NY 10005, bmarkley@cahill.com, (Tel: 212.701.3230) and Samson A. Enzer, Cahill Gordon & Reindel LLP, 32 Old Slip, 19th Floor, New York, NY 10005, senzer@cahill.com, (Tel: 212.701.3125), to facilitate any follow-on action;

20. VeriSign, Inc., Identity Digital, Cloudflare, Inc., and Cloud South shall (1) refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives, and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with hosting companies, data centers, the Plaintiff, or other ISPs to execute this order; (2) not enable, and shall take all reasonable steps to prevent, any circumvention of this order by Defendants or Defendants' representatives associated with

Defendants' IP Addresses or the domains listed in **Appendix A**, including but not limited to enabling, facilitating, and/or allowing Defendants or Defendants' representatives or resellers to rent, lease, purchase, or otherwise obtain another IP Address associated with your services; (3) preserve, retain, and produce to Plaintiff all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling Defendants' IP Addresses, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers, and telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage, access and contact records and all records, documents and logs associated with Defendants' or Defendants' Representatives' use of or access to Defendants' IP Addresses or the domains listed in **Appendix A**; and (4) provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order.

IT IS FURTHER ORDERED that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including any one or combination of (1) personal delivery upon Defendants who provided to the data centers and Internet hosting providers contact information in the United States; (2) personal delivery through the Hague Convention on Service Abroad or other treaties upon Defendants who provided contact information outside the United States; (3) transmission by e-mail, electronic messaging addresses, facsimile, and mail to the known email and messaging addresses of Defendants and to their contact information provided by Defendants to the domain registrars, registries, data centers, Internet hosting providers, and website providers who host the software code associated with

Handwritten: Plaintiff's counsel
via

Defendants' IP Addresses or the domains identified in **Appendix A**; and (4) publishing notice to the Defendants on a publicly available Internet website.

Handwritten: Plaintiffs are directed to ~~attempt~~ attempt service by all available such means, and to effect service by December 13, 2023.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before the Hon. Paul A. Engelmayer on December 20, 2023, at 9 a.m. to show cause, if there is any, why the Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this Order.

Handwritten: in courtroom 1305 of the Thurgood Marshall United States Courthouse, 40 Centre St., NYC, NY 10007.

IT IS FURTHER ORDERED that Microsoft, on behalf of Plaintiff, shall post bond in the amount of \$15,000 as cash to be paid into the Court registry.

IT IS FURTHER ORDERED that the Defendants shall file with the Court and serve on Plaintiff's counsel any answering affidavits, pleadings, motions, expert reports or declarations, and/or legal memoranda no later than two (2) ~~five (5)~~ days prior to the hearing on Plaintiff's request for a preliminary injunction, i.e., by Monday, December 18, 2023, at 9 a.m. Plaintiff may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Eastern Standard Time) on the appropriate dates listed in this paragraph.

IT IS SO ORDERED

Entered this 7th day of December, 2023.

Paul A. Engelmayer
Hon. Paul A. Engelmayer

Exhibit 2

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

MICROSOFT CORPORATION, a Washington Corporation, FORTRA, LLC, a Minnesota Corporation, and HEALTH-ISAC, INC., a Florida Corporation,

Plaintiff,

v.

JOHN DOES 1-2, JOHN DOES 3-4 (AKA CONTI RANSOMWARE GROUP), JOHN DOES 5-6 (AKA LOCKBIT RANSOMWARE GROUP), JOHN DOES 7-8 (AKA DEV-0193), JOHN DOES 9-10 (AKA DEV-0206), JOHN DOES 11-12 (AKA DEV-0237), JOHN DOES 13-14 (AKA DEV-0243), JOHN DOES 15-16 (AKA DEV-0504), Controlling Computer Networks and Thereby Injuring Plaintiffs and Their Customers,

Defendants.

Case No. 23-cv-2447-LDH-JRC

FILED UNDER SEAL

ORDER GRANTING PLAINTIFFS' *EX PARTE* MOTION TO SUPPLEMENT THE PRELIMINARY INJUNCTION

The Court, having considered the pleadings and declaration in support of Plaintiffs Microsoft Corp. (“Microsoft”), Fortra LLC (“Fortra”), and Health-ISAC, Inc. (“Health-ISAC”) (collectively, “Plaintiffs”) Motion to Supplement the Preliminary Injunction Order, hereby orders that the terms of the Preliminary Injunction Order (“Preliminary Injunction Order”), Dkt. No. 20, shall apply to the additional domains set forth in Appendix A to this order. As set forth below, Defendants have violated the Preliminary Injunction.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiffs’ Motion to Supplement the Preliminary Injunction Order, the Court hereby makes the following findings of fact and conclusions of law:

1. The Defendants were served with notice of the TRO and Preliminary Injunction via the alternative service methods previously authorized by this Court.
2. After receiving notice of the TRO and Preliminary Injunction, the Defendants have continued to engage in the conduct enjoined by the Preliminary Injunction Order, and therefore continue to violate the Preliminary Injunction Order. In particular, using new domains, Defendants have intentionally and without authorization, continued and attempted to access and send malicious software, code, and instructions to protected computers, operating systems, and networks of Plaintiffs and their customers, attacking such computers, systems and networks, and exfiltrating information from those computers, systems and networks..
3. There is good cause to believe that Defendants are likely to continue the foregoing conduct and to engage in the illegal conduct and purposes enjoined by the Preliminary Injunction Order, unless further relief is ordered to expeditiously prevent Defendants from maintaining the domains for such prohibited and unlawful purposes.
4. There is good cause to believe that, unless further relief is ordered to expeditiously prevent Defendants from maintaining the domains for purposes enjoined by the Preliminary Injunction Order, immediate and irreparable harm will result to Plaintiffs, their customers, and to the public, from the Defendants’ ongoing violations.

