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		

PLAINTIFF MICROSOFT'S MEMORANDUM OF LAW IN SUPPORT OF ITS MOTION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Orders

Statutes

Other Authorities

Plaintiff Microsoft Corporation ("Microsoft" or the "Company") seeks judicial relief to disrupt a criminal enterprise, run by the Defendants, that sells tools and services for committing cybercrime (the "Fraudulent Enterprise" or "Enterprise"). The Fraudulent Enterprise uses internet "bots" to defraud Microsoft's security systems, allowing for the creation 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 spray computer viruses across the Internet, engage in phishing scams, and commit crippling cyberattacks, terrorizing Microsoft customers around the world.

Defendants have also developed and unleashed bots to obtain so-called "CAPTCHA" tokens, which they sell to their customers for use in bypassing online puzzles commonly used by Microsoft and other technology companies to prove that an Internet user is a real person. These criminal services specifically target not only Microsoft, but other technology companies as well, including X (formerly Twitter) and Google. While the fraudulent email accounts and CAPTCHA tokens sold by Defendants are typically only valid for a short period of time before Microsoft identifies and invalidates them, Defendants acquire and sell the accounts and tokens so quickly, and in such volume, that they have still managed to collect millions of dollars in unlawful proceeds, while causing irreparable harm to Microsoft and its customers.

As explained below and in the accompanying declarations, this action is the culmination of an extensive investigation led by Microsoft's Digital Crimes Unit ("DCU"), with support from external counsel and experienced consultants, including former officials from the U.S. Department of Justice. The investigation included undercover test purchases of email accounts and CAPTCHA tokens from Defendants' own websites, as well as cryptocurrency payments to online accounts that Defendants control. The investigation identified clear evidence that the Defendants not only operate the online marketplaces where these illicit goods and services are sold, but that they personally wrote the code underlying those websites, and even created and uploaded to YouTube a "how-to" video, in which they boldly described their scheme in detail.

Microsoft brings this action to obtain injunctive relief to disrupt the Defendants' ongoing criminal scheme and to recover damages for their (1) violations of the Racketeer Influenced and Corrupt Organizations Act, (2) infringements of Microsoft's valuable trademarks and other violations of the Lanham Act, (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.

The relief sought includes judicial authorization to direct several providers of technological infrastructure used by the Fraudulent Enterprise to take specific actions to disrupt the scheme. *See* Microsoft's Proposed Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause ("Proposed Order"). It is imperative that these actions be closely coordinated, such that—for example—Internet protocol ("IP") addresses used by the Fraudulent Enterprise in various locations are turned off immediately, and simultaneously, upon receipt of this Court's orders. It is also critical that these actions be shielded from anyone associated with the Fraudulent Enterprise until the takedown of this infrastructure is complete. If Defendants are alerted to these efforts prior to their completion, there is substantial risk they will relocate the infrastructure to alternative domains, thwarting this effort to stop the Fraudulent Enterprise.

I. STATEMENT OF FACTS

A. Background

1. Microsoft's Market-Leading Services, Reputation, and Trademarks

Microsoft is one of the leading computer technology companies in the world, offering globally-recognized products, including its Windows operating system; the Microsoft 365 family of business productivity software, including its Word, Excel, and PowerPoint software applications; Outlook software for managing email communications, calendaring, and tasks; Teams for virtual collaboration; Skype for instant messaging software; and LinkedIn for professional networking.

Microsoft's customers include individuals, state and federal courts, law enforcement agencies, governments, hospitals, private businesses large and small, non-profit organizations, public-sector institutions, and others. The Company's products include widely-used email services, including via Outlook email accounts (with the domain "outlook.com") or Hotmail email accounts (with the domain "hotmail.com"). While Microsoft offers subscription-based Outlook and Hotmail email account services with premium benefits, it also offers free versions of both services to attract new users and form lasting customer relationships. *See* Declaration of Jason Lyons in Support of Plaintiff Microsoft's Motion for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause ("Lyons Decl.") ¶ 7.

In response to the increasing rate and pace of cybercrime threats in recent years, Microsoft has developed, and offered to the marketplace, comprehensive cybersecurity solutions powered in part by artificial intelligence. *See* Declaration of Shinesa Cambric in Support of Plaintiff Microsoft's Motion for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause ("Cambric Decl.") ¶¶ 7–18. Currently, more than one million customer organizations utilize these cybersecurity services to protect their digital estates. *See* Declaration of Jason Rozbruch in Support of Plaintiff Microsoft's Motion for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause ("Rozbruch Decl.") Ex. 14 (Microsoft Annual Report 2023) at 3. Due to the superior quality and effectiveness of Microsoft's products and services and its expenditure of significant resources to market them to customers, Microsoft has generated substantial goodwill while building brand names into strong and famous worldwide symbols that are well-recognized within the Company's channels of trade. *See* Cambric Decl. ¶¶ 5, 20.

Microsoft has registered trademarks representing the quality of its products and services and its brand, including—among others—Outlook® and Hotmail®. *See* Lyons Decl. ¶ 30. Copies of the trademark registrations for these trademarks are attached as Appendix B to the Complaint. *Id.*

2. <u>Microsoft's Efforts to Prevent Cybercrime</u>

The success of Microsoft's business depends on its ability to deliver services in a safe and secure fashion while generating and sustaining consumer trust and confidence in the integrity of the digital economy and Internet as a whole. *See* Cambric Decl. ¶ 7. Accordingly, the Company undertakes costly, time-consuming, and labor-intensive efforts to secure its ecosystem to help ensure that its customers enjoy a positive, worry-free experience when they use Microsoft's services. *Id.* Microsoft has spent tens of millions of dollars over the last few years alone employing top-flight technical, legal, and business experts to prevent, disrupt, and deter cybercrime. *Id.* ¶¶ 5, 7, 20; *see* Declaration of Patrice Boffa in Support of Plaintiff Microsoft's Motion for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause ("Boffa Decl.") ¶ 18.

First, to use Microsoft services, every customer must sign up for their own personal Microsoft account. Lyons Decl. ¶¶ 8, 12. In so doing, customers must agree to the terms of Microsoft's Services Agreement and that they will abide by a strict code of conduct, representing that they: (a) will not use any false, inaccurate, or misleading information when signing up for a Microsoft account; (b) will not transfer their Microsoft account credentials to anyone else; and (c) will not engage in any activity that is fraudulent, false, or misleading (such as by impersonating someone else, creating fraudulent accounts, or automating inauthentic activity). *Id.* ¶ 12.

Second, Microsoft employs security measures to verify that each user attempting to open a Microsoft account is a human being. Lyons Decl. ¶¶ 8, 20; Boffa Decl. ¶¶ 5–6; Cambric Decl. ¶ 10. For example, the Company contracts with a leading cybersecurity vendor, Arkose Labs, to employ a state-of-the-art CAPTCHA defense service, which serves as a gatekeeper, requiring every would-be user to represent that they are a human (not a bot), and to verify the accuracy of that representation by solving several puzzles—which, if answered correctly, provide a high level of confidence that the user is real. Cambric Decl. ¶ 10. After solving the CAPTCHA puzzle, the user must then provide identifying information, including their birthday and name, so that Microsoft has additional data on file to confirm the user's authenticity. *See* Declaration of Maurice Mason in Support of Plaintiff Microsoft's Motion for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause ("Mason Decl.") ¶ 10.

Third, Microsoft employs a variety of internal tools that leverage artificial intelligence and machine learning to prevent bots and other malicious actors from entering its systems. Cambric Decl. ¶ 11. The Company also employs engineers, data scientists, and other investigators to monitor its systems such as Outlook and Skype for signs of suspicious behavior (such as indications of bots opening fraudulent Microsoft accounts in bulk) and suspend Microsoft accounts that are believed with a high degree of certainty to be acting in violation of Microsoft's terms of service. *Id.*

Fourth, Microsoft established the DCU in 2008. As noted, this is an internal team of technical, legal, and business experts that fight cybercrime on a global scale, protect individuals and organizations, and safeguard the integrity of Microsoft services. DCU investigators frequently uncover evidence of cybercrime not otherwise detected by law enforcement, and may bring information to the attention of law enforcement for criminal prosecution. At its core, DCU works to increase the operational cost of cybercrime by disrupting the infrastructure used by cybercriminals through civil lawsuits and technical measures.

To date, DCU has disrupted the infrastructure of roughly 25 botnets, which are networks of computers controlled by cybercriminals, or in some cases nation-states. Those botnets were used to inject malware for unauthorized access to a victim's computer, or to deploy ransomware (a form of malware) to encrypt a victim's computer system until a ransom was paid to the attacker in exchange for a password needed to regain control of the system. Cambric Decl. ¶ 9.[1] DCU regularly prevents these botnets from distributing their malware, controlling victims' computers, and terrorizing individuals and organizations around the world. In partnership with U.S. and foreign governments, as well as Internet service

[1] *See, e.g.*, *Microsoft Corp.* v. *John Does 1-2*, No. 1:23-cv-02447 (E.D.N.Y. 2023) (Morrison, J.); *Microsoft Corp.* v. *Malikov*, No. 1:22-cv-01328 (N.D. Ga.) (Cohen, J.); *Microsoft Corp.* v. *John Does 1-5.*, No. 1:15-cv-6565 (E.D.N.Y. 2015) (Gleeson, J.); *Microsoft Corp.* v. *John Does 1-39*, No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.); *Microsoft Corp.* v. *Peng Yong*, No. 1:12-cv-1004 (E.D. Va. 2012) (Lee, J.); *Microsoft Corp.* v. *Piatti*, No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.); *Microsoft Corp.* v. *John Does 1-11*, No. 2:11-cv-00222 (W.D. Wash. 2011) (Robart, J.); *Microsoft Corp.* v. *John Does 1-27*, No. 1:10-cv-156 (E.D. Va. 2010) (Brinkema, J.).

providers, DCU has identified and shared information about crimes against approximately 500 million botnet victims worldwide.

B. The Defendants' Criminal Scheme

Defendants are engaged in what is known as crime-as-a-service ("CaaS"), a business model involving the sale of sophisticated criminal tools and services by experienced cybercriminals to customers (sometimes with much less experience) for the commission of future crimes. CaaS schemes such as the one run by Defendants are especially harmful to the public, as they empower vast numbers of criminals with limited knowledge and expertise to carry out attacks with relative ease. *See* Mason Decl. ¶¶ 6–23; Boffa Decl. ¶¶ 14–15; Declaration of Christopher Stangl in Support of Plaintiff Microsoft's Motion for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause ("Stangl Decl.") ¶¶ 10–11. While these Defendants are sophisticated, and their criminal conduct wide-ranging, their scheme to obtain and sell fraudulent email accounts and CAPTCHA tokens is, at its core, fairly straightforward.

1. The Procurement and Sale of Fraudulent Microsoft Email Accounts

Defendants' online marketplace for the sale of fraudulent Microsoft Outlook accounts can be found at https://hotmailbox.me/home (the "Hotmailbox Website"). Lyons Decl. ¶¶ 10, 13–18; Stangl Decl. ¶ 10; Mason Decl. ¶ 5; Boffa Decl. ¶ 10. The shelves of this virtual store are effectively stocked by Defendants' bots, which, through a series of false representations, and by impersonating actual humans, obtain millions of free Microsoft email accounts. Among other things, the Defendants, through their bots:

- falsely represent that they will not "circumvent any restrictions on access to, usage, or availability of [Microsoft's] Services" (Lyons Decl. Ex. 2 § 3(a)(vi)), when, in fact, they are actively breaching Microsoft's security restrictions against bots;
- provide false and fictitious identifying information, including fake names

and birthdates for non-existent persons purporting to be real users of Microsoft services;

- falsely represent they will "not . . . use any false, inaccurate or misleading information when signing up for [a] Microsoft account" (*id.* § 4(a)(i)), when, in fact, the bots already misrepresented that they are human users and provided fake identifying information;

- falsely represent they will not "transfer [their] Microsoft account credentials to another user or entity" (*id.*), when, in fact, the Defendants intend to, and regularly do, sell such account credentials to customers of their criminal services;

- falsely represent they will not "engage in activity that is fraudulent, false or misleading" such as "impersonating someone else, creating fake accounts, [or] automating inauthentic activity" (*id.* § 3(a)(v)), when, in fact, they do exactly those things in bypassing Microsoft's CAPTCHA challenges (discussed below) and opening Outlook email accounts in the names of fictitious users;

- falsely represent they will not "help others break these rules" (*id.* § 3(a)(x)), when, in fact, Defendants' entire scheme is designed to help their customers violate multiple Microsoft rules, including those that prohibit "anything illegal" (*id.* § 3(a)(i)), sending "spam or engag[ing] in phishing, or try[ing] to generate or distribute malware" (*id.* § 3(a)(iii)), engaging in "activity that is harmful" to others (*id.* § 3(a)(vii)), and "infring[ing] upon the rights of others" (*id.* § 3(a)(viii)).

After making these overtly false statements, Defendants cause their bots to fraudulently solve and bypass Microsoft's CAPTCHA defenses. When any user (including the bots) seeks to create a free Microsoft account they are asked to: "Please solve the [following] puzzle so we know you're not a robot." *See* Mason Decl. ¶ 13. Microsoft then presents a CAPTCHA challenge, for example, asking the user to click each square containing a traffic light, crosswalk, automobile, or the like, in a picture of a puzzle. *Id.* ¶¶ 10, 13, 16. On millions of occasions, Defendants' bots solved these CAPTCHA challenges, each time falsely representing they were "not a robot." Lyons Decl. ¶ 14; Cambric Decl. ¶ 19; Boffa Decl. ¶ 16.