5. Therefore, in accordance with Fed. R. Civ. P. 65(a), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a) and the Court's inherent equitable authority, good cause and the interests of justice require that this Order be Granted.

SUPPLEMENTAL PRELIMINARY INJUNCTION

IT IS THEREFORE ORDERED that, the terms of the Preliminary Injunction Order shall be supplemented and shall be enforced against Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants and pursuant to the All Writs Act, with respect to any currently registered Internet domain set forth in **Appendix A**, the domain registries shall take the following actions:

A. Within three (3) business days of receipt of this Order, shall unlock and change the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. To the extent the registrar of record does not assist in changing the registrar of record for the domain under its control, the domain registry for the domain, or its administrators, including backend registry operators or administrators, within five (5) business days of receipt of this Order, shall change, or assist in changing, the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. The purpose of this paragraph is to ensure that Microsoft has control over the hosting and administration of the domain in its registrar account at MarkMonitor or such other registrar specified by Microsoft. Microsoft shall provide to the domain registry or registrar of record any requested registrar information or account details necessary to effectuate the foregoing.

B. The domain shall be made active and shall resolve in the manner set forth in this order, or as otherwise specified by Microsoft, upon taking control of the domain;

C. The domain registries shall take reasonable steps to work with Microsoft to ensure the transfer of the domain and to ensure that Defendants cannot use it to make unauthorized access to computers, infect computers, compromise computers and computer networks, monitor the owners and users of computers and computer networks, steal information from them or engage in any other activities prohibited by this Order;

D. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following, or other information as may be specified by Microsoft:

Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
United States
Phone: +1.4258828080
Facsimile: +1.4259367329
domains@microsoft.com

E. Prevent transfer, modification or deletion of the domain by Defendants and prevent transfer or control of the domain to the account of any party other than Microsoft;

F. Take all steps required to propagate to the foregoing changes through the Domain Name System (“DNS”), including domain registrars.

IT IS FURTHER ORDERED that copies of this Order may be served by any means authorized by law, including any one or combination of (1) personal delivery upon Defendants who provided accurate contact information in the U.S., if any; (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their hosting companies and as agreed to by Defendants in their hosting agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

IT IS SO ORDERED

Entered this 16 day of June 2023.

s/ LDH

HON. LASHANN DEARCY HALL
UNITED STATES DISTRICT COURT JUDGE

Exhibit 3

continued to engage in the conduct enjoined by the Preliminary Injunction, and therefore continue to violate the Preliminary Injunction. In particular, the Defendants have intentionally and without authorization, continued and attempted to access and send malicious software, code, and instructions to protected computers, operating systems, and networks of Microsoft and its customers, attacking such computers, systems and networks, and exfiltrating information from those computers, systems and networks, using new domains which include Microsoft's trademarks.

3. There is good cause to believe that Defendants are likely to continue the foregoing conduct and to engage in the illegal conduct and purposes enjoined by the Preliminary Injunction, unless further relief is ordered to expeditiously prevent Defendants from maintaining the registration of domains for such prohibited and unlawful purposes, on an ongoing basis.

4. There is good cause to believe that, unless further relief is ordered to expeditiously prevent Defendants from maintaining the registration of domains for purposes enjoined by the Preliminary Injunction, on an ongoing basis, immediate and irreparable harm will result to Microsoft, Microsoft's customers and to the public, from the Defendants' ongoing violations.

5. Therefore, in accordance with Fed. R. Civ. P. 65(b) and 53(a)(1)(C), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a) and the court's inherent equitable authority, good cause and the interests of justice require that this Order be Granted.

SUPPLEMENTAL PRELIMINARY INJUNCTION

IT IS THEREFORE ORDERED that, the terms of the Preliminary Injunction shall be supplemented and shall be enforced against the Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants, as follows:

1. With respect to any registered Internet domains that are determined to be "Strontium Domains," through the process set forth in this Order, and where the relevant domain registry is located in the United States, the domain registry shall take the following actions:

A. Maintain unchanged the WHOIS or similar contact and identifying

information as of the time of receipt of the order determining the domains to be Strontium Domains, and maintain the domains with the current registrar;

B. The domains shall remain active and continue to resolve in the manner set forth in this Order;

C. Prevent transfer, modification or deletion of the domains by Defendants or third parties at the registrar or otherwise;

D. The domains shall be redirected to secure servers by changing the authoritative name servers to NS149.microsoftinternetsafety.net and NS150.microsoftinternetsafety.net and, as may be necessary, the IP addresses associated with name servers or taking other reasonable steps to work with Microsoft to ensure the redirection of the domains and to ensure that Defendants cannot use them to make unauthorized access to computers, infect computers, compromise computers and computer networks, monitor the owners and users of computers and computer networks, steal information from them or engage in any other activities prohibited by the Preliminary Injunction;

E. Take all steps required to propagate to the foregoing changes through the Domain Name System (“DNS”), including domain registrars; and

F. Preserve all evidence that may be used to identify the Defendants using the domains.

2. With respect to any registered Internet domains that are determined to be “Strontium Domains,” through the process set forth in this Order, and where the relevant domain registry is located outside of the United States, any such non-U.S. domain registry is respectfully requested, but is not ordered, to provide assistance to Microsoft to prevent the Defendants’ use of the domains to make unauthorized access to computers, infect computers, compromise computers and computer networks, monitor the owners and users of computers and computer networks, steal information from them or engage in any other activities prohibited by the Preliminary Injunction.

IT IS FURTHER ORDERED that “Strontium Domains” are domains which are

determined to meet the following two criteria:

Criteria 1: The domains are used by the Defendants to break into computers and networks of the organizations that Strontium targets, or control the reconnaissance of those networks, or, ultimately, exfiltrate sensitive information from them, or are otherwise used by the Defendants to carry out the activities and purposes prohibited by the Preliminary Injunction. A domain is determined to be a Strontium Domain by comparing the activities and patterns associated with that domain with known confirmed Strontium Domains. The following factors concerning the domain will be used in this analysis:

Delivers malicious software, code, commands, exploits and/or “backdoor” functionality previously associated with Strontium, including but not limited to: Win32/Foosace, Coreshell, xtunnel, Backdoor.Win32/XAgentRat.A!dha, Gamefish, SPLM, Xagent, Chopstick, Oldbait, Eviltoss, Jhuhugit, Advstoshell, Netui, Sourface, or similar code or functionality deployed in a manner previously associated with Strontium.	Associated with remote code execution through browser drive-by or malicious attachment, privilege escalation or sandbox escape, security feature bypass, social engineering based attack and/or bootstrapped add-on, escalation of privileges, DLL file backdoor, credential stealing functionality, SSL tunnel, and/or functionality to deliver code or functions to “air gapped” USB devices, deployed in a manner previously associated with Strontium or similar code or functionality.
Domain registration information	Use of Bitcoin DNS providers
Name servers	Start of Authority (SOA) records
Resolves to IP of past Strontium domain, command and control server or similar infrastructure	Resolves to IP used in past Strontium malware
Used to deceive, target, obtain information from, and/or communicate commands or code to recipients, persons, institutions or networks previously targeted by Strontium.	Used to deceive, target, obtain information from, and/or communicate commands or code to recipients that may possess or be able to provide sensitive information or trade secrets of persons, entities or networks related to the defense, critical infrastructure or high technology sectors, journalists, political advisors or organizations, government bodies, diplomatic institutions, and/or military forces and installations.
SSL Cert Issuer_DN	SSL Cert Subject_DN
Host	Registrar

Criteria 2: The domains (a) use and infringe Microsoft’s trademarks, trade names or service marks or confusingly similar variants, or (b) use any false or deceptive designation, representation or description, which would damage or injure Microsoft or give Defendants an

unfair competitive advantage or result in deception of consumers, or (c) suggest in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or pass off Defendants' activities, products or services as Microsoft's. Such trademarks and brands shall include, but are not limited to the following trademarks, brands and/or confusingly similar variants: "365," "Azure," "Bing," "Excel," "Exchange," "Healthvault," "Hotmail," "Live," "Microsoft," "Minecraft," "MSDN," "MSFT," "MS," "MSN," "O365," "Office," "OneDrive," "Outlook," "OWA," "Passport," "PowerPoint," "SharePoint," "Skype," "Surface," "Visio," "Win," "Windows," and "Xbox."

IT IS FURTHER ORDERED that the following processes shall be used to determine whether a domain is a Strontium Domain and to determine the disposition of such domains:

1. **Domains Listed At Appendix B:** With respect to the specific domains listed in Appendix B, which substantially meet the requirements to constitute Strontium Domains, based on Defendants' prior pattern of activities, Microsoft shall determine whether Defendants have registered such domains, through consideration of the factors in Criteria 1, set forth above. Upon Microsoft's determination that domains in Appendix B meet the criteria to constitute a Strontium Domain, Microsoft shall serve written notice of such determination on the relevant domain registries. The domain registries shall retain the right to dispute Microsoft's authority to enforce this order as to them or to dispute Microsoft's determination. Upon receipt of such written notice, the domain registries shall promptly take the action ordered herein with respect to such Strontium Domains. If the domain registries dispute Microsoft's authority or its determinations, or if Defendants or any third party dispute action taken by domain registries or Microsoft's determinations pursuant to this Order, the domain registries, Defendants or any third parties may submit written objections to the Court Monitor for resolution by the Court Monitor, as set forth below, and subject to the right to judicial review. Any such objections by domain registries shall be submitted to the Court Monitor within two business days of receipt of written notice from Microsoft. In the course of deciding any objections submitted by registries, Defendants or third parties, the Court Monitor shall take and hear evidence and shall make determinations and issue

orders whether domains are Strontium Domains, as set forth further below.

2. Domains Not Listed At Appendix B And Criteria Outside Of This Order:

With respect to (a) domains not listed in Appendix B, but which are otherwise alleged to meet the criteria to constitute Strontium Domains, and (b) domains that are alleged to be Strontium Domains based on new criteria not listed in this Order, Microsoft shall submit a written motion to the Court Monitor seeking a declaration that such domains are Strontium Domains. The Court Monitor shall take and hear evidence and shall make determinations and issue orders whether domains are Strontium Domains, as set forth further below.