Defendant Tu sought to explain this CAPTCHA-solving process in a how-to video he posted on YouTube. *See* Mason Decl. ¶¶ 16–17 (discussing July 3, 2023 YouTube video titled, "1stCAPTCHA Chrome Extension - Automatic reCAPTCHA Solver," *available at* https://www.youtube.com/watch?v=Me4qnLu3UKM). Defendant Tu stated:

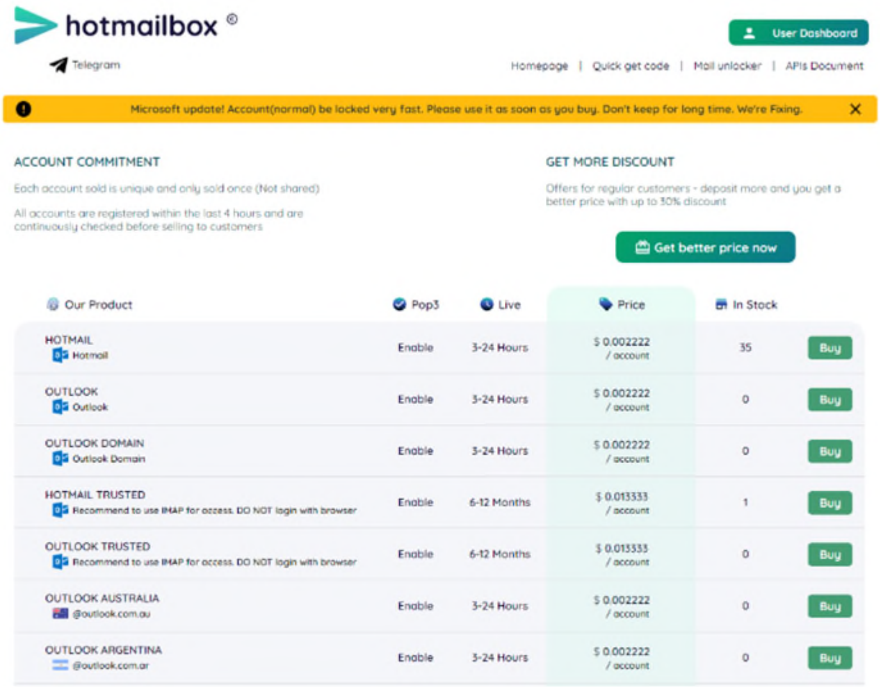
> We use state-of-the-art deep learning algorithms by Google, Meta, Microsoft, and NVIDIA AI. When you encounter a CAPTCHA challenge, it is solved in the cloud, and our active learning pipeline automatically and continuously improves the AI. Simply put, as more users use our extension, our AI gets better at solving CAPTCHAs. When new CAPTCHA types are added, our AI learns to solve them in real-time!

Id. ¶ 17; *see also* Boffa Decl. ¶¶ 8–9 (explaining that Microsoft cybersecurity vendor Arkose Labs "observed anomalies in Microsoft account-creation traffic, including the creation of accounts at a scale so large, fast, and efficient that it must have been perpetrated through automated, machine-learning technology (rather than through human actions)").

Each time Defendants' bots complete a CAPTCHA test (*e.g.*, by correctly identifying all the traffic lights, crosswalks, or automobiles, etc.), the CAPTCHA software provides a unique digital token that the bots redeem to satisfy that particular CAPTCHA challenge, which the bots then use to procure a Microsoft email account. Boffa Decl. ¶¶ 5, 7.

The Hotmailbox Website offers Defendants' customers a literal menu of these fraudulently-obtained Microsoft email accounts for purchase. Lyons Decl. ¶ 13. For example, as shown in Figure 1 below, a customer can purchase one of these Microsoft Outlook accounts registered in the name of a fictitious user for $0.002222, or 1,000 of them for $2.22. *See* Lyons Decl. ¶ 13; Boffa Decl. ¶ 17. Defendants disclose that the account will only be "live" for 3 to 24 hours, which is the result of Microsoft's continuous efforts to identify and suspend fraudulent accounts. Cambric Decl. ¶¶ 11, 16; Boffa Decl. ¶ 9. Given that bona fide consumers can open Microsoft Outlook accounts on their own for free, there is no conceivable lawful purpose for buying a Microsoft Outlook account registered to a fake person in breach of Microsoft's terms of service. *See* Stangl Decl. ¶ 10; Mason Decl. ¶¶ 25–29; Lyons Decl. ¶ 9. The brazenly criminal nature of this scheme is made plain by the banner at the top of the screen in Figure 1 noting that each account will be "locked very fast," so "[p]lease use it as soon as you buy." Lyons Decl. ¶ 18.

FIGURE 1



Microsoft update! Account(normal) be locked very fast. Please use it as soon as you buy. Don't keep for long time. We're Fixing.

ACCOUNT COMMITMENT

Each account sold is unique and only sold once (Not shared)

All accounts are registered within the last 4 hours and are continuously checked before selling to customers

GET MORE DISCOUNT

Offers for regular customers - deposit more and you get a better price with up to 30% discount

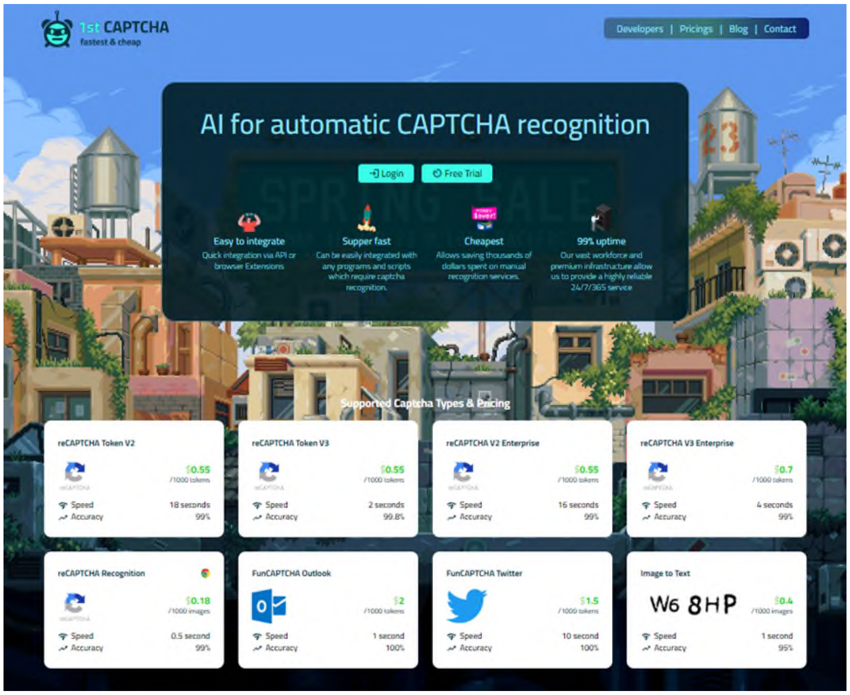
Our Product	Pop3	Live	Price	In Stock	
HOTMAIL Hotmail	Enable	3-24 Hours	$ 0.002222 / account	35	Buy
OUTLOOK Outlook	Enable	3-24 Hours	$ 0.002222 / account	0	Buy
OUTLOOK DOMAIN Outlook Domain	Enable	3-24 Hours	$ 0.002222 / account	0	Buy
HOTMAIL TRUSTED Recommend to use IMAP for access. DO NOT login with browser	Enable	6-12 Months	$ 0.013333 / account	1	Buy
OUTLOOK TRUSTED Recommend to use IMAP for access. DO NOT login with browser	Enable	6-12 Months	$ 0.013333 / account	0	Buy
OUTLOOK AUSTRALIA @outlook.com.au	Enable	3-24 Hours	$ 0.002222 / account	0	Buy
OUTLOOK ARGENTINA @outlook.com.ar	Enable	3-24 Hours	$ 0.002222 / account	0	Buy

Figure 1 also illustrates how the Defendants' Hotmailbox Website continuously and systematically misappropriates Microsoft's trademarks—including those relating to Microsoft Outlook—without Microsoft's authorization. Lyons Decl. ¶¶ 30–32. As explained below in Sections I(F) and II(B)(1)(b), the Defendants continuously sully Microsoft's valuable trademarks and brand by utilizing those trademarks to sell fraudulent accounts and to sell CAPTCHA-defeating tokens on their 1stCAPTCHA Website as discussed below. Those trademarks are also misappropriated every time a cybercriminal uses a fraudulent Microsoft account sold by the Enterprise to send an email to an unwitting victim, because those emails appear to be from a legitimate Microsoft account, but are actually a Trojan horse used to spread malware and cause substantial and sometimes devastating harm.

2. <u>The Procurement and Sale of CAPTCHA-Defeating Tokens</u>

As noted, Defendants also operate a second illicit online marketplace—available at https://1stcaptcha.com—where they market and sell CAPTCHA tokens recovered by their bots (the "1stCAPTCHA Website"). This site does not sell actual email addresses like the Hotmailbox Website, but instead offers tokens that can be used directly by Defendants' customers to defeat CAPTCHA tests presented by Microsoft, or any other business (*e.g.*, a social media company) that uses a similar anti-fraud tool. For example, as shown in Figure 2, a customer can purchase 1,000 CAPTCHA-solving tokens—each procured by the fraudulent process described above—for $2, enabling them to obtain for themselves numerous fraudulent Microsoft Outlook accounts, or to use the tokens on other sites. *See id.* ¶ 20. As a result of Microsoft's continuous efforts to prevent such misuses of its services, the tokens are only useable for a matter of seconds or less. *See* Lyons Decl. ¶ 23; Boffa Decl. ¶ 5.

FIGURE 2



AI for automatic CAPTCHA recognition

Easy to integrate
Quick integration via API or browser Extensions

Supper fast
Can be easily integrated with any programs and scripts which require captcha recognition.

Cheapest
Allows saving thousands of dollars spent on manual recognition services.

99% uptime
Our vast workforce and premium infrastructure allow us to provide a highly reliable 24/7/365 service

Supported Captcha Types & Pricing

reCAPTCHA Token V2
$0.55 /1000 tokens
Speed 18 seconds
Accuracy 99%

reCAPTCHA Token V3
$0.55 /1000 tokens
Speed 2 seconds
Accuracy 99.8%

reCAPTCHA V2 Enterprise
$0.55 /1000 tokens
Speed 16 seconds
Accuracy 99%

reCAPTCHA V3 Enterprise
$0.7 /1000 tokens
Speed 4 seconds
Accuracy 99%

reCAPTCHA Recognition
$0.18 /1000 images
Speed 0.5 second
Accuracy 99%

FunCAPTCHA Outlook
$2 /1000 tokens
Speed 1 second
Accuracy 100%

FunCAPTCHA Twitter
$1.5 /1000 tokens
Speed 10 second
Accuracy 100%

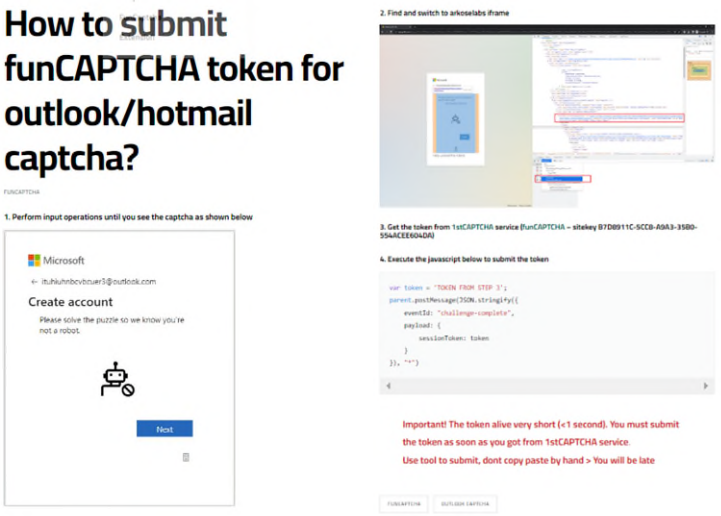
Image to Text
W6 8HP
$0.4 /1000 images
Speed 1 second
Accuracy 95%

The 1stCAPTCHA Website also includes a blog that brazenly provides step-by-step instructions on how to use such tokens to bypass Microsoft's security systems to obtain fraudulent Outlook accounts. Lyons Decl. ¶ 23.[2] As explained by Defendants, Step 1 is to commence the process of opening a Microsoft account. *Id.* Step 2 begins when the CAPTCHA challenge is presented ("so we know you're not a robot"), at which point the customer is instructed to buy a CAPTCHA-solving token, which Defendants' bots then obtain for the customer through the fraudulent process described above. *See id.* The guidance tells customers they can use their own bots to open Microsoft accounts in bulk with such tokens, noting that customers should "[u]se tool

[2] *See id.* Ex. 3 (*How to submit funCAPTCHA token for outlook/hotmail captcha?*, 1STCAPTCHA (Sept. 6, 2023), https://1stcaptcha.com/blog/how-to-submit-funcaptcha-token-for-outlook-hotmail-captcha/).

to submit" the tokens; "dont [*sic*] copy paste by hand > You will be late" as "[t]he token alive very short (< 1 second)." *See id.*[3]

FIGURE 3



How to submit funCAPTCHA token for outlook/hotmail captcha?

FUNCAPTCHA

1. Perform input operations until you see the captcha as shown below

Microsoft
← ituhiuhnbcvbcuer3@outlook.com
Create account
Please solve the puzzle so we know you're not a robot.
Next

2. Find and switch to arkoselabs iframe

3. Get the token from 1stCAPTCHA service (funCAPTCHA – sitekey B7D8911C-5CC8-A9A3-35B0-554ACEE604DA)

4. Execute the javascript below to submit the token

```
var token = 'TOKEN FROM STEP 3';
parent.postMessage(JSON.stringify({
    eventId: "challenge-complete",
    payload: {
        sessionToken: token
    }
}), "*")
```

Important! The token alive very short (<1 second). You must submit the token as soon as you got from 1stCAPTCHA service.
Use tool to submit, dont copy paste by hand > You will be late

The 1stCAPTCHA Website blog also contains entries explaining how to defeat the CAPTCHA defenses employed by X (formerly Twitter) and Google, *see* Lyons Decl. ¶ 23,[4] demonstrating that Defendants' scheme is a significant issue not only for Microsoft, but for the technology industry as a whole. Boffa Decl. ¶ 21.

To meet the ever-changing threats from criminal actors like the Defendants, Microsoft devotes tens of millions of dollars of resources each year to upgrading its cybersecurity measures,

[3] Defendants initially marketed this criminal service via websites available at https://anycaptcha.com (the "AnyCAPTCHA Website") and https://nonecaptcha.com (the "NoneCAPTCHA Website"), but later rebranded and moved the service to the 1stCAPTCHA Website. Lyons Decl. ¶¶ 10, 22; Mason Decl. ¶ 5; Boffa Decl. ¶¶ 9–12, 15, 20. Since this rebranding, internet users who attempt to visit the AnyCAPTCHA and NoneCAPTCHA Websites are automatically redirected to the 1stCAPTCHA Website. Lyons Decl. ¶ 22.

[4] *See id.* Ex. 4 (*How to bypass Twitter FunCAPTCHA using 1stCAPTCHA*, 1STCAPTCHA (Sept. 17, 2023), https://1stcaptcha.com/blog/how-to-bypass-twitter-funcaptcha-using-1stcaptcha/); *id.* Ex. 5 (*How to distinguish between different types of reCAPTCHA: v2, v3, enterprise*, 1STCAPTCHA (Sept. 6, 2023), https://1stcaptcha.com/blog/how-to-distinguish-recaptcha-v2-v3-enterprise/).

including making its CAPTCHA challenges more difficult for bots to solve, Cambric Decl. ¶¶ 5, 7, 20; *see* Boffa Decl. ¶ 18, though Defendants have continually adapted in an attempt to overcome these measures, Cambric Decl. ¶ 17; Boffa Decl. ¶ 9. For example, in late August 2023, in response to measures taken by Microsoft to suspend fraudulent Microsoft Outlook accounts that were purchased from the Defendants' Hotmailbox Website, the Defendants posted the banner (depicted in Figure 1 above) warning customers to use the accounts immediately. *See* Lyons Decl. ¶¶ 13, 18.