IT IS FURTHER ORDERED that, pursuant to Federal Rule of Civil Procedure 53(a)(1)(C) and the court's inherent equitable powers, **Hon. Faith Hochberg (Ret.)** is appointed to serve as Court Monitor in order to make determinations on disputes regarding whether particular domains are Strontium Domains, to make determinations and orders regarding whether particular domains are Strontium Domains, and to monitor Defendants' compliance with the Preliminary Injunction. Prior to being appointed, the Court Monitor must file an affidavit "disclosing whether there is any ground for disqualification under 28 U.S.C. § 455." Fed. R. Civ. P. 53(b)(3); *see also* Fed. R. Civ. P. 53(a)(2) (discussing grounds for disqualification). Filed concurrently with this Order is the affidavit submitted to the court by the Court Monitor. The following sets forth the terms of the appointment of the Court Monitor:

1. Duties: The duties of the Court Monitor shall include the following:

A. Carrying out all responsibilities and tasks specifically assigned to the Court Monitor in this Order;

B. Resolving objections submitted by domain registries, Defendants or other third parties, to Microsoft's determinations that domains constitute Strontium Domains and, with respect to motions submitted by Microsoft that particular domains constitute Strontium Domains, making determinations whether such domains are or are not Strontium Domains;

C. Otherwise facilitating the Parties' or third parties' resolution of disputes concerning compliance with obligations under this Order or any orders issued by the Court

Monitor, and recommending appropriate action by the court in the event an issue cannot be resolved by the Parties or third parties with the Court Monitor's assistance;

D. Investigating matters related to the Court Monitor's duties, and enforcing orders related to the matters set forth in this Order.

E. Monitoring and reporting on Defendants' compliance with their obligations under the Preliminary Injunction and this Order;

F. The Court Monitor shall have all authority provided under Federal Rule of Civil Procedure 53(c).

2. Orders Regarding Strontium Domains: The Court Monitor shall resolve objections and shall make determinations and issue orders whether domains are Strontium Domains, pursuant to the terms set forth in the Preliminary Injunction, this Order and pursuant to the following process:

A. Upon receipt of a written objection from any domain registries, Defendants or any other third parties contesting any determinations by Microsoft that particular domains constitute Strontium Domains, or upon receipt of a written motion from Microsoft for a finding that particular domains constitute Strontium Domains, the Court Monitor shall take and hear evidence whether a domain is a Strontium Domain, pursuant to the standards set forth in Rule 65 of the Federal Rules of Civil Procedure. Any party opposing such objection or motion shall submit to the Court Monitor and serve on all parties an opposition or other response within twenty four (24) hours of receipt of service of the objection or motion. The Court Monitor shall issue a written ruling on the objection or motion no later than two (2) days after receipt of the opposition or other response. Any party may seek and the Court Monitor may order provisional relief, including redirection of domains or other temporary disposition of domains, while any objection or motion is pending. A form of order which may be used by the Special Master is attached as Appendix C.

B. It is the express purpose of this order to afford prompt and efficient relief and disposition of Strontium Domains. Accordingly, in furtherance of this purpose, all

objections, motions and responses shall be embodied and communicated between the Court Monitor, parties and third parties in electronic form, by electronic mail or such other means as may be reasonably specified by the Court Monitor. Also in furtherance of this purpose, hearings shall be telephonic or in another expedited form as may be reasonably specified by the Court Monitor.

C. The Court Monitor's determinations regarding any objection or any motion shall be embodied in a written order, which shall be served on all Parties and relevant third parties (including domain registries and/or registrars).

D. The Court Monitor is authorized to order the Parties and third parties to comply with such orders (pursuant to 28 U.S.C. § 1651(a)), subject to the Parties' and third parties' right to judicial review, as set forth herein.

E. If no Party or third party objects to the Court Monitor's orders and determinations pursuant to the judicial review provisions herein, then the Court Monitor's orders and determinations need not be filed on the docket. However, at the time the Court Monitor submits his or her periodic reports to the court, as set forth below, the Monitor shall separately list in summary form his or her uncontested orders and determinations.

3. **Judicial Review:** Judicial review of the Court Monitor's orders, reports or recommendations, shall be carried out as follows:

A. If any Party or third party desires to object to any order or decision made by the Court Monitor, the Party shall notify the Court Monitor within one business day of receipt of service of the order or decision, and thereupon the Court Monitor shall promptly file on the court's docket the written order setting forth the Monitor's decision or conditions pursuant to Federal Rule of Civil Procedure 53(d). The Party or third party shall then object to the Court Monitor's order in the manner prescribed in this Order.

B. The Parties and third parties may file objections to, or a motion to adopt or modify, the Court Monitor's order, report, or recommendations no later than 10 calendar days after the order is filed on the docket. The court will review these objections under the standards

set forth in Federal Rule of Civil Procedure 53(f).

C. Any party may seek and the Court may order provisional relief, including redirection of domains or other temporary disposition of domains, while any objection or motion is pending.

D. The orders, reports and recommendations of the Court Monitor may be introduced as evidence in accordance with the Federal Rules of Evidence.

E. Before a Party or third party seeks relief from the court for alleged noncompliance with any court order that is based upon the Court Monitor's report or recommendations, the Party or third party shall: (i) promptly notify the other Parties or third party and the Court Monitor in writing; (ii) permit the Party or third party who is alleged to be in noncompliance five business days to provide the Court Monitor and the other parties with a written response to the notice, which either shows that the party is in compliance, or proposes a plan to cure the noncompliance; and (iii) provide the Court Monitor and parties an opportunity to resolve the issue through discussion. The Court Monitor shall attempt to resolve any such issue of noncompliance as expeditiously as possible.

4. **Recordkeeping:** The Court Monitor shall maintain records of, but need not file those orders, reports and recommendations which are uncontested by the Parties or third parties and for which judicial review is not sought. The Court Monitor shall file on the court's docket all written orders, reports and recommendations for which judicial review is sought, along with any evidence that the Court Monitor believes will assist the court in reviewing the order, report, or recommendation. The Court Monitor shall preserve any documents the Monitor receives from the Parties.

5. **Periodic Reporting:** The Court Monitor shall provide periodic reports to the court and to the Parties concerning the status of Defendants' compliance with this Order and other orders of the court or the Court Monitor, including progress, any barriers to compliance, and potential areas of noncompliance. The periodic reports shall also include a summary of all uncontested orders and determinations and a listing of *ex parte* communications. The Court

Monitor shall file a report with the court under this provision at least once every 120 days.

6. **Access to Information:** The Court Monitor shall have access to individuals and non-privileged information, documents and materials under the control of the Parties or third parties that the Monitor requires to perform his or her duties under this Order, subject to the terms of judicial review set forth herein. The Court Monitor may communicate with a Party's or a third party's counsel or staff on an *ex parte* basis if reasonably necessary to carry out the Court Monitor's duties under this Order. The Court Monitor may communicate with the court on an *ex parte* basis concerning non-substantive matters such as scheduling or the status of the Court Monitor's work. The Court Monitor may communicate with the court on an *ex parte* basis concerning substantive matters with 24 hours written notice to the Parties and any relevant third party. The Court Monitor shall document all *ex parte* oral communications with a Party's or third party's counsel or staff in a written memorandum to file summarizing the substance of the communications, the participants to the communication, the date and time of the communication and the purpose of the *ex parte* communication. At the time the Court Monitor submits his or her periodic reports to the court, the Monitor shall separately list his or her *ex parte* communications with the Parties.

7. **Engagement of Staff and Consultants:** The Court Monitor may, consistent with a budget to be approved by the court, hire staff or expert consultants to assist the Court Monitor in performing his or her duties. The Court Monitor will provide the Parties advance written notice of his or her intention to hire a particular consultant, and such notice will include a resume and a description of duties of the consultant.

8. **Budget, Compensation, and Expenses:** Microsoft shall fund the Court Monitor's work pursuant to a budget proposed by the Court Monitor and approved by the Court. The Court Monitor shall incur only such fees and expenses as may be reasonably necessary to fulfill the Court Monitor's duties under this Order, or such other orders as the court may issue. Every 60 days the Court Monitor shall submit to the court an itemized statement of fees and expenses, which the court will inspect for regularity and reasonableness. If the court determines

the itemized statement is regular and reasonable, the court will sign it and transmit it to Microsoft. Microsoft shall then remit to the Court Monitor any court-approved amount, within 30 calendar days of court approval.

9. **Other Provisions:** As an agent and officer of the court, the Court Monitor and those working at his or her direction shall enjoy the same protections from being compelled to give testimony and from liability for damages as those enjoyed by other federal judicial adjuncts performing similar functions. Nevertheless, any Party or non-party may request that the court direct the Court Monitor to disclose documents or other information reasonably necessary to an investigation or the litigation of legal claims in another judicial forum that are reasonably related to the Court Monitor's work under this Order. The Court shall not order the Court Monitor to disclose any information without providing the Parties notice and an opportunity to be heard. As required by Rule 53(b)(2) of the Federal Rules of Civil Procedure, the court directs the Court Monitor to proceed with all reasonable diligence. The Court Monitor shall be discharged or replaced only upon an order of the Court. The parties, their successors in office, agents, and employees will observe faithfully the requirements of this Order and cooperate fully with the Court Monitor, and any staff or expert consultant employed by the Court Monitor, in the performance of their duties.

10. **Retention of Jurisdiction:** The Court will retain jurisdiction to enforce and modify this Order until such time as the Court finds that Microsoft does not seek further determinations regarding any additional Strontium Domains or that Defendants establish, by a preponderance of the evidence, that there is no risk of continued use of Strontium Domains in violation of the Preliminary Injunction. Under no circumstances will the court's jurisdiction to modify or enforce this Order lapse before January 1, 2026.

IT IS FURTHER ORDERED that copies of this Order and all other pleadings and documents in this action, including orders, determinations, reports and recommendations of the Court Monitor, may be served by any means authorized by law, including (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by

Defendants to Defendants' domain registrars and/or hosting companies and as agreed to by Defendants in the domain registration or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatory to such treaties.

IT IS SO ORDERED.

Entered this 6th day of December, 2016.

Alexandria, Virginia
12/6 / 16

/s/
Gerald Bruce Lee
United States District Judge

Exhibit 4

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING A
COMPUTER NETWORK AND THEREBY
INJURING PLAINTIFF AND ITS
CUSTOMERS,

Defendants.

Civil Action No: 1:19-cv-00716-ABJ

FILED UNDER SEAL

FILED

MAY 22 2019

Clerk, U.S. District & Bankruptcy
Courts for the District of Columbia

SUPPLEMENTAL INJUNCTION ORDER

The Court, having considered the pleadings and declaration in support of Microsoft Corporation’s (“Microsoft”) Motion to Supplement Preliminary Injunction Order, hereby orders that the terms of the Preliminary Injunction Order (“Preliminary Injunction Order”), Dkt. 18, shall apply to the additional domains set forth in the **Appendix A** to this order. As set forth below, Defendants have violated the Preliminary Injunction.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, memorandum, and all other pleadings and papers relevant to Microsoft’s Motion to Supplement the Preliminary Injunction and Microsoft’s original motion for Temporary Restraining Order and Preliminary Injunction, the Court hereby makes the following findings of fact and conclusions of law:

- I. The Defendants were served with notice of the Preliminary Injunction.
- II. After receiving notice of the Preliminary Injunction, the Defendants have continued to engage in the conduct enjoined by the Preliminary Injunction Order, and therefore

continue to violate the Preliminary Injunction Order. In particular, Defendants have intentionally and without authorization, continued and attempted to access and send malicious software, code, and instructions to protected computers, operating systems, and networks of Microsoft and its customers, attacking such computers, systems and networks, and exfiltrating information from those computers, systems and networks, using new domains.