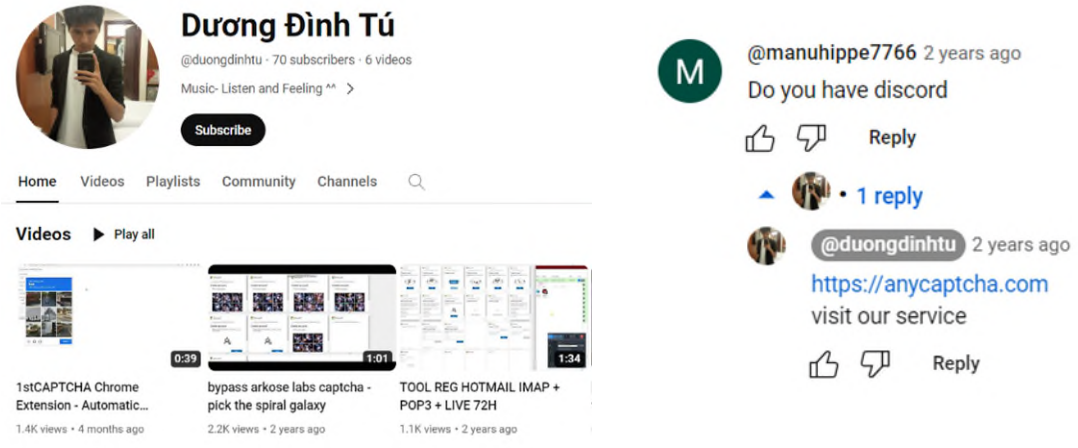
C. Evidence Linking Defendants to the CAPTCHA Fraud

Defendants Duong Dinh Tu ("Tu"), Linh Van Nguyen ("Linh") (a/k/a Nguyen Van Linh), and Tai Van Nguyen ("Tai") are members of and have been operating an illegal enterprise, including the criminal services offered by the Hotmailbox and 1stCAPTCHA Websites. It is not presently known whether there are others who are also part of this criminal conspiracy.

1. Defendant Duong Dinh Tu

According to a search of publicly available Internet domain registration data using a domain name lookup (also called a WHOIS lookup), Defendant Duong Dinh Tu of Vietnam has been the registrant of the Hotmailbox Website from at least in or about November 2021 through in or about July 2023. Mason Decl. ¶ 7. Defendant Tu has a YouTube channel—under the YouTube handle "@duongdinhtu"—on which he publicizes both the Hotmailbox and 1stCAPTCHA services. *Id.* ¶ 9. This YouTube channel includes videos showing recordings of a computer running bots to defraud Microsoft and bypass its CAPTCHA challenges. *See id.* ¶¶ 9–17. As shown in Figure 4, Tu's YouTube channel includes a video entitled "bypass arkose labs captcha" that has been viewed thousands of times, and includes a comments page in which he posted a comment referring to 1stCAPTCHA as "our service." *Id.* ¶¶ 9, 15.

FIGURE 4



Dương Đình Tú

@duongdinhtu · 70 subscribers · 6 videos

Music- Listen and Feeling ^^ >

Subscribe

Home Videos Playlists Community Channels

Videos ▶ Play all

0:39 1stCAPTCHA Chrome Extension - Automatic...
1.4K views • 4 months ago

1:01 bypass arkose labs captcha - pick the spiral galaxy
2.2K views • 2 years ago

1:34 TOOL REG HOTMAIL IMAP + POP3 + LIVE 72H
1.1K views • 2 years ago

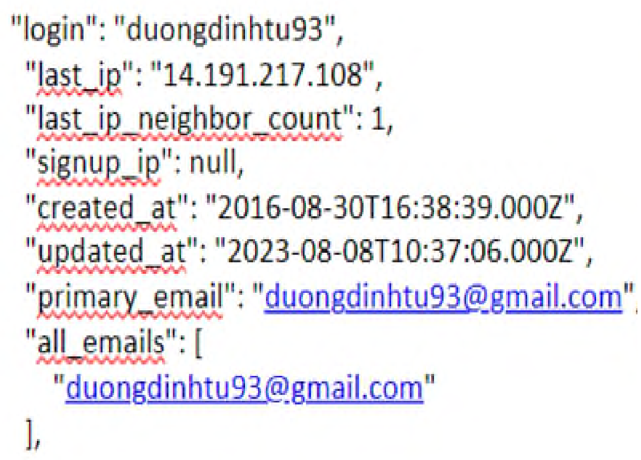
@manuhippe7766 2 years ago
Do you have discord
Reply

1 reply

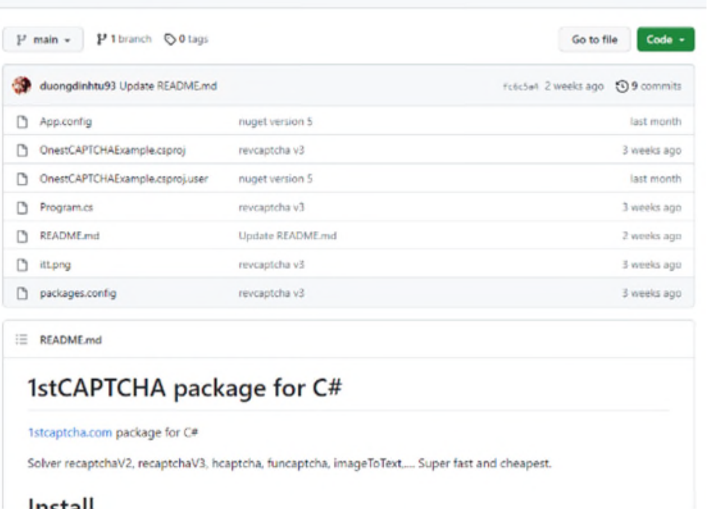
@duongdinhtu 2 years ago
https://anycaptcha.com
visit our service
Reply

DCU's investigation also confirmed that Defendant Tu has personally edited the source code for the 1stCAPTCHA service via a website known as GitHub, *available at* https://github.com/1stcaptcha (the "1stCAPTCHA GitHub Page"). *Id.* ¶ 18. GitHub is an Internet cloud-based repository of computer code that helps software developers collaborate in programming, storing, managing, revising, and tracking changes to their code. *See id.* ¶ 18; *see also* Lyons Decl. ¶ 25. Among other things, the 1stCAPTCHA GitHub Page houses the software code necessary to utilize the CAPTCHA-solving tokens sold on the 1stCAPTCHA Website. Mason Decl. ¶ 18. As shown in Figure 5, Tu has edited the 1stCAPTCHA source code several times, including as recently as August 8, 2023, via a GitHub account registered under his Gmail account address ("duongdinhtu93@gmail.com"). *Id.*

FIGURE 5



```
"login": "duongdinhtu93",
 "last_ip": "14.191.217.108",
 "last_ip_neighbor_count": 1,
 "signup_ip": null,
 "created_at": "2016-08-30T16:38:39.000Z",
 "updated_at": "2023-08-08T10:37:06.000Z",
 "primary_email": "duongdinhtu93@gmail.com",
 "all_emails": [
   "duongdinhtu93@gmail.com"
 ],
```



duongdinhtu93 Update README.md fc6c5a4 2 weeks ago 9 commits

App.config	nuget version 5	last month
OnestCAPTCHAExample.csproj	revcaptcha v3	3 weeks ago
OnestCAPTCHAExample.csproj.user	nuget version 5	last month
Program.cs	revcaptcha v3	3 weeks ago
README.md	Update README.md	2 weeks ago
itt.png	revcaptcha v3	3 weeks ago
packages.config	revcaptcha v3	3 weeks ago

README.md

1stCAPTCHA package for C#

1stcaptcha.com package for C#

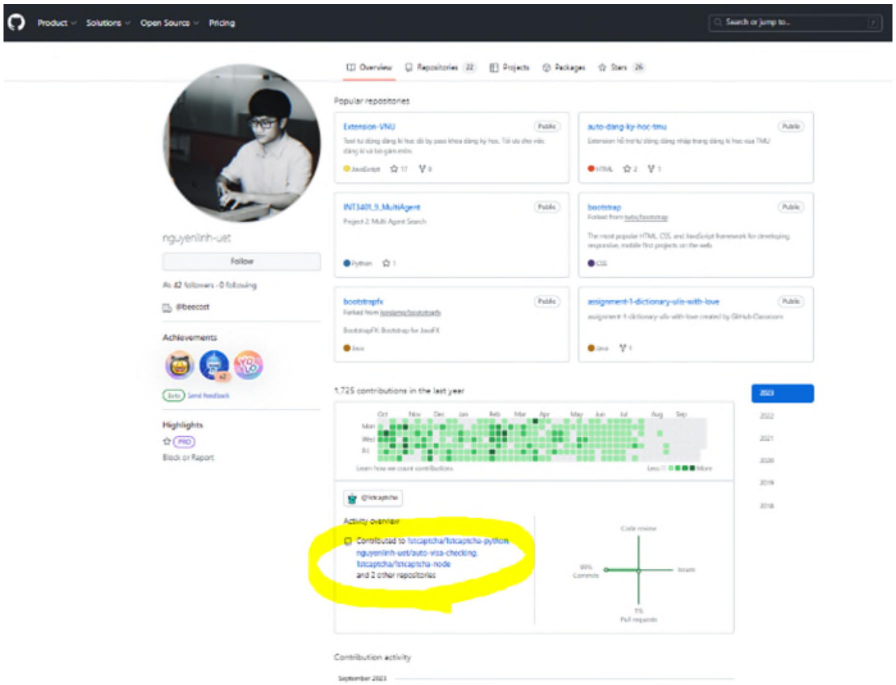
Solver recaptchaV2, recaptchaV3, hcaptcha, funcaptcha, imageToText,.... Super fast and cheapest.

Install

1. **Defendant Linh Van Nguyen (a/k/a Nguyen Van Linh)**

Defendant Linh Van Nguyen (a/k/a Nguyen Van Linh) also edited the source code for the 1stCAPTCHA service via the 1stCAPTCHA GitHub Page on over 100 occasions during the period from approximately October 2020 through July 2023. Mason Decl. ¶ 19. A screenshot of his GitHub account page is depicted in Figure 6 below. *See id.*

FIGURE 6



nguyenlinh-uet

42 followers · 0 following

@beecost

Popular repositories

Extension-VNU

auto-dang-ky-hoc-tmu

INT3401_5_MultiAgent

Project 2: Multi Agent Search

bootstrap

The most popular HTML, CSS, and JavaScript framework for developing responsive, mobile first projects on the web.

bootstrapfx

BootstrapFX: Bootstrap for JavaFX

assignment-1-dictionary-uis-with-love

1,725 contributions in the last year

Learn how we count contributions

@1stcaptcha

Activity overview

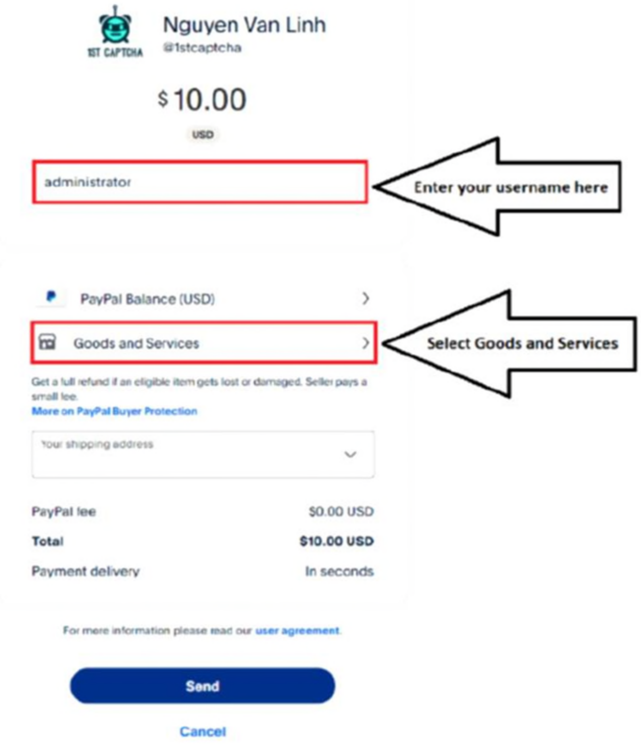
Contributed to 1stcaptcha/1stcaptcha-python, nguyenlinh-uet/auto-visa-checking, 1stcaptcha/1stcaptcha-node and 2 other repositories

Contribution activity

September 2023

Linh is also connected directly to the 1stCAPTCHA Website via the payment processing service, PayPal, which is used by Defendants, unbeknownst to PayPal, to collect illicit proceeds. *Id.* ¶ 20. A screenshot of this PayPal interface plainly identifies Linh's association with the 1stCAPTCHA Website's PayPal account, as depicted in Figure 7. *Id.*

FIGURE 7



1ST CAPTCHA

Nguyen Van Linh
@1stcaptcha

$10.00
USD

administrator

Enter your username here

PayPal Balance (USD)

Goods and Services

Select Goods and Services

Get a full refund if an eligible item gets lost or damaged. Seller pays a small fee.
More on PayPal Buyer Protection

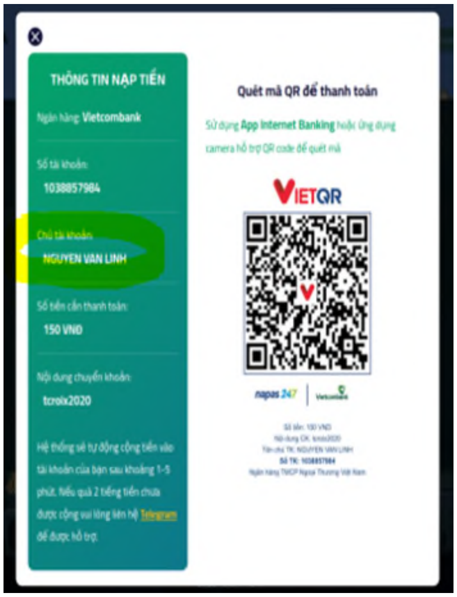
Your shipping address

PayPal fee	$0.00 USD
Total	**$10.00 USD**
Payment delivery	In seconds

For more information please read our user agreement.

The 1stCAPTCHA Website also permits customers to send cash for illicit services through a payment processing service at Vietcombank. *Id.* ¶ 21. A screenshot of the user interface to submit a Vietcombank payment to 1stCAPTCHA—noting Linh's association with 1stCAPTCHA's Vietcombank account—is depicted in Figure 8 below. *Id.*

FIGURE 8



THÔNG TIN NẠP TIỀN

Ngân hàng: Vietcombank

Số tài khoản:
1038857984

Chủ tài khoản:
NGUYEN VAN LINH

Số tiền cần thanh toán:
150 VND

Nội dung chuyển khoản:
tcroix2020

Hệ thống sẽ tự động cộng tiền vào tài khoản của bạn sau khoảng 1-5 phút. Nếu quá 2 tiếng tiền chưa được cộng vui lòng liên hệ Telegram để được hỗ trợ.

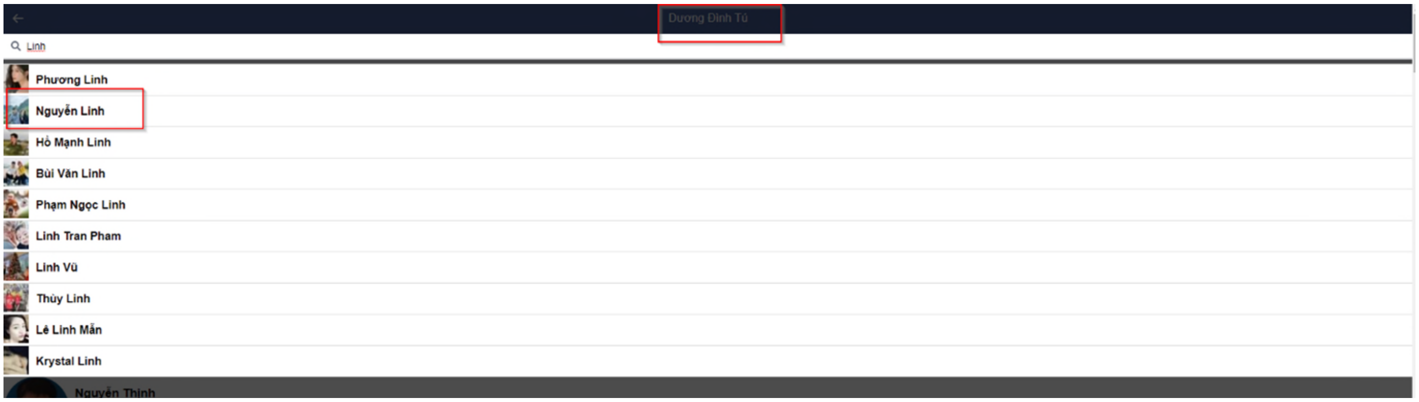
Quét mã QR để thanh toán

Sử dụng App Internet Banking hoặc ứng dụng camera hỗ trợ QR code để quét mã

Số tiền: 150 VND
Nội dung CK: tcroix2020
Tên chủ TK: NGUYEN VAN LINH
Số TK: 1038857984
Ngân hàng TMCP Ngoại Thương Việt Nam

Defendants Linh Van Nguyen (a/k/a Nguyen Van Linh) and Duong Dinh Tu are "friends" on Facebook, according to Defendant Tu's Facebook "friends" list. *Id.* ¶ 22. A screenshot from the Facebook account of Defendant Tu, showing that Tu is "friends" with "Nguyen Linh" (who is believed to be Defendant Linh Van Nguyen), is depicted in Figure 9 below. *Id.*

FIGURE 9



Dương Đình Tú

Linh

Phương Linh
Nguyễn Linh
Hồ Mạnh Linh
Bùi Văn Linh
Phạm Ngọc Linh
Linh Tran Pham
Linh Vũ
Thùy Linh
Lê Linh Mẫn
Krystal Linh
Nguyễn Thịnh

2. Defendant Tai Van Nguyen

Like his co-Defendants, Defendant Tai Van Nguyen has edited the source code for the 1stCAPTCHA service via the 1stCAPTCHA GitHub Page. *Id.* ¶ 23. Tai has a GitHub account registered to his email account "nvt.kscntt@gmail.com." *Id.* According to data retrieved from his GitHub account, Tai edited the 1stCAPTCHA's source code as recently as July 2023. *Id.*

D. Defendants' Connection to This District

To investigate the Defendants' criminal activities, Microsoft retained external cybercrime experts at the Berkeley Research Group ("BRG"). Lyons Decl. ¶ 28. From August through October 2023, BRG made several undercover purchases of Microsoft Outlook accounts from the Hotmailbox Website and CAPTCHA-defeating tokens from the 1stCAPTCHA Website, including purchases made from BRG's offices in New York, New York. *See* Stangl Decl. ¶¶ 12–28. These undercover purchases confirmed that the Hotmailbox and 1stCAPTCHA Websites provide Microsoft Outlook accounts and CAPTCHA-defeating tokens to obtain bulk fraudulent Outlook accounts in exchange for payment, and that those tools successfully bypass Microsoft's CAPTCHA security measures. *See id.*

Information obtained through BRG's undercover purchases demonstrates that Defendants are utilizing at least one Internet service provider ("ISP") data center that is located in New York, New York to facilitate the Enterprise's criminal services. Lyons Decl. ¶¶ 28–29. Indeed, nearly 80% of the fraudulent Microsoft accounts obtained through BRG's undercover purchases from the Hotmailbox Website were registered with IP addresses deriving from an ISP data center in New York, New York. *See id.*

E. Harm to Microsoft, Its Customers, and the Public

Despite Microsoft's best efforts at protecting itself and its customers, the Defendants' bots have repeatedly and persistently used fraud to bypass the Company's security measures and CAPTCHA challenges, procuring millions of fraudulent Microsoft email accounts, along with CAPTCHA tokens, and selling them to cybercriminals. *See* Cambric Decl. ¶ 19; Mason Decl. ¶¶ 25–29. As set forth above, fraudulent accounts sold by the Defendants can be used, and are believed to have been used, in cybercrime activity that has inflicted severe harm on Microsoft customers. Mason Decl. ¶¶ 25–29. Through their criminal enterprise, Defendants have caused tens of millions of dollars in damage to Microsoft and have irreparably harmed its reputation, goodwill, and critical customer relationships. Cambric ¶¶ 5, 7, 20; Boffa Decl. ¶¶ 17–18.

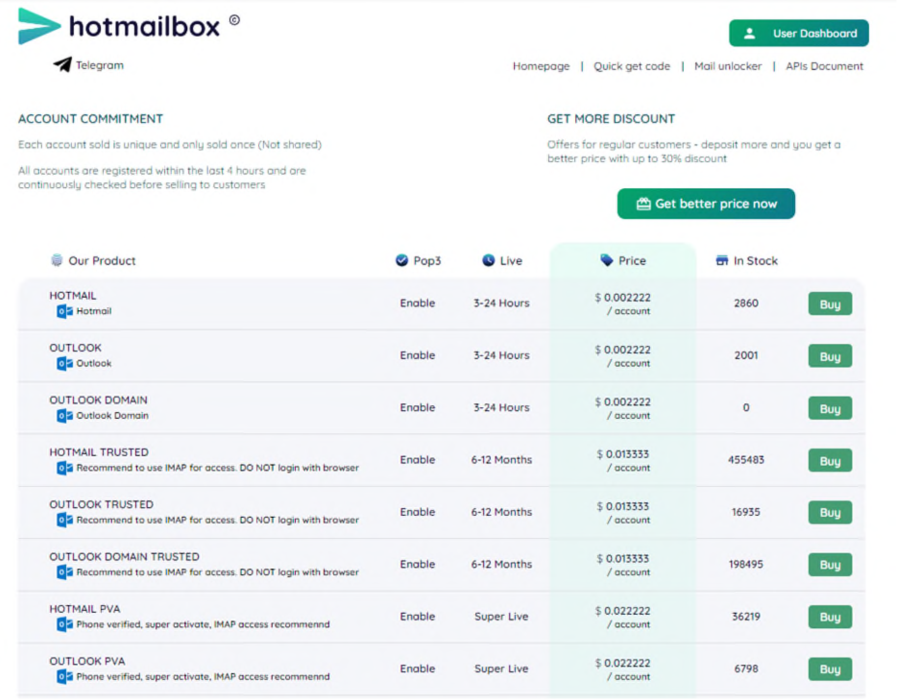
As described in the declarations accompanying this motion, Microsoft email accounts fraudulently obtained and sold by Defendants have been used to perpetrate cybercrime activity, including crimes committed by the groups known to Microsoft as Storm-0252, Storm-0455, and Octo Tempest, the latter of which recently brought ransomware attacks against flagship Microsoft customers. Mason Decl. ¶¶ 25–29. During these attacks, the computer systems of those customers were infected with ransomware that disabled operation-critical systems, resulting in service disruptions that inflicted hundreds of millions of dollars of damage. *Id.* Additionally, in or about March 2023, a major Microsoft customer and partner reported that it received a flood of requests from Outlook and Hotmail accounts—later determined to have come from the Hotmailbox Website—seeking free trials of its services. Cambric Decl. ¶ 21. The requests were so numerous that they eventually caused outages in that company's systems, leading it to block all new account sign-ups from Microsoft Outlook and Hotmail, thus irreparably harming Microsoft's business relationship with the company. *Id.*

Defendants' ongoing fraudulent scheme presents a continuing threat to Microsoft, its customers, and the public, all of whom have suffered and will continue to suffer irreparable harm at the hands of Defendants absent injunctive and other relief to disrupt their criminal scheme. Cambric Decl. ¶ 22; Lyons Decl. ¶ 35. Indeed, as a direct result of Defendants' conduct, Microsoft has already been forced to spend tens of millions of dollars in connection with investigating, identifying, and remediating the threats caused by the Fraudulent Enterprise. Cambric Decl. ¶¶ 5, 7, 20; Boffa Decl. ¶¶ 17–18.

F. Defendants' Exploitation of Microsoft's Trademarks

In selling fraudulent Microsoft accounts, the Hotmailbox Website misuses several Microsoft trademarks without Microsoft's authorization, including its Outlook launch icon trademark, its Outlook word mark, and its Hotmail word mark, registration copies of which are annexed as Appendix B to Microsoft's Complaint. Lyons Decl. ¶¶ 30–31. A screenshot of the Hotmailbox Website illustrating how it misappropriates those trademarks, as well as a zoomed-in side-by-side comparison with Microsoft's trademarks, are depicted in Figures 10 and 11 below. *Id.*

FIGURE 10



ACCOUNT COMMITMENT

Each account sold is unique and only sold once (Not shared)

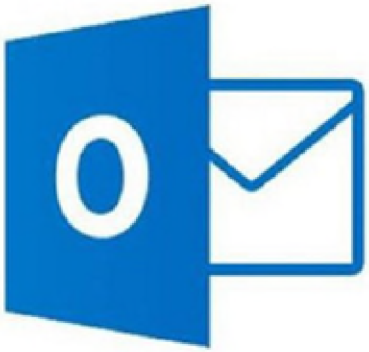
All accounts are registered within the last 4 hours and are continuously checked before selling to customers

GET MORE DISCOUNT

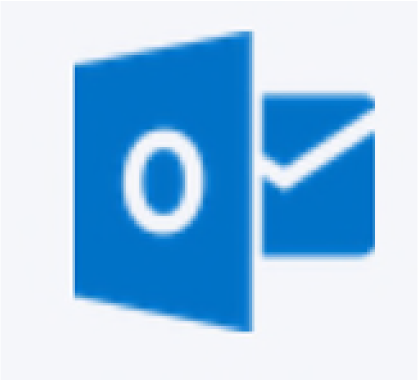
Offers for regular customers - deposit more and you get a better price with up to 30% discount

Our Product	Pop3	Live	Price	In Stock	
HOTMAIL Hotmail	Enable	3-24 Hours	$ 0.002222 / account	2860	Buy
OUTLOOK Outlook	Enable	3-24 Hours	$ 0.002222 / account	2001	Buy
OUTLOOK DOMAIN Outlook Domain	Enable	3-24 Hours	$ 0.002222 / account	0	Buy
HOTMAIL TRUSTED Recommend to use IMAP for access. DO NOT login with browser	Enable	6-12 Months	$ 0.013333 / account	455483	Buy
OUTLOOK TRUSTED Recommend to use IMAP for access. DO NOT login with browser	Enable	6-12 Months	$ 0.013333 / account	16935	Buy
OUTLOOK DOMAIN TRUSTED Recommend to use IMAP for access. DO NOT login with browser	Enable	6-12 Months	$ 0.013333 / account	198495	Buy
HOTMAIL PVA Phone verified, super activate, IMAP access recommennd	Enable	Super Live	$ 0.022222 / account	36219	Buy
OUTLOOK PVA Phone verified, super activate, IMAP access recommennd	Enable	Super Live	$ 0.022222 / account	6798	Buy

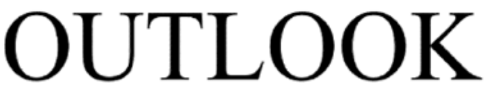
FIGURE 11



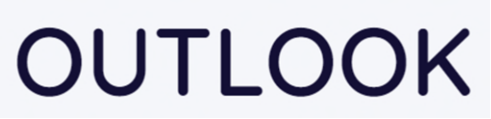
Microsoft’s Registered Trademark



Hotmailbox Website

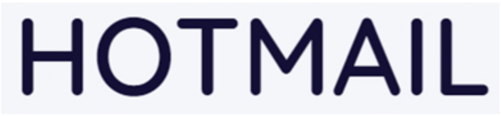


Microsoft’s Registered Trademark



Hotmailbox Website

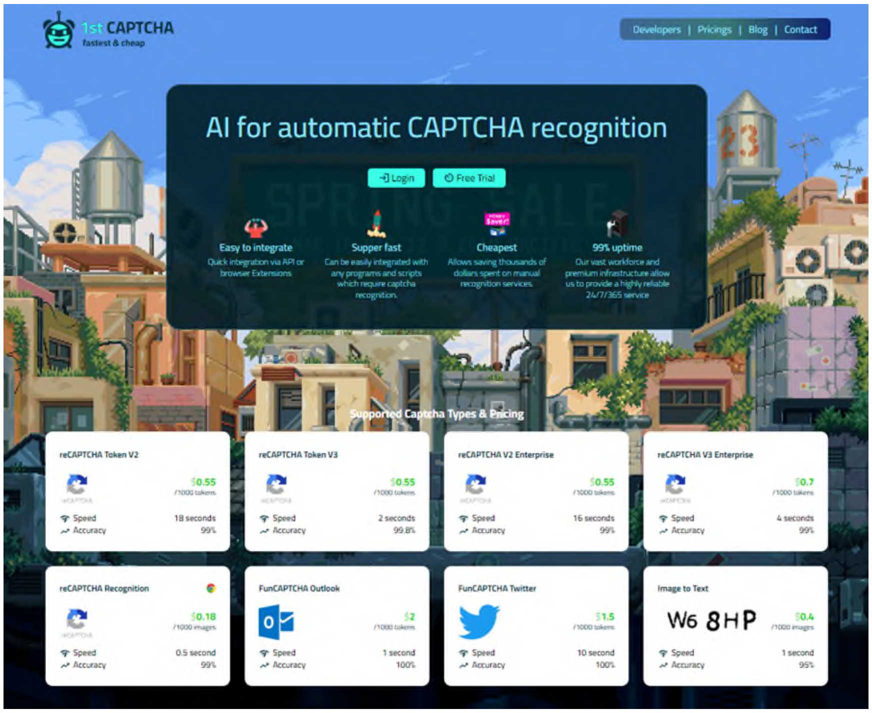
Microsoft's Registered Trademark



Hotmailbox Website

The 1stCAPTCHA Website also uses Microsoft's Outlook launch icon trademark without Microsoft's authorization to sell fraudulently-obtained CAPTCHA tokens. *Id.* ¶ 32. A screenshot of the 1stCAPTCHA Website illustrating how it misappropriates that trademark, as well as a zoomed-in side-by-side comparison with Microsoft's trademark, are depicted in Figures 12 and 13 below. *Id.*

FIGURE 12



AI for automatic CAPTCHA recognition

Easy to integrate
Quick integration via API or browser Extensions

Supper fast
Can be easily integrated with any programs and scripts which require captcha recognition.