III. There is good cause to believe that Defendants are likely to continue the foregoing conduct and to engage in the illegal conduct and purposes enjoined by the Preliminary Injunction Order, unless further relief is ordered to expeditiously prevent Defendants from maintaining the registration of domains for such prohibited and unlawful purposes.

IV. There is good cause to believe that, unless further relief is ordered to expeditiously prevent Defendants from maintaining the registration of domains for purposes enjoined by the Preliminary Injunction Order, immediate and irreparable harm will result to Microsoft, Microsoft's customers and to the public, from the Defendants' ongoing violations.

V. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a) and the Court's inherent equitable authority, good cause and the interests of justice require that this Order be Granted.

SUPPLEMENTAL PRELIMINARY INJUNCTION

IT IS THEREFORE ORDERED that, the terms of the Preliminary Injunction Order shall be supplemented and shall be enforced against Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants, as follows:

1. With respect to any currently registered Internet domains set forth in **Appendix A**, the domain registries shall take the following actions:

A. Within five (5) business days of receipt of this Order, shall unlock and

change the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. To the extent the registrar of record does not assist in changing the registrar of record for the domain under its control, the domain registry for the domain, or its administrators, including backend registry operators or administrators, within five (5) business days of receipt of this Order, shall change, or assist in changing, the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. The purpose of this paragraph is to ensure that Microsoft has control over the hosting and administration of the domain in its registrar account at MarkMonitor or such other registrar specified by Microsoft. Microsoft shall provide to the domain registry or registrar of record any requested registrar information or account details necessary to effectuate the foregoing.

B. The domain shall be made active and shall resolve in the manner set forth in this order, or as otherwise specified by Microsoft, upon taking control of the domain;

C. The domain shall be redirected to secure servers by changing the authoritative name servers to NS151.microsoftinternetsafety.net and NS152.microsoftinternetsafety.net and, as may be necessary, the IP addresses associated with name servers or taking other reasonable steps to work with Microsoft to ensure the redirection of the domain and to ensure that Defendants cannot use it to make unauthorized access to computers, infect computers, compromise computers and computer networks, monitor the owners and users of computers and computer networks, steal information from them or engage in any other activities prohibited by the Injunction;

D. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following, or other information as may be specified by Microsoft:

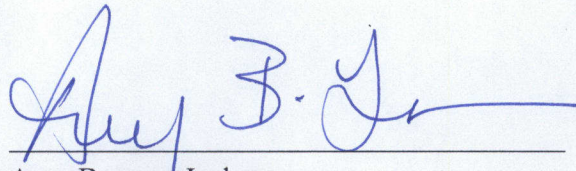
Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
United States
Phone: +1.4258828080
Facsimile: +1.4259367329
domains@microsoft.com

E. Prevent transfer, modification or deletion of the domain by Defendants and prevent transfer or control of the domain to the account of any party other than Microsoft;

F. Take all steps required to propagate to the foregoing changes through the Domain Name System ("DNS"), including domain registrars.

IT IS SO ORDERED

Entered this 22nd day of May, 2019



Amy Berman Jackson
United States District Judge

APPENDIX A

APPENDIX A

.COM, .NET DOMAINS

Registry

c/o

VeriSign, Inc.

VeriSign Information Services, Inc.

12061 Bluemont Way

Reston, Virginia 20190

United States

<p>scribdinc.com</p>	<p>Registrant Name: Whois Agent Registrant Organization: Domain Protection Services, Inc. Registrant Street: PO Box 1769 Registrant City: Denver Registrant State/Province: CO Registrant Postal Code: 80201 Registrant Country: US Registrant Phone: +1.7208009072 Registrant Fax: +1.7209758725 Registrant Email: https://www.name.com/contact-domain-whois/scribdinc.com abuse@name.com</p>
<p>telegram.net</p>	<p>Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Phone Ext: Registrant Fax: +852.30197491 Registrant Fax Ext: Registrant Email: whoisprivacy@domainidshield.com</p>

.INFO DOMAINSRegistry

Afilias, Inc.
 300 Welsh Road
 Building 3, Suite 105
 Horsham, PA 19044
 United States

bahaius.info	Registration Name: Domain ID Shield Service Registration Organization: Domain ID Shield Service CO., Limited Registration Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registration City: Hong Kong Registration State/Province: Hong Kong Registration Postal Code: 999077 Registration Country: HK Registration Phone: +852.21581835 Registration Phone Ext: Registration Fax: +852.30197491 Registration Fax Ext: Registration Email: whoisprivacy@domainidshield.com
customers-reminder.info	Registration Name: Domain ID Shield Service Registration Organization: Domain ID Shield Service CO., Limited Registration Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registration City: Hong Kong Registration State/Province: Hong Kong Registration Postal Code: 999077 Registration Country: HK Registration Phone: +852.21581835 Registration Phone Ext: Registration Fax: +852.30197491 Registration Fax Ext: Registration Email: whoisprivacy@domainidshield.com
identity-verification-service.info	Registration Name: Domain ID Shield Service Registration Organization: Domain ID Shield Service CO., Limited Registration Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD,