Cheapest
Allows saving thousands of dollars spent on manual recognition services.

99% uptime
Our vast workforce and premium infrastructure allow us to provide a highly reliable 24/7/365 service

Supported Captcha Types & Pricing

reCAPTCHA Token V2
$0.55 /1000 tokens
Speed 18 seconds
Accuracy 99%

reCAPTCHA Token V3
$0.55 /1000 tokens
Speed 2 seconds
Accuracy 99.8%

reCAPTCHA V2 Enterprise
$0.55 /1000 tokens
Speed 16 seconds
Accuracy 99%

reCAPTCHA V3 Enterprise
$0.7 /1000 tokens
Speed 4 seconds
Accuracy 99%

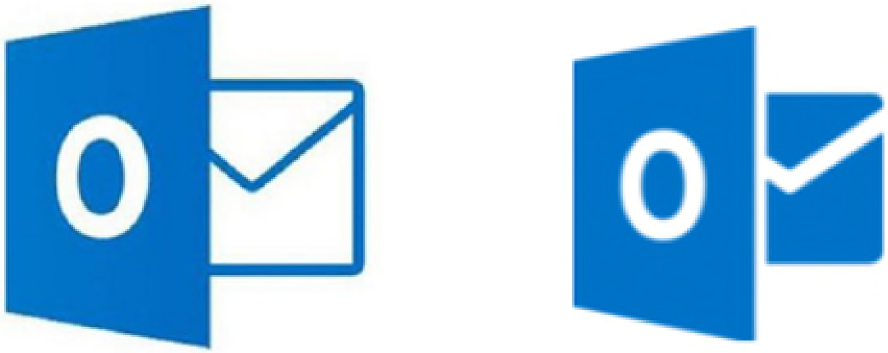
reCAPTCHA Recognition
$0.18 /1000 images
Speed 0.5 second
Accuracy 99%

FunCAPTCHA Outlook
$2 /1000 tokens
Speed 1 second
Accuracy 100%

FunCAPTCHA Twitter
$1.5 /1000 tokens
Speed 10 second
Accuracy 100%

Image to Text
W6 8HP
$0.4 /1000 images
Speed 1 second
Accuracy 95%

FIGURE 13



Microsoft's Registered Trademark 1stCAPTCHA Website

G. Disrupting the Fraudulent Enterprise

Through this lawsuit, Microsoft is requesting judicial authorization to take down the digital infrastructure supporting Defendants' operations. *Id.* ¶ 33. It is imperative that the requested actions be closely coordinated, such that IP addresses used by the Defendants' Fraudulent

Enterprise in various locations are directed by the Court to be turned off immediately, and simultaneously, to prevent the Defendants from relocating to alternative infrastructure and domains. *Id.* Microsoft's Proposed Order is therefore framed in a manner that enables coordinated efforts that will maximize the effectiveness of the relief sought. *Id.*

In the aggregate, the steps set forth in Microsoft's Proposed Order will immediately prevent Defendants from operating their Enterprise and will give control of their websites to Microsoft. *Id.* ¶ 34. The steps described in the Proposed Order are appropriate and necessary to suspend the ongoing injuries inflicted by the Fraudulent Enterprise on Microsoft, its consumers, and the public. *Id.* ¶ 35; Cambric Decl. ¶ 22.

II. ARGUMENT

Plaintiff's requested relief is warranted because (1) it is likely to succeed on the merits of its claims under the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962 ("RICO") and the Lanham Act, 15 U.S.C. §§ 1114 *et seq.*, 1125(a) and (c), and for tortious interference with business relationships, conversion, trespass to chattels, and unjust enrichment; (2) Defendants' conduct has caused Plaintiff irreparable harm, including to its reputational value and goodwill; (3) the balance of equities tips decidedly in Plaintiff's favor, as there is no legitimate reason why Defendants should be permitted to continue their unlawful scheme; (4) issuing an injunction is in the public interest because it will deprive cybercriminals of key tools that they use to harm the public; and (5) the All Writs Act provides this Court with the authority needed to direct third parties to assist Plaintiff in dismantling Defendants' unlawful infrastructure. The relief sought by Plaintiff must occur *ex parte* because if Defendants are notified of this action, they will swiftly move their infrastructure, frustrating the prosecution of this action.

A. Legal Standard

A plaintiff is entitled to a temporary restraining order and preliminary injunction where (1) it is likely to succeed on the merits, (2) it is likely to suffer irreparable harm in the absence of preliminary relief, (3) the balance of equities tips in its favor, and (4) an injunction is in the public interest. *Winter* v. *Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008); *Citigroup Glob. Mkts., Inc.* v. *VCG Special Opportunities Master Fund Ltd.*, 598 F.3d 30, 34 (2d Cir. 2010); *see also Abdul Wali* v. *Coughlin*, 754 F.2d 1015, 1025 (2d Cir. 1985) ("A movant seeking to [demonstrate that 'he is likely to prevail on the merits'] need not show that success is an absolute certainty. He need only make a showing that the probability of his prevailing is better than fifty percent.").

In the Second Circuit, this standard is "flexible" and a movant is entitled to relief—even without demonstrating a likelihood of success on the merits—if it can show that there are "serious questions going to the merits" and that the "balance of hardships tips *decidedly* in its favor," assuming that the other factors are satisfied. *Citigroup Glob. Mkts., Inc.*, 598 F.3d at 35–38 (internal quotation marks omitted) (quoting *Jackson Dairy, Inc.* v. *H. P. Hood & Sons, Inc.*, 596 F.2d 70, 72 (2d Cir. 1979)); *see also id.* at 35 ("The 'serious questions' standard permits a district court to grant a preliminary injunction in situations where it cannot determine with certainty that the moving party is more likely than not to prevail on the merits of the underlying claims, but where the costs outweigh the benefits of not granting the injunction.").

B. Plaintiff's Requested Relief Is Warranted

In this case, there is a very high likelihood that Plaintiff will succeed on the merits, and that Plaintiff (along with other companies and the public at large) will continue to be irreparably harmed if the Defendants are able to continue to operate their Enterprise—specifically, the Hotmailbox and 1stCAPTCHA Websites. Defendants have no legitimate interests that would be harmed if this Court issues a temporary restraining order and injunction, and the effect on third parties (such as domain registries and registrars or IP address hosting companies) from which Defendants acquired the Appendix A domains will be negligible and temporary. The public interest also weighs heavily in favor of relief because harms caused by Defendants affect not only Microsoft, but also other companies and the public at large. Accordingly, the relief Plaintiff requests is warranted.

1. Plaintiff Is Likely to Succeed on the Merits of Its Claims

Plaintiff is likely to succeed on the merits of its claims, and as such its request for a Temporary Restraining Order and a preliminary injunction should be granted. Plaintiff sets forth the following statutory and common law claims: (1) violation of RICO, 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.

a) Plaintiff Is Likely to Succeed on Its RICO Claim

RICO prohibits "any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity." 18 U.S.C. § 1962(c). It is unlawful under RICO "for any person to conspire to violate" § 1962(c), regardless of whether that conspiracy ultimately comes to fruition. *Id.* § 1962(d). Moreover, "[a]ny person injured in his business or property by reason of a violation of" either of these provisions is entitled to recovery, *id.* § 1964(c), and this Court has "jurisdiction to prevent and restrain" such violations "by issuing appropriate orders," *id.* § 1964(a). *See also United States* v. *Carson*, 52 F.3d 1173, 1181–82 (2d Cir. 1995) ("the jurisdictional powers in § 1964(a) serve the goal of foreclosing future violations," and "the equitable relief available under RICO is intended to be 'broad enough to do all that is necessary'") (quoting S. Rep. No. 91-617, at 79 (1969)); *United States* v. *Sasso*, 215 F.3d 283, 290 (2d Cir. 2000) (same); *Trane Co.* v. *O'Connor Sec.*, 718 F.2d 26, 29 (2d Cir. 1983) (preliminary injunctions are proper under RICO where plaintiff "establishe[s] a likelihood of irreparable harm"). Microsoft is also entitled to disgorgement of Defendants' profits because such disgorgement will "serve[] to 'prevent and restrain' future RICO violations" by Defendants. *See Carson*, 52 F.3d at 1182; *Sasso*, 215 F.3d at 290–91; *United States* v. *Priv. Sanitation Indus. Ass'n of Nassau/Suffolk, Inc.*, 914 F. Supp. 895, 901 (E.D.N.Y. 1996). In other words, awarding Microsoft disgorgement of Defendants' profits is appropriate here because taking away the roughly $3 million in profits they have collected, *see* Boffa Decl. ¶ 17, will deprive the Defendants of the resources needed to continue their scheme, *see Carson*, 52 F.3d at 1182; *Sasso*, 215 F.3d at 290–91; *Priv. Sanitation Indus. Ass'n of Nassau/Suffolk, Inc.*, 914 F. Supp. at 901.

Put simply, the evidence before this Court demonstrates that Defendants have formed and associated with an unlawful enterprise, which they have used to engage in a pattern of racketeering activity involving millions of predicate acts of wire fraud, *see* 18 U.S.C. § 1343, which is a RICO predicate act under 18 U.S.C. § 1961(1)(B).

i. The Racketeering Enterprise

An associated-in-fact enterprise consists of "a group of persons associated together for a common purpose of engaging in a course of conduct" and "is proved by evidence of an ongoing organization, formal or informal, and by evidence that the various associates function as a continuing unit." *Boyle* v. *United States*, 556 U.S. 938, 944–45 (2009) (quoting *United States* v. *Turkette*, 452 U.S. 576, 583 (1981)). Such an enterprise "must have at least three structural features: a purpose, relationships among those associated with the enterprise, and longevity sufficient to permit these associates to pursue the enterprise's purpose." *Id.* at 946.

In this case, the Fraudulent Enterprise has existed at least since August 2021, *see* Boffa Decl. ¶ 8, when Defendants conspired to, and did, form an association-in-fact racketeering enterprise with a common purpose of developing and operating a scheme to profit from fraudulently-procured Microsoft accounts. This enterprise has continuously and effectively carried out its purpose of profiting from unlawful conduct through the AnyCAPTCHA, NoneCAPTCHA, 1stCAPTCHA, and Hotmailbox Websites, among other means, and will continue to do so absent the relief Microsoft requests.

The purpose of the Fraudulent Enterprise and the relationship between the Defendants is proven by (1) the repeated development and dissemination of fraudulently-procured Microsoft accounts, as well as CAPTCHA-defeating tokens, (2) the subsequent development and operation of fraudulently-procured Microsoft accounts to proliferate cyberattacks, and (3) Defendants' respective and interrelated roles in the sale, operation of, and profiting from their unlawful scheme, in furtherance of their common financial interests. *See* Mason Decl. ¶¶ 6–23 (explaining the roles of each Defendant in the Fraudulent Enterprise); *see also Boyle*, 556 U.S. at 947 (relationship and common interest may be inferred from "evidence used to prove the pattern of racketeering activity"); *United States* v. *Diaz*, 176 F.3d 52, 79 (2d Cir. 1999) ("[E]vidence of prior uncharged crimes and other bad acts . . . [i]s relevant because it tend[s] to prove the existence, organization and nature of the RICO enterprise, and a pattern of racketeering activity by each defendant-appellant.").

The fact that the Defendants are associated in a common criminal enterprise is evidenced by, among other things, their collective collaboration in programming the software used to perpetrate their fraudulent scheme on the 1stCAPTCHA GitHub Page, *see* Mason Decl. ¶¶ 18–19, 23, and the Facebook "friendship" between Defendants Linh and Tu, *id.* ¶ 22. *See supra* Section I(C).

ii. **Defendants' Pattern of Racketeering**

A pattern for RICO purposes "requires at least two acts of racketeering activity," the "last of which occurred within ten years" after "the commission of a prior act of racketeering activity." *H.J. Inc.* v. *Northwestern Bell Tel. Co.*, 492 U.S. 229, 237 (1989) (quoting 18 U.S.C. § 1961). A threat of continuing activity "is generally presumed when the enterprise's business is primarily or inherently unlawful." *MinedMap, Inc.* v. *Northway Mining*, *LLC*, 2022 WL 570082, at *2 (2d Cir. Feb. 25, 2022) (quoting *Spool* v. *World Child Int'l Adoption Agency*, 520 F.3d 178, 185 (2d Cir. 2008)). In this case, Defendants have conspired to, and have, conducted and participated in the operations of the Fraudulent Enterprise through a continuous pattern of predicate racketeering acts of wire fraud. Each predicate act of wire fraud is related to and in furtherance of the common unlawful purpose shared by the members of the Enterprise. These acts are ongoing and will continue unless and until this Court grants Plaintiff's request for a Temporary Restraining Order.

Defendants' acts of racketeering activity include millions of acts of wire fraud in violation of 18 U.S.C. § 1343. Under § 1343, whoever, "having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire" communication "in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice," is guilty of wire fraud. Defendants' illegal acts were conducted using interstate or foreign wires, and thus affected interstate or foreign commerce. Violation of the wire fraud statute constitutes "racketeering activity." 18 U.S.C. § 1961(1)(B).

In particular, Defendants received millions of dollars in payments in interstate and international commerce in exchange for their illicit services by operating the AnyCAPTCHA, NoneCAPTCHA, 1stCAPTCHA, and Hotmailbox Websites. *See* Mason Decl. ¶¶ 20–21; Lyons Decl. ¶¶ 17, 27; Stangl Decl. ¶¶ 10–28; Boffa Decl. ¶ 17; *see also United States* v. *Lowson*, 2010 WL 9552416, at *2 (D.N.J. Oct. 12, 2010) (denying motion to dismiss wire fraud counts where defendants "knowingly and willfully engaged to defraud Ticketmaster" by "circumvent[ing] computer code," by "writ[ing] automated software to defeat the vendors' security measures, including CAPTCHA," and by "opening thousands of connections and using CAPTCHA Bots to quickly solve CAPTCHA challenges"); *see also id.* (defendants "allegedly used various means of deception, including mimicking the steps a human would take when answering CAPTCHA challenges (including making mistakes), using thousands of non-consecutive IP addresses to create the illusion that the addresses were not owned by a single company," and "registering for fan clubs under fake names"). Here, as in *Lowson*, Defendants' "deceptive tactics in themselves suggest that the defendants knew what they were doing was wrong." 2010 WL 9552416, at *2; *see also* Lyons Decl. ¶ 18 (Defendants' "instruction on the Hotmailbox Website to use the fraudulent Microsoft accounts 'as soon as you buy,'" in order "to avoid suspension" by Microsoft, is "evidence that the Fraudulent Enterprise is aware that its account-creation and sale scheme violates Microsoft's Services Agreement").

iii. Plaintiff Was Harmed as a Direct Result of Defendants' Racketeering Activity

As a direct result of Defendants' conduct, Microsoft has been forced to spend tens of millions of dollars in connection with investigating, identifying, and remediating the threats caused by the Fraudulent Enterprise's racketeering activity. Cambric Decl. ¶¶ 5, 7, 20; Boffa Decl. ¶¶ 17–18. There is, accordingly, (1) "a direct relationship between the plaintiff's injury and the defendant's injurious conduct" and (2) "but for the RICO violation, [Microsoft] would not have been injured." *Alix* v. *McKinsey & Co.*, 23 F.4th 196, 203 (2d Cir. 2022), *cert. denied*, 143 S. Ct. 302 (2022). Plaintiff is therefore likely to succeed on the merits of its RICO claim.

b) Plaintiff Is Likely to Succeed on Its Lanham Act Claims

Defendants' misappropriation of Microsoft's registered trademarks constitutes trademark dilution, trademark infringement, false designation of origin, federal false advertising, and federal unfair competition under Sections 43(c), 32(1), and 43(a) of the Lanham Act.

Section 43(c) of the Lanham Act prohibits the use of a mark or trade name in commerce that is likely to cause dilution by blurring or dilution by tarnishment of the famous mark, regardless of the presence or absence of actual or likely confusion, of competition, or of actual economic injury. 15 U.S.C. § 1125(c); *see also Glob. Brand Holdings, LLC* v. *Church & Dwight Co.*, 2017 WL 6515419, at *1–2 (S.D.N.Y. Dec. 19, 2017) ("a 'trademark dilution' claim does not require a plaintiff to demonstrate likelihood of confusion between the two marks . . . [the mark's] 'fame is the key ingredient'") (quoting *Savin Corp*. v. *Savin Grp*., 391 F.3d 439, 449 (2d Cir. 2004)).

Section 32(1) of the Lanham Act prohibits the use of a reproduction, counterfeit, copy, or "colorable imitation" of a registered mark in connection with the distribution of goods and services where such use is likely to cause confusion or mistake or to deceive. 15 U.S.C. § 1114(1).

Section 43(a) of the Lanham Act prohibits the use of a trademark, any false designation of origin, false designation of fact, or misleading representation of fact which:

> is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person, or . . . in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities.

15 U.S.C. § 1125(a). Microsoft is likely to succeed under each provision.

First, Defendants' conduct constitutes a clear violation of Lanham Act Section 43(c) (15 U.S.C. § 1125(c)) because they use Microsoft's registered trademarks on their Hotmailbox and 1stCAPTCHA Websites (*i.e.*, in commerce) without Microsoft's authorization, Lyons Decl. ¶¶ 30–32, and because Microsoft's asserted marks are "famous and distinctive," *see Microsoft Corp.* v. *Does 1-2*, 2020 WL 13894281, at *7 (E.D. Va. Nov. 20, 2020) (Microsoft's "Hotmail®" and "Outlook®" trademarks are "famous and distinctive"), *report and recommendation adopted*, 2021 WL 12124650 (E.D. Va. Apr. 5, 2021).[5] Although Defendants' misuse of Microsoft's registered trademarks may not necessarily cause "confusion, mistake, or misrepresentation"—as the

[5] "To be considered famous, a mark must be widely recognized by the general consuming public of the United States." *Adidas Am., Inc.* v. *Thom Browne Inc.*, 599 F. Supp. 3d 151, 161 (S.D.N.Y. 2022) (internal citations and quotations omitted) (finding fame of mark sufficiently pled when complaint included "numerous examples of media coverage identifying the [mark's] global fame as well as examples of its ubiquity"). The factors a court may consider in determining whether a mark is famous all support the conclusion that each of the registered trademarks at issue is famous: (1) duration, extent, and geographic reach of mark's advertising and publicity; (2) amount, volume, and geographic extent of sales of goods and services offered under the mark; (3) extent of actual recognition of the mark; and (4) whether the mark is registered. *See* 15 U.S.C. § 1125(c)(2)(A).

cybercriminals visiting Defendants' Websites presumably know that the services offered are illicit and not sanctioned by Microsoft—Microsoft nonetheless has a valid trademark dilution claim under 15 U.S.C. § 1125(c). *See Bd. of Managers of Soho Int'l Arts Condo.* v. *City of N.Y.*, 2003 WL 21403333, at *18 (S.D.N.Y. June 17, 2003) ("'[D]ilution' under the Lanham Act does not require . . . [a] likelihood of confusion, mistake, or misrepresentation . . . The owner need only demonstrate that another has used the trademark in commerce.").

Second, Defendants' conduct also violates Lanham Act Sections 32(1) and 43(a) (15 U.S.C. §§ 1114(1) and 15 U.S.C. § 1125(a)) on the ground that such conduct has caused "initial-interest confusion" and "post-sale confusion." *Coty Inc.* v. *Excell Brands, LLC*, 277 F. Supp. 3d 425, 441, 458 (S.D.N.Y. 2017) (finding that plaintiff established likelihood of success on the merits as to its claims under the Lanham Act Sections 32(1) and 43(a) and noting that, "in addition to confusion arising at the point of sale, courts recognize, and [plaintiff] alleges, two other types of confusion: initial-interest and post-sale confusion"). Initial-interest confusion, on the one hand, occurs "when a consumer, seeking a particular trademark holder's product, is instead lured away to the product of a competitor because of the competitor's use of a similar mark, even though the consumer is not actually confused about the source of the products or services at the time of actual purchase." *1-800 Contacts, Inc.* v. *WhenU.com*, 309 F. Supp. 2d 467, 491 (S.D.N.Y. 2003), *rev'd and remanded on other grounds*, 414 F.3d 400 (2d Cir. 2005). Post-sale confusion, on the other hand, may occur "among non-purchasers" and may "aris[e] from use of a mark outside of a retail environment after any sale or purchase of a product has concluded." *Id.*

Initial-Interest Confusion: Here, Defendants, by using near-identical versions of Microsoft's registered trademarks, Lyons Decl. ¶¶ 30–32, may cause consumers seeking legitimate Microsoft accounts to accidentally arrive on Defendants' Websites. *See, e.g.*, *Coty Inc.*, 277 F.

Supp. 3d at 441–42; *Planned Parenthood Fed'n of Am., Inc.* v. *Bucci*, 1997 WL 133313, at *12 (S.D.N.Y. Mar. 24, 1997) (Defendant's use of a domain name and home page address similar to plaintiff's mark "on their face, causes confusion among Internet users and may cause Internet users who seek plaintiff's web site to expend time and energy accessing defendant's web site."), *aff'd*, 152 F.3d 920 (2d Cir. 1998); *N.Y. State Soc'y of Certified Pub. Accts.* v. *Eric Louis Assocs., Inc.*, 79 F. Supp. 2d 331, 342 (S.D.N.Y. 1999) (use by defendant of a domain name and metatag similar to plaintiff's common-law service mark "caused a likelihood of confusion because it created initial interest confusion"); *Bihari* v. *Gross*, 119 F. Supp. 2d 309, 319 (S.D.N.Y. 2000) ("In the cyberspace context, the concern is that potential customers of one website will be diverted and distracted to a competing website. The harm is that the potential customer believes that the competing website is associated with the website the customer was originally searching for and will not resume searching for the original website."); *BigStar Ent., Inc.* v. *Next Big Star, Inc.*, 105 F. Supp. 2d 185, 207 (S.D.N.Y. 2000) ("The concern is that many of those initially interested potential customers of plaintiff's would be diverted and distracted by defendants' site and would either believe that defendants' site is associated with plaintiff's or would not return to plaintiff's domain.").

Post-Sale Confusion: Here, Defendants sell fraudulent Microsoft accounts to cybercriminals who in turn use them to conduct phishing scams, deploy cyberattacks, and engage in other unlawful conduct. *See* Mason Decl. ¶¶ 25–29. Cybercriminals may therefore use Microsoft's Outlook word mark in a context "among non-purchasers" and "outside of a retail environment," and thus in a manner that causes post-sale confusion. *See 1-800 Contacts, Inc.*, 309 F. Supp. 2d at 491. For example, after a cybercriminal purchases a fraudulent Microsoft Outlook account from the Defendants, the cybercriminal may send emails containing ransomware-infected attachments to unwitting victims, who are lulled into opening the attachments by the fact that they were transmitted by a seemingly legitimate Microsoft email account bearing the Outlook word mark.

Third, Defendants' violations of the Lanham Act, as set forth above, entitle Microsoft to (i) disgorgement of Defendants' profits and (ii) treble damages. *See* 15 U.S.C. § 1117(a)–(b).

Microsoft is entitled to disgorgement because it has demonstrated Defendants' violation of 15 U.S.C. § 1125(a), as well as Defendants' *willful* violation of 15 U.S.C. § 1125(c). *See id.* § 1117(a) (A plaintiff that "establishe[s]" a "violation under section 1125(a)," or "a willful violation under section 1125(c) . . . shall be entitled . . . to recover (1) defendant's profits, (2) any damages sustained by the plaintiff, and (3) the costs of the action."); *id.* § 1117(b) ("In assessing damages for any violation of section 1114(1)(a) . . . , the court shall, unless the court finds extenuating circumstances, enter judgment for three times such profits or damages . . . ."); *see also Romag Fasteners, Inc.* v. *Fossil, Inc.*, 140 S. Ct. 1492, 1495, 1497 (2020) (recognizing that disgorgement under Lanham Act is available where defendant infringes trademark or where defendant *willfully* dilutes trademark). Here, the circumstances weigh strongly in favor of awarding Defendants' profits to Microsoft. Defendants plainly misuse Microsoft's trademarks in a willful manner, their resulting gains are unquestionably ill-gotten, and their unjust enrichment has caused Microsoft and its users significant financial and reputational harm. The disgorgement of profits attributable to Defendants' infringing scheme is also necessary to deter future violations.

Microsoft is also entitled to treble damages under 15 U.S.C. § 1117(b) because Defendants were fully aware that they were without the right or authority to use Microsoft's trademarks in order to sell the illicit products they offered on the Hotmailbox and 1stCAPTCHA Websites. *See* 15 U.S.C. § 1117(b) (treble damages appropriate where defendant "*intentionally* us[es] a mark or designation, *knowing* such mark or designation is a counterfeit mark . . . , in connection with the sale, offering for sale, or distribution of goods or services") (emphasis added); *Chanel, Inc.* v. *Veronique Idea Corp.*, 795 F. Supp. 2d 262, 271 (S.D.N.Y. 2011) (recognizing plaintiff's entitlement to treble damages when "no rational jury could fail to find that Defendants intentionally purchased and sold jewelry products bearing [plaintiff's mark] at issue *with full knowledge* that they were without the right or authority to do so") (emphasis added). Moreover, an award of treble damages would serve to prevent further infringement by Defendants. *See Victorinox AG* v. *The B & F Sys., Inc.*, 2015 WL 9256944, at *3 (S.D.N.Y. Dec. 15, 2015) (awarding treble damages to deter future misconduct and as a "fair approach" to the "difficult task" of quantifying the extent of confusion and tarnishment), *aff'd*, 709 F. App'x 44 (2d Cir. 2017), *as amended* (2d Cir. Oct. 4, 2017).

c) Plaintiff Is Likely to Succeed on Its Tortious Interference Claim

Under New York law, a claim for tortious interference requires that (1) the plaintiff had business relations with a third party; (2) the defendant interfered with those business relations; (3) the defendant acted for a wrongful purpose or used dishonest, unfair, or improper means; and (4) the defendant's acts injured the relationship. *Catskill Dev., L.L.C.* v. *Park Place Ent. Corp.*, 547 F.3d 115, 132 (2d Cir. 2008). With respect to the third element, a defendant's "commission of a 'crime or an independent tort' clearly constitutes wrongful means." *Id.* (quoting *Carvel Corp.* v. *Noonan*, 3 N.Y.3d 182, 189 (2004)).

Here, Defendants acted for a wrongful purpose and through dishonest, unfair, and improper means, to interfere with and cause damage to Microsoft's business relationships, not only with its end-user customers, but also with key corporate partners. Cambric Decl. ¶¶ 5, 19–22; *see also Google LLC* v. *Starovikov*, 2021 WL 6754263, at *2–3 (S.D.N.Y. Dec. 16, 2021) (finding likelihood of success on Google's tortious interference with business relationships claim where cybercriminal defendants, among other wrongful conduct, "injur[ed] Google's goodwill").

d) **Plaintiff Is Likely to Succeed on Its Conversion Claim**

Under New York law, a claim for conversion requires that (1) plaintiff's property subject to conversion is a specific identifiable thing; (2) plaintiff had ownership, possession, or control over the property before its conversion; and (3) defendant exercised an unauthorized dominion over the thing in question, to the alteration of its condition or to the exclusion of the plaintiff's rights. *Moses* v. *Martin*, 360 F. Supp. 2d 533, 541 (S.D.N.Y. 2004); *see also Thyroff* v. *Nationwide Mut. Ins. Co.*, 8 N.Y.3d 283, 284, 288–89 (2007) (conversion applies to electronic computer records and data).