	<p>MONGKOK, KOWLOON, HONG KONG Registration City: Hong Kong Registration State/Province: Hong Kong Registration Postal Code: 999077 Registration Country: HK Registration Phone: +852.21581835 Registration Phone Ext: Registration Fax: +852.30197491 Registration Fax Ext: Registration Email: whoisprivacy@domainidshield.com</p>
inbox-drive.info	<p>Registration Name: Jennifer J. Bradley Registration Organization: roseron co Registration Street: 2811 Maple Avenue Registration City: Modesto Registration State/Province: CA Registration Postal Code: 95354 Registration Country: US Registration Phone: +1.251548796 Registration Phone Ext: Registration Fax: +1.251548796 Registration Fax Ext: Registration Email: amanda.cristiani15@gmail.com</p>
inbox-sharif.info	<p>Registration Name: Jennifer J. Bradley Registration Organization: roseron co Registration Street: 2811 Maple Avenue Registration City: Modesto Registration State/Province: CA Registration Postal Code: 95354 Registration Country: AF Registration Phone: +1.2564158796 Registration Phone Ext: Registration Fax: +1.2564158796 Registration Fax Ext: Registration Email: amanda.cristiani15@gmail.com</p>
magic-delivery.info	<p>Registration Name: William Brown Registration Organization: will co Registration Street: 410 Coulter Lane Registration City: Richmond Registration State/Province: VA Registration Postal Code: 23226 Registration Country: VA Registration Phone: +1.8042873632 Registration Phone Ext:</p>

	Registration Fax: +1.8042873632 Registration Fax Ext: Registration Email: williambrown.wl.br@gmail.com
recovery-services.info	Registration Name: Domain ID Shield Service Registration Organization: Domain ID Shield Service CO., Limited Registration Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registration City: Hong Kong Registration State/Province: Hong Kong Registration Postal Code: 999077 Registration Country: HK Registration Phone: +852.21581835 Registration Phone Ext: Registration Fax: +852.30197491 Registration Fax Ext: Registration Email: whoisprivacy@domainidshield.com
verification-services.info	Registration Name: Domain ID Shield Service Registration Organization: Domain ID Shield Service CO., Limited Registration Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registration City: Hong Kong Registration State/Province: Hong Kong Registration Postal Code: 999077 Registration Country: HK Registration Phone: +852.21581835 Registration Phone Ext: Registration Fax: +852.30197491 Registration Fax Ext: Registration Email: whoisprivacy@domainidshield.com

.WORLD DOMAINS

Registry

Binky Moon, LLC

Donuts Inc.

5808 Lake Washington Blvd. NE, Suite 300

Kirkland, WA 98033

United States

youridentityactivity.world	Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Domain Protection Services, Inc. Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: CO Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY abuse@name.com
----------------------------	---

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X		
MICROSOFT CORPORATION,	:	
	:	
Plaintiff,	:	Case No. 23 Civ. 10685 (PAE)
-against-	:	
	:	
DUONG DINH TU,	:	
LINH VAN NGUYEN, and	:	
TAI VAN NGUYEN,	:	<u>REQUEST TO FILE UNDER SEAL</u>
	:	
Defendants.	:	
-----X		

**MICROSOFT’S MEMORANDUM OF LAW IN SUPPORT OF ITS MOTION FOR AN
EX PARTE SUPPLEMENTAL PRELIMINARY INJUNCTION ORDER**

Plaintiff Microsoft Corporation (“Microsoft”) seeks an *Ex Parte* Supplemental Preliminary Injunction Order to address Defendants’ continuing efforts to sell tools and services for committing cybercrime (the “Fraudulent Enterprise”) from a new Internet domain (“rockcaptcha.com” or the “RockCAPTCHA Website”).

Plaintiff incorporates by reference herein the arguments and evidence set forth in its Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause (ECF No. 12) (“TRO Motion”). As set forth in Plaintiff’s TRO Motion, the Fraudulent Enterprise has used internet “bots” to defraud Microsoft’s security systems, allowing for the creation of hundreds of millions of free Microsoft email accounts in the names of fake people. Defendants then sell these fraudulent accounts in bulk in their own illicit online marketplace to other criminals, who use the accounts to spread computer viruses across the Internet, engage in phishing scams, and commit crippling cyberattacks, terrorizing Microsoft customers around the world. The Fraudulent Enterprise continues to cause substantial, irreparable harm to Microsoft and its customers.

Microsoft seeks injunctive relief to further disrupt the Defendants' criminal scheme, which has recently been reconstituted on a new website, and to ultimately recover damages, for Defendants' (1) violations of the Lanham Act (15 U.S.C. §§ 1114 *et seq.*, 1125(a), (c)), (2) violations of the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962) ("RICO"), (3) tortious interference with Microsoft's business relationships with its customers, (4) conversion of Microsoft's property, (5) trespass to Microsoft's chattels, and (6) unjust enrichment at Microsoft's expense.

I. BACKGROUND

On December 7, 2023, this Court granted an *Ex Parte* temporary restraining order ("TRO") tailored to halt the illegal activities of the Fraudulent Enterprise.¹ Working with the third parties whose infrastructure had been abused by the Defendants to perpetrate their fraudulent activity, Microsoft finished effectuating the TRO on December 12, 2023 (*see* ECF No. 5), and on December 13, 2023, served Defendants with the TRO and other case documents (*see* ECF No. 20 at 2–3 (detailing Microsoft's efforts to effectuate service on Defendants "by all available means")). On December 19, 2023, the Court converted the TRO into an Order for Preliminary Injunction (ECF No. 23), and Microsoft served Defendants with the Preliminary Injunction Order (*see* ECF No. 26). Since then, Microsoft has been conducting third-party discovery to support a default judgment in this proceeding (*see* ECF No. 32).