In this case, Defendants interfered with and converted Microsoft's account-creation systems. Defendants deceived Microsoft's CAPTCHA defense systems, infiltrated those systems, and then stole valuable information therefrom which Defendants used to create and sell fraudulent accounts and tokens for subsequent use by criminals for cybercrime activity and other unlawful ends. *See* Mason Decl. ¶¶ 3, 5, 9–17, 25–29; Cambric Decl. ¶¶ 5–6, 15, 17, 19; Stangl Decl. ¶¶ 10–11; Boffa Decl. ¶¶ 3, 5, 8–13; Lyons Decl. ¶¶ 4, 12–15, 19–24. Accordingly, Microsoft, will succeed on its conversion claim.

e) **Plaintiff Is Likely to Succeed on Its Trespass to Chattels Claim**

Under New York law, a claim for trespass to chattels requires that (1) defendants acted with intent, (2) to physically interfere with plaintiff's lawful possession, and (3) harm resulted. *Rekor Sys., Inc.* v. *Loughlin*, 2022 WL 789157, at *13 (S.D.N.Y. Mar. 14, 2022); *Register.com, Inc.* v. *Verio, Inc.*, 356 F.3d 393, 404 (2d Cir. 2004) ("A trespass to a chattel may be committed by intentionally . . . using or intermeddling with a chattel in the possession of another, where the chattel is impaired as to its condition, quality, or value.") (alteration in original) (internal quotations and citations omitted).

Defendants have interfered with and taken as their own Plaintiff's resources, particularly the "tokens" procured from the CAPTCHA challenges employed by Microsoft. These activities injure the value of Plaintiff's property and constitute a trespass. Defendants' deception of Microsoft's CAPTCHA defense systems, followed by Defendants' infiltration of those systems and stealing of valuable CAPTCHA-defeating tokens (for subsequent use by criminals to deploy cyberattacks and for other unlawful ends), constitute trespass without permission of Microsoft's systems and property, leading to substantial harm. Cambric ¶¶ 5, 7, 20; Boffa Decl. ¶¶ 17–18.

f) <u>Plaintiff Is Likely to Succeed on Its Unjust Enrichment Claim</u>

Under New York law, a claim for unjust enrichment requires that (1) defendant benefitted, (2) at plaintiff's expense, and (3) equity and good conscience require restitution. *Beth Israel Med. Ctr.* v. *Horizon Blue Cross & Blue Shield of N.J., Inc.*, 448 F.3d 573, 586 (2d Cir. 2008). Defendants have clearly benefitted at Microsoft's expense by infiltrating Microsoft's systems, stealing the data necessary to create fraudulent Microsoft accounts, and then selling those fraudulent accounts (along with CAPTCHA tokens) to cybercriminals for them to wreak havoc on Microsoft and its customers. Defendants have profited from their unlawful selling of fraudulent Microsoft accounts to the tune of roughly $3 million. Boffa Decl. ¶ 17.

Unjust enrichment "contemplates an obligation imposed by equity to prevent injustice," *Cooper* v. *Anheuser-Busch, LLC*, 553 F. Supp. 3d 83, 115 (S.D.N.Y. 2021) (internal quotations and citations omitted), and prohibiting Defendants from profiting from their crimes would do just that. Courts have found a likelihood of success on the merits of unjust enrichment claims in similar circumstances. *See, e.g.*, *Starovikov*, 2021 WL 6754263, at *3 (finding that Google demonstrated likelihood of success on its unjust enrichment claim against cybercriminals); *Ex Parte* Temporary Restraining Order, Seizure Order and Order to Show Cause Re Preliminary Injunction at 3, *Microsoft Corp.* v. *John Does 1-2*, No. 1:23-cv-02447 (E.D.N.Y. Mar. 31, 2023) (Morrison, J.), ECF No. 13 (finding that Microsoft demonstrated likelihood of success on its claim for unjust enrichment against cybercriminals); *Ex Parte* Temporary Restraining Order, Seizure Order and Order to Show Cause Re Preliminary Injunction at 2, *Microsoft Corp.* v. *John Does 1-5.*, No. 1:15-cv-6565 (E.D.N.Y. Nov. 23, 2015), ECF No. 12 (same); *Ex Parte* Temporary Restraining Order, Seizure Order and Order to Show Cause Re Preliminary Injunction at 3, *Microsoft Corp.* v. *John Does 1-39*, No. 1:12-cv-1335 (E.D.N.Y. Mar. 19, 2012) (Kuntz, J.), ECF No. 13 (same). Accordingly, Plaintiff is likely to succeed on the merits of its claim for unjust enrichment.

2. **<u>Defendants' Conduct Has Caused Irreparable Harm</u>**

Microsoft has suffered a "reduc[tion]" in "reputational value and goodwill," which "constitutes the irreparable harm that is requisite to the issuance of the preliminary injunction." *See Church of Scientology Int'l* v. *Elmira Mission of the Church of Scientology*, 794 F.2d 38, 44 (2d Cir. 1986); *see also Register.com, Inc.*, 356 F.3d at 404 ("[Defendant's] actions would cause [plaintiff] irreparable harm through loss of reputation, good will, and business opportunities."); *Tom Doherty Assocs., Inc.* v. *Saban Ent., Inc.*, 60 F.3d 27, 38 (2d Cir. 1995) ("a loss of prospective goodwill can constitute irreparable harm"); *Broker Genius, Inc.* v. *Volpone*, 313 F. Supp. 3d 484, 496 (S.D.N.Y. 2018) (same); *Starovikov*, 2021 WL 6754263, at *2 (finding irreparable harm where defendants' conduct "infring[ed] Google's trademarks, injur[ed] Google's goodwill, and damag[ed] its reputation"); *O.D.F. Optronics Ltd.* v. *Remington Arms Co.*, 2008 WL 4410130, at *8 (S.D.N.Y. Sept. 26, 2008) ("harm to [plaintiff's] goodwill and loss of customer relationships" sufficed for requisite showing of "irreparable harm"); *see also Engine Cap. Mgmt., LP* v. *Engine*

No. 1 GP LLC, 2021 WL 1372658, at *12 (S.D.N.Y. Apr. 12, 2021) ("a rebuttable presumption of irreparable harm arises if a plaintiff demonstrates a likelihood of success on the merits" of its Lanham Act claim) (citing 15 U.S.C. § 1116(a)), *appeal withdrawn*, 2021 WL 5831085 (2d Cir. Aug. 17, 2021).

Here, notwithstanding Microsoft's best efforts at protecting itself and its customers, Defendants have caused tens of millions of dollars in damage to Microsoft and have irreparably harmed its reputation, goodwill, and critical customer relationships. *See* Cambric Decl. ¶¶ 5, 7, 20; Boffa Decl. ¶¶ 17–18. Defendants' ongoing fraudulent scheme presents a continuing threat to Microsoft, its customers, and the public, all of whom have suffered and will continue to suffer irreparable harm at the hands of the Defendants' Enterprise absent injunctive and other relief to disrupt the criminal scheme. *See* Cambric Decl. ¶ 22; Lyons Decl. ¶ 35.

This harm is irreparable, moreover, because Microsoft is unlikely to ever be compensated—even after final judgment—due to the fact that Defendants are elusive cybercriminals who will seek to evade the enforcement of any award. *See CRP/Extell Parcel I, L.P.* v. *Cuomo*, 394 F. App'x 779, 781 (2d Cir. 2010) ("[W]e have held that a finding of irreparable harm may lie in connection with an action for money damages where the claim involves an obligation owed by an insolvent or a party on the brink of insolvency.") (citing *Brenntag Int'l Chems. Inc.* v. *Bank of India*, 175 F.3d 245, 249–50 (2d Cir. 1999)); *see also id.* at 782 (irreparable harm exists where "there is a substantial chance that upon final resolution of the action the parties cannot be returned to the positions they previously occupied") (quoting *Brenntag Int'l Chems. Inc.*, 175 F.3d at 249–50).

3. **The Balance of Equities Tips Decidedly in Plaintiff's Favor**

The balance of equities decidedly tips in Microsoft's favor because Defendants will suffer no harm to any legitimate interest if this Court issues a temporary restraining order and preliminary injunction. There is simply no reason (in equity or otherwise) why Defendants should be permitted to continue engaging in an illegal scheme to injure Microsoft, its customers, and third parties. *See, e.g.*, *Starovikov*, 2021 WL 6754263, at *2–3 (finding that balance of hardships tipped in plaintiff Google's favor, that there was "no legitimate reason" why defendants should be able to continue their conduct, and that there was "no countervailing factor weighing against a preliminary injunction," where defendants, a "criminal enterprise," were "infringing Google's trademarks" and "injuring Google's goodwill"); *FTC* v. *Verity Int'l, Ltd.*, 2000 WL 1805688, at *1 (S.D.N.Y. Dec. 8, 2000) (finding that "equities weigh[ed] in favor of" restraining order that would "protect the public from [defendant's] deceptive practice," which likely violated federal law).

4. **The Public Interest Favors an Injunction**

This Court's issuance of an injunction would serve the public interest and is explicitly authorized by RICO and the Lanham Act. Every day that passes, Defendants sell more fraudulently-procured Microsoft accounts to cybercriminals who will then use them for cybercrime activity and other unlawful means. The public interest is clearly served by enforcing statutes designed to protect the public, such as RICO and the Lanham Act. *See, e.g.*, *ProFitness Physical Therapy Ctr.* v. *Pro-Fit Orthopedic & Sports Physical Therapy P.C.*, 314 F.3d 62, 68 (2d Cir. 2002) (acknowledging the "strong interest in preventing public confusion"); *Starovikov*, 2021 WL 6754263, at *4 ("the public interest is clearly served by enforcing statutes designed to protect the public, such as RICO . . . and the Lanham Act"); *Juicy Couture, Inc.* v. *Bella Int'l Ltd.*, 930 F. Supp. 2d 489, 505 (S.D.N.Y. 2013) (issuing preliminary injunction in connection with Lanham

Act claim and finding that the "public interest would not be disserved," where plaintiff established that defendants' actions were "likely to cause consumer confusion").

Numerous courts have granted injunctive relief targeted at disabling malicious cybercrime infrastructures. *See, e.g.*, *Microsoft Corp.* v. *John Does 1-2*, No. 1:23-cv-02447 (E.D.N.Y. Mar. 31, 2023) (Morrison, J.), ECF No. 13; *Microsoft Corp.* v. *Malikov*, No. 1:22-cv-01328 (N.D. Ga. Apr. 8, 2022) (Cohen, J.), ECF No. 27; *Microsoft Corp.* v. *John Does 1-5*, No. 1:15-cv-6565 (E.D.N.Y. Dec. 8, 2015) (Gleeson, J.), ECF No. 18; *Microsoft Corp.* v. *Peng Yong*, No. 1:12-cv-1004 (E.D. Va. Sept. 10, 2012) (Lee, J.), ECF No. 21; *Microsoft Corp. et al.* v. *John Does 1-39*, No. 1:12-cv-1335 (E.D.N.Y. Mar. 29, 2012) (Johnson, J.), ECF No. 22; *Microsoft Corp.* v. *Piatti*, No. 1:11-cv-1017 (E.D. Va. Sept. 22, 2011) (Cacheris, J.), ECF No. 14; *Microsoft Corp.* v. *John Does 1-11*, No. 2:11-cv-00222 (W.D. Wash. Mar. 9, 2011) (Robart, J.), ECF No. 19; *Microsoft Corp.* v. *John Does 1-27*, No. 1:10-cv-156 (E.D. Va. Feb. 22, 2010) (Brinkema, J.), ECF No. 13; *Starovikov*, 2021 WL 6754263; *FTC* v. *Pricewert LLC*, No. 5:09-cv-2407 (N.D. Cal. June 2, 2009) (Whyte, J.), ECF No. 12. The same result is warranted here.

In the foregoing cases, each involving claims similar to those presented here, the courts granted as a remedy the transfer of malicious domains to the control of the plaintiff(s), and away from the control of defendant(s). Such relief is appropriate and necessary, within the Court's broad equitable authority to craft remedies to prevent irreparable harm, and is not prohibited by any statute or rule of law.

Federal courts have very broad, inherent equitable authority to craft injunctions for any civil violation of law—especially in cases involving violations of RICO and the Lanham Act. Indeed, RICO contemplates broadly that district courts

> shall have jurisdiction to prevent and restrain violations of section 1962 . . . by issuing appropriate orders, including, but not limited to: ordering any person to

> divest himself of any interest, direct or indirect, in any enterprise; imposing reasonable restrictions on the future activities or investments of any person, including, but not limited to, prohibiting any person from engaging in the same type of endeavor as the enterprise engaged in, the activities of which affect interstate or foreign commerce; or ordering dissolution or reorganization of any enterprise, making due provision for the rights of innocent persons.

18 U.S.C. § 1964(a); *see Chevron Corp.* v. *Donziger*, 833 F.3d 74, 137 (2d Cir. 2016) ("[A] federal court is authorized to grant equitable relief to a private plaintiff who has proven injury to its business or property by reason of a defendant's violation of § 1962[.]"). Likewise, the Lanham Act contemplates that district courts "shall have power to grant injunctions, according to the principles of equity and upon such terms as the court may deem reasonable, to prevent the violation of any right of the registrant of a mark registered in the Patent and Trademark Office or to prevent a violation under subsection (a), (c), or (d) of section 1125 of this title." 15 U.S.C. § 1116(a); *see Coty Inc.*, 277 F. Supp. 3d at 465 ("courts may grant injunctions 'according to the principles of equity and upon such terms as the court may deem reasonable'") (quoting 15 U.S.C. § 1116(a)). *See also Weinberger* v. *Romero-Barcelo*, 456 U.S. 305, 313 (1982) ("Unless a statute in so many words, or by a necessary and inescapable inference, restricts the court's jurisdiction in equity, the full scope of that jurisdiction is to be recognized and applied.") (quoting *Porter* v. *Warner Holding Co.*, 328 U.S. 395, 398 (1946)); *Federal Marine Terminals, Inc.* v. *Burnside Shipping Co.*, 394 U.S. 404, 412 (1969) ("[T]he legislative grant of a new right does not ordinarily cut off or preclude other nonstatutory rights in the absence of clear language to that effect.").

This language evinces a Congressional intent to afford broad remedies, and federal courts have taken that view in prior cybercrime matters brought by Microsoft. Orders to disable Defendants' cybercrime infrastructure would be squarely within the Court's broad equitable authority.

5. **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 would direct that the third-party domain registries and service providers, through which Defendants operate their Fraudulent Enterprise, reasonably cooperate to effectuate this order. Specifically, the Proposed Order provides that the domains listed in Appendix A be disabled or transferred to Plaintiff's control, in order to mitigate the risk and injury caused by Defendants. These third parties are the only entities that can effectively disable Defendants' domains, disable Defendants' malicious software at those domains, and preserve the evidence. Consequently, their cooperation is necessary.

Plaintiff requests this relief under the All Writs Act ("AWA"), which 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 the AWA can extend to third parties necessary to affect the implementation of a court order:

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

United States v. *N.Y. Tel. Co.*, 434 U.S. 159, 174 (1977) (citations omitted); *see also id.* at 176 (holding order to telephone company to assist in implementation of a pen register warrant was authorized under the All Writs Act).

There are two steps to any analysis of the AWA as applied to third parties. First, there are three threshold requirements: (1) issuance of the writ must be "in aid of" the issuing court's jurisdiction, (2) the type of writ requested must be "necessary or appropriate" to provide such aid to the issuing court's jurisdiction, and (3) the issuance of the writ must be "agreeable to the usages and principles of law." *See United States* v. *Amante*, 418 F.3d 220, 222 (2d Cir. 2005); *Yonkers*

Racing Corp. v. *City of Yonkers*, 858 F.2d 855, 863 (2d Cir. 1988); 28 U.S.C. § 1651. If these threshold requirements are met, *New York Telephone* directs courts, in their discretion, to consider three requirements for third-party writs: (1) "the closeness of [the third party's] relationship to the underlying criminal conduct and government investigation"; (2) "the burden the requested order would impose on [the third party]"; and (3) "the necessity of imposing such a burden on [the third party]." *In re Apple, Inc.*, 149 F. Supp. 3d 341, 344, 351 (E.D.N.Y. 2016); *see also N.Y. Tel. Co.*, 434 U.S. at 174–78.

Plaintiff has plainly met the threshold factors. First, this action was commenced under multiple federal statutes—the Lanham Act and RICO—meaning that the Court "unquestionably has subject matter jurisdiction over this action pursuant to 28 U.S.C. Section 1331, and, therefore, has jurisdiction to issue the requested [AWA] Order." *United Spinal Ass'n* v. *Bd. of Elections in City of N.Y.*, 2017 WL 8683672, at *5 (S.D.N.Y. Oct. 11, 2017), *report and recommendation adopted*, 2018 WL 1582231 (S.D.N.Y. Mar. 27, 2018). This Court's utilization of the AWA is also "necessary or appropriate" here. As the Supreme Court stated in *New York Telephone*, "[u]nless appropriately confined by Congress, a federal court may avail itself of all auxiliary writs as aids in the performance of its duties." 434 U.S. at 172–73. The requested writ is necessary here given the structure of Defendants' Fraudulent Enterprise, which exploits the infrastructure and businesses of third parties such as domain registries and registrars. *See In re Apple, Inc.*, 149 F. Supp. 3d at 352 (recognizing the order was necessary and appropriate in a cell phone decryption case).

Plaintiff's Proposed Order also comports with appropriate principles of law. When the first two requirements are met, the All Writs Act empowers the court "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." *U.S. Commodity Futures Trading Comm'n* v. *Amaranth Advisors, LLC*, 523 F. Supp. 2d 328, 335 (S.D.N.Y. 2007) (quoting *In re Baldwin-United Corp.*, 770 F.2d 328, 338 (2d Cir. 1985)). In this case, where Defendants constantly "recycle and mask IP addresses"—*i.e.*, in order to avoid detection, Defendants constantly change the IP addresses from which the fraudulent accounts are logging into Microsoft's systems (Lyons Decl. ¶¶ 28–29)—an order that enjoins Defendants but does not direct the domain registries under the AWA will leave Microsoft, and then this Court, playing a game of "whack-a-mole." *See, e.g.*, *Arista Records, LLC* v. *Tkach*, 122 F. Supp. 3d 32, 34 (S.D.N.Y. 2015) (noting that, in a domain name seizure case, "Plaintiffs explain that they were then drawn into what they describe as a technological globetrotting game of 'whack-a-mole' in an effort to enforce the TRO"). Because of the resilient nature of Defendants' Fraudulent Enterprise, *see* Cambric Decl. ¶ 17; Boffa Decl. ¶ 9, any partial disruption will have little to no effect as Defendants will maintain the ability to reassert control. In other words, this Court's decision will not be fully enforced.

The third parties named in the Proposed Order are also each completely necessary for an effective permanent injunction. Absent a complete disabling of Defendants' malicious software and a transfer of the relevant domains away from their control, Defendants will be able simply to shift their infrastructure to new IP addresses and domains. The AWA was enacted for precisely this sort of case. *See In re Application of United States for an Order Authorizing an In-Progress Trace of Wire*, 616 F.2d 1122, 1129 (9th Cir. 1980) ("[T]he Court [in *New York Telephone*] 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.'") (alteration in original) (quoting *N.Y. Tel. Co.*, 434 U.S. at 175); *In re Baldwin-United Corp.*, 770 F.2d at 338 ("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."); *see also Dell, Inc.* v. *Belgiumdomains, LLC*, 2007 WL 6862341, at *4–6 (S.D. Fla. Nov. 21, 2007) (applying All Writs Act in conjunction with trademark seizure under Rule 65 and Lanham Act and directing third party VeriSign, Inc. to take actions on certain domain names); *In re Baldwin-United Corp.*, 770 F.2d at 339 ("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.").

In sum, requiring these third parties to reasonably assist in the execution of this order will not offend due process, as the Proposed Order (1) requires only minimal assistance from the third parties in executing the order (acts that they would take in the ordinary course of their operations), (2) requires that it be implemented with the least degree of interference with the normal operation of the third parties, and (3) does not deprive the third parties of any tangible or significant property interests.[6] If, in the implementation of the Proposed Order, any third party wishes to bring an issue to the attention of the Court, Plaintiff will bring it immediately. The third 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). Accordingly, the directions to the third parties in the Proposed Order are narrow, satisfy due process, and are necessary to effect the requested relief and ensure that the relief is not rendered fruitless.

6. An *Ex Parte* TRO and Preliminary Injunction Is the Only Effective Means of Relief, and Alternative Service Is Warranted Under the Circumstances

The Temporary Restraining Order that Microsoft requests must issue *ex parte* for the relief to be effective given the extraordinary factual circumstances here—namely, Defendants' technical

[6] Microsoft will work with the providers identified in the Proposed Order to deploy technology designed to ensure no third party is deprived of any property interest.

sophistication and ability to move their malicious infrastructure if they are given any advance notice of this action. Rule 65 of the Federal Rules of Civil Procedure permits an *ex parte* temporary restraining order where, as here, the moving party sets forth facts showing an immediate and irreparable injury and why notice should not be required. *See* Fed. R. Civ. P. 65(b)(1); *see also In re Vuitton et Fils S.A.*, 606 F.2d 1, 4 (2d Cir. 1979) ("Ex parte temporary restraining orders are no doubt necessary in certain circumstances . . .") (quoting *Granny Goose Foods, Inc.* v. *Brotherhood of Teamsters & Auto Truck Drivers, Local No. 70*, 415 U.S. 423, 439 (1974)).

If notice is given prior to issuance of a Temporary Restraining Order, Defendants will likely be able to quickly mount an alternate infrastructure for their Fraudulent Enterprise. Lyons Decl. ¶ 33. Thus, providing notice of the requested Temporary Restraining Order will undoubtedly facilitate efforts by Defendants to defend their operations. It is well established that *ex parte* relief is appropriate under the circumstances present here, where notice would render the requested relief ineffective. *See, e.g.*, *In re Vuitton et Fils S.A.*, 606 F.2d at 4–5 (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 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").

Moreover, where (as here) there is evidence that operators of cybercrime infrastructure will attempt to evade enforcement attempts if they have notice, *ex parte* relief is particularly appropriate. *See, e.g., Microsoft Corp.* v. *John Does 1-2*, No. 1:23-cv-02447 (E.D.N.Y. Mar. 31, 2023), ECF No. 13; *Microsoft Corp.* v. *Peng Yong*, No. 1:12-cv-1004 (E.D. Va. Sept. 10, 2012), ECF No. 21; *Microsoft Corp.* v. *Piatti*, No. 1:11-cv-1017 (E.D. Va. Sept. 22, 2011), ECF No. 14; *Microsoft Corp.* v. *John Does 1-27*, No. 1:10-cv-156 (E.D. Va. Feb. 22, 2010), ECF No. 13. In each of these cases, courts issued *ex parte* TROs to disable cybercrime infrastructure, recognizing the risk that Defendants would move the infrastructure and destroy evidence if prior notice were given.

To ensure due process, immediately upon entry of the requested *ex parte* Temporary Restraining Order, Plaintiff will undertake all reasonable efforts to effect formal and informal notice of the preliminary injunction hearing to Defendants and to serve the Complaint and all other papers. Specifically:

Plaintiff Will Provide Notice by Email, Facsimile and/or Mail: Microsoft has identified or will identify email addresses, mailing addresses, and/or facsimile numbers provided by the Defendants, and will further identify such contact information pursuant to the terms of the requested Temporary Restraining Order. *See* Rozbruch Decl. ¶¶ 11–15. Plaintiff will provide notice of the preliminary injunction hearing and will effect service of the Complaint by immediately sending the same pleadings described above to the email addresses provided to the hosting companies, registrars, and registries, and to any other email addresses, facsimile numbers, and mailing addresses that can be identified. *Id.* Based on Microsoft's investigation, it appears that the most effective means of contacting the Defendants are the email addresses used to register the domains at issue or to otherwise carry out their activities. *Id.* ¶ 10. Notably, when Defendants registered for the domain names of their websites, they agreed not to engage in abusive activities and to accept notice of hosting-related disputes through the email, facsimile, and mail addresses provided by them. *Id.* ¶¶ 21–32.

Plaintiff Will Provide Notice to Defendants by Publication: Plaintiff will notify the Defendants of the preliminary injunction hearing and the Complaint against their misconduct by publishing the materials on a centrally located, publicly accessible source on the Internet for a period of 6 months. *Id.* ¶ 12.

Plaintiff Will Provide Notice to Defendants by Personal Delivery: Plaintiff has identified domain names from which Defendants' infrastructure operates, and, pursuant to the requested Temporary Restraining Order, will obtain from the domain registrars any and all physical addresses of the Defendants. Microsoft will also attempt to serve by hand, pursuant to Federal Rules of Civil Procedure 4(e)(2)(A) and 4(f)(3), the formal notice of the preliminary injunction hearing, the Complaint, the instant motion and supporting documents, as well as any Order issued by this Court to any United States addresses, to the extent any are identified. *Id.* ¶ 14.

Plaintiff Will Provide Notice by Personal Delivery and Treaty If Possible: If valid physical addresses of Defendants can be identified, Microsoft will notify Defendants and serve process upon them by personal delivery, or through the Hague Convention on service of process or similar treaty-based means, to the extent available. *See id.* ¶ 14.

Notice and service by the foregoing means satisfy due process; are appropriate, sufficient, and reasonable to apprise Defendants of this action; and are necessary under the circumstances.

Legal notice and service by email, facsimile, mail, and publication satisfies due process as these means are reasonably calculated, in light of the circumstances, to apprise the interested parties of the requested Temporary Restraining Order, the preliminary injunction hearing, and the lawsuit. *See Mullane* v. *Cent. Hanover Bank & Tr. Co.*, 339 U.S. 306, 314 (1950). Such methods are also authorized under Federal Rule of Civil Procedure 4(f)(3), which allows a party to serve defendants by means not prohibited by international agreement.

Moreover, Plaintiff's proposed methods of notice and service have been approved in other cases involving international defendants attempting to evade authorities. *See, e.g.*, *Rio Props., Inc.* v. *Rio Int'l Interlink*, 284 F.3d 1007, 1013–18 (9th Cir. 2002) (authorizing service by email on international defendant); *Payne* v. *McGettigan's Mgmt. Servs. LLC*, 2019 WL 6647804, at *1–2 (S.D.N.Y. Nov. 19, 2019) (noting that courts have found various alternative methods of service appropriate and authorizing service via email on foreign defendant); *Elsevier, Inc.* v. *Siew Yee Chew*, 287 F. Supp. 3d 374, 379–80 (S.D.N.Y. 2018) (finding, in trademark infringement action, that service on foreign defendants via email satisfied constitutional standards of due process); *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ¶ 7, *Microsoft Corp.* v. *John Does 1-27*, No. 1:10-cv-156 (E.D. Va. Feb. 22, 2010) (Brinkema J.), ECF No. 13 (finding service proper where plaintiff effectuated notice of temporary restraining order and preliminary injunction order, preliminary injunction hearing, and complaint by "personal delivery upon defendants who provided contact information in the U.S."; "personal delivery through the Hague Convention on Service Abroad upon defendants who provided contact information in China"; "transmission by e-mail, facsimile and mail to the contact information provided by defendants to their domain name registrars and as agreed to by defendants in their domain name registration agreements"; and "publishing notice on a publicly available Internet website"); *Microsoft Corp.* v. *Does 1-18*, 2014 WL 1338677, at *3 (E.D. Va. Apr. 2, 2014) (finding service was proper where plaintiff sent "copies of the original Complaint, Russian translations, a link to all pleadings, and the temporary restraining order notice language to all email addresses associated with the Bamital botnet command and control domains" and "published in English and Russian the Complaint, Amended Complaint, Summons, and all orders and pleadings in this action at the publicly available website www.noticeofpleadings.com") (citing Fed. R. Civ. P. 4(f)(3)).

Such service is particularly warranted in cases such as this involving Internet-based misconduct, carried out by international defendants, causing immediate, irreparable harm. As the Ninth Circuit observed:

> [Defendant] had neither an office nor a door; it had only a computer terminal. If any method of communication is reasonably calculated to provide [defendant] with notice, surely it is email—the method of communication which [defendant] utilizes and prefers. In addition, email was the only court-ordered method of service aimed directly and instantly at [Defendant] . . . Indeed, when faced with an international e-business scofflaw, playing hide-and-seek with the federal court, email may be the only means of effecting service of process.

Rio Properties, Inc., 284 F.3d at 1018. Significantly, courts in the Second Circuit have followed *Rio Properties*. *See, e.g.*, *Payne*, 2019 WL 6647804, at *1; *Elsevier, Inc.*, 287 F. Supp. 3d at 379–80.

For all of the foregoing reasons, Plaintiff respectfully requests that this Court enter the requested Temporary Restraining Order and Order to Show Cause why a preliminary injunction should not issue, and further order that the means of notice of the preliminary injunction hearing, the Complaint, the instant motion and supporting documents, as well as any Order issued by this Court, as set forth herein, meet Federal Rule of Civil Procedure 4(f)(3), satisfy due process, and are reasonably calculated to notify Defendants of this action.

III. CONCLUSION

For the reasons set forth herein, Plaintiff respectfully requests that this Court grant its motion for a Temporary Restraining Order and Order to Show Cause regarding why a preliminary injunction should not issue. Plaintiff further respectfully requests that the Court permit notice of the preliminary injunction hearing and above-referenced documents by alternative means.

Dated: December 7, 2023
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