Microsoft has confirmed through its own investigation that Defendants, in blatant violation of the Court's Preliminary Injunction Order, have reconstituted the unlawful marketplace

¹ Microsoft respectfully notes that that apparently the TRO was never published on the case docket. For the Court's convenience, Microsoft attaches a true and correct copy of the TRO as Exhibit 1 to the Declaration of Jason Rozbruch in Support of Microsoft's Motion for an *Ex Parte* Supplemental Preliminary Injunction Order ("Rozbruch Decl.").

supporting their Fraudulent Enterprise under the RockCAPTCHA Website. *See* Declaration of Jason Lyons in Support of Microsoft’s Motion for an *Ex Parte* Supplemental Preliminary Injunction Order. (“Lyons Decl.”) ¶¶ 6–10. Plaintiff asks the Court for an order directing the RockCAPTCHA Website’s (1) registry operator to change the registrar of record for the domain to Plaintiff’s registrar of choice, which will then change the registrant of the domain to Plaintiff, and to take reasonable steps to work with Plaintiff to ensure the transfer of the domain; and (2) hosting service provider to disable all services provided thereto.

II. ARGUMENT

The supplemental relief Plaintiff seeks has been granted in similar prior cases when defendants began using new domains after the court granted preliminary relief. *See, e.g.*, Order Granting *Ex Parte* Motion to Supplement the Preliminary Injunction, *Microsoft Corp. v. John Does 1-2*, No. 1:23-cv-02447 (E.D.N.Y. June 16, 2023) (Hall, J.), ECF No. 24 (Rozbruch Decl. Ex. 2) (granting supplemental injunction to seize additional domains associated with defendants’ unlawful infrastructure); Supplemental Preliminary Injunction Order, *Microsoft Corp. v. John Does 1-2*, No. 1:16-cv-00993 (E.D. Va. Dec. 6, 2016) (Lee, J.), ECF No. 49 (Rozbruch Decl. Ex. 3) (same); Supplemental Injunction Order, *Microsoft Corp. v. John Does 1-2*, No. 1:19-cv-00716 (D.D.C. May 22, 2019) (Berman Jackson, J.), ECF No. 21 (Rozbruch Decl. Ex. 4) (same).

Here, absent the requested relief, Microsoft and its customers will continue to suffer irreparable harm, as detailed in Microsoft’s prior submissions. Microsoft is likely to succeed on the merits because the domain at issue in this motion is used for the same unlawful purposes and generally in the same unlawful manner as the domains that were the subject of Plaintiff’s TRO Motion. Lyons Decl. ¶¶ 6–11. Disabling the additional domain at issue is necessary to prevent irreparable harm to Plaintiff and its customers.

It is imperative that this supplemental relief be ordered and effectuated on an *ex parte* basis, shielded from anyone associated with the Fraudulent Enterprise until it is complete. Lyons Decl. ¶ 12. If Defendants are alerted to these efforts prior to completion, there is substantial risk they will relocate the infrastructure to an alternative domain or domains, thwarting this effort to further discourage and ultimately stop the Fraudulent Enterprise. *Id.* As discussed in Microsoft’s TRO Motion, *ex parte* relief is appropriate here because Microsoft has set forth facts showing immediate and irreparable injury and a sound basis for why notice should not be required. *See* ECF No. 13 (Memorandum of Law in Support of TRO Motion) at 49–51. In this case, Defendants have already demonstrated that they have the technical sophistication and ability to move their malicious infrastructure, and would likely immediately do so if given the opportunity before a Court order is issued. Lyons Decl. ¶¶ 12–13; *see also* Fed. R. Civ. P. 65(b)(1); *In re Vuitton et Fils S.A.*, 606 F.2d 1, 4–5 (2d Cir. 1979) (holding that notice prior to issuing temporary restraining order was not necessary where notice would “serve only to render fruitless further prosecution of the action”); *id.* at 2 (plaintiff’s “[prior] experience . . . taught it that once one member of this community of counterfeiters learned that he had been identified by [plaintiff] and was about to be enjoined from continuing his illegal enterprise, he would immediately transfer his inventory to another counterfeit seller, whose identity would be unknown to [plaintiff]”); *AT&T Broadband v. Tech Commc’ns, Inc.*, 381 F.3d 1309, 1319–20 (11th Cir. 2004) (affirming *ex parte* search and seizure order to seize contraband technical equipment, given evidence that, in the past, defendants and persons similarly situated had secreted evidence once notice was given); *Little Tor Auto Ctr. v. Exxon Co., USA*, 822 F. Supp. 141, 143 (S.D.N.Y. 1993) (*ex parte* temporary restraining order is appropriate where contraband “may be destroyed as soon as notice is given”). Although the Defendants have already demonstrated an ability to reconstitute their malicious infrastructure following Microsoft’s

disruption efforts, their new, reconstituted websites operate on a much lesser scale, with far fewer customers. Lyons Decl. ¶ 12. As demonstrated in the Lyons Declaration, additional unannounced disruptions of these illicit operations will further frustrate Defendants' efforts to maintain and add customers, weaken their credibility in the marketplace, and ultimately cause the Fraudulent Enterprise to fail. *Id.* Immediately upon execution of the requested Supplemental Preliminary Injunction Order and disabling of the RockCAPTCHA Website, Plaintiffs will provide appropriate notice to the Defendants, consistent with the email and publication alternative service methods already authorized by this Court. *See* ECF Nos. 20, 23, 26.

III. CONCLUSION

For the reasons set forth in this memorandum of law and the Lyons Declaration submitted herewith, and based on the evidence previously submitted by Microsoft in this proceeding, Microsoft respectfully requests that the court grant its Motion for an *Ex Parte* Supplemental Preliminary Injunction Order.

Dated: July 23, 2024
New York, New York

CAHILL GORDON & REINDEL LLP

By: 

Brian T. Markley
Samson A. Enzer
Jason Rozbruch
32 Old Slip
New York, New York 10005

MICROSOFT CORPORATION
Sean Farrell
One Microsoft Way
Redmond, Washington 98052

Counsel for Plaintiff Microsoft Corporation