UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

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

COMPLAINT

Plaintiff Microsoft Corporation ("Microsoft"), by and through its attorneys at Cahill Gordon & Reindel LLP, brings this action against Defendants Duong Dinh Tu, Linh Van Nguyen (a/k/a Nguyen Van Linh), and Tai Van Nguyen (collectively, "Defendants"), alleging as follows:

NATURE OF THIS ACTION

1. Microsoft brings this action to halt the Defendants' ongoing scheme to use Internet "bots" to hack into and deceive Microsoft's security systems into believing that they are legitimate human consumers of Microsoft services, open Microsoft Outlook email accounts in names of fictitious users, and sell those fraudulent accounts to cybercriminals for use as tools in perpetrating a wide variety of online crimes. The Defendants have used such criminal tactics to injure not just Microsoft, but numerous other technology companies like X (formerly Twitter) and Google and their customers. Swift judicial intervention is necessary to put an end to the industry-wide destruction being caused by the Defendants' continuing crimes.

2. A bot is a software application that runs automated tasks on the Internet, usually with the intent to imitate human activity (such as messaging), often on a massive scale. By

leveraging their capacity to rapidly perform repetitive tasks, bots can be abused for a wide array of illegal ends, including to spray emails and other communications to disseminate computer viruses, such as "ransomware" used to extort payments from victims, and other types of malicious software ("malware"). Microsoft has spent tens of millions of dollars on security measures to protect legitimate users of Microsoft's services from the harms associated with bots, and to ensure that users of its software, services, and systems are bona fide human consumers.

3. One such protective measure is the use of so-called "CAPTCHA" tests. CAPTCHA stands for "Completely Automated Public Turing test to tell Computers and Humans Apart." The CAPTCHA tests used by Microsoft require every would-be user who wishes to open a Microsoft email account to represent that they are a human being rather than a bot, and verify the accuracy of that representation by solving several puzzles—which, if answered correctly, provide a high level of confidence that the user is, in fact, human.

4. The Defendants are members of a criminal enterprise (hereinafter the "Fraudulent Enterprise" or "Enterprise") that uses lies and deception to breach Microsoft's CAPTCHA and other security measures, procure fraudulent Microsoft Outlook email accounts, and then sell these fraudulent accounts to a roster of cybercriminals. The Defendants and their Enterprise have developed CAPTCHA-defeating software bots which—by fraudulently impersonating millions of individual human computer users, and misrepresenting that they would abide by Microsoft's terms of service with the intent to violate those terms—deceived and bypassed Microsoft's CAPTCHA-fortified security measures. The Defendants' Enterprise sells fraudulent CAPTCHA-defeating software bots targeting not just Microsoft, but also other technology companies (like X and Google). Their fraudulent scheme thus represents a significant industry-wide problem.

5. Since at least 2021, the Defendants have been engaged in a scheme to obtain

millions of Microsoft Outlook email accounts in the names of fictitious users based on a series of false representations, and then sell these fraudulent accounts to malicious actors for use in various types of cybercrime.

6. Upon information and belief, evidence[1] gathered thus far by Microsoft's investigation in this case shows that Microsoft email accounts—which were fraudulently obtained by Defendants and sold to cybercriminals—have been used by organized cybercrime groups known to Microsoft as "Storm-0252," "Storm-0455," and "Octo Tempest" to engage in cybercrime activity, including email phishing[2] scams, which are frequently used as a vehicle for spreading ransomware and other malware. This evidence also shows that Octo Tempest recently committed massive ransomware attacks against flagship Microsoft customers that infected the computer systems of those customers with ransomware which disabled critical operational systems, resulting in service disruptions that inflicted hundreds of millions of dollars of damage.

7. From their criminal scheme, the Defendants and their Enterprise have earned millions of dollars in illicit revenues, caused tens of millions of dollars in damage to Microsoft and its customers, and harmed Microsoft's reputation, goodwill, and critical customer relationships. Unless enjoined and held accountable, Defendants will continue with impunity, wreaking havoc

[1] This evidence includes, among other things, data showing that Autonomous System Numbers ("ASNs") associated with emails used in attacks by Storm-0252, Storm-0455, and Octo Tempest match ASNs associated with accounts sold by Defendants, indicating that these groups have used emails acquired from the Defendants' fraudulent scheme to conduct their cybercriminal activities. An ASN is a unique identifier that is globally available and allows one Internet-connected email server to exchange routing information with other email servers.

[2] As used here, email phishing refers to a type of online scam where a criminal sends an email purporting to be from a legitimate source to lull the recipient of the email into trusting the sender and clicking on an embedded hyperlink or opening an attachment that dispenses malware onto the recipient's computer. The term "phishing" is a spin on the word fishing, because the criminal is dangling a fake "lure" (the seemingly legitimate email) hoping the recipient will "bite" on the malware-infected link or attachment.

on Microsoft, its customers, and the public.

8. Microsoft brings this action to obtain injunctive relief to disrupt the Defendants' ongoing criminal scheme and to recover damages for their (i) violations of the Racketeer Influenced and Corrupt Organizations Act ("RICO"), (ii) infringements of Microsoft's valuable trademarks and other violations of the Lanham Act, (iii) tortious interference with Microsoft's business relationships with its customers, (iv) conversion of Microsoft's property, (v) trespass to Microsoft's chattels, and (vi) unjust enrichment.

PARTIES

9. Plaintiff Microsoft is a corporation duly organized under the laws of the state of Washington, with its headquarters and principal place of business in Redmond, Washington.

10. Defendant Duong Dinh Tu ("Tu") is an individual residing in Vietnam. Upon information and belief, Tu has used and can be contacted at several email accounts, including "duongdinhtu93@gmail.com" and "duongdinhtu93@outlook.com."

11. Defendant Linh Van Nguyen (a/k/a Nguyen Van Linh) ("Linh") is an individual residing in Vietnam. Upon information and belief, Linh has used and can be contacted at several email accounts, including "17021195@vnu.edu.vn" and "nguyenlinh.uet@gmail.com."

12. Defendant Tai Van Nguyen ("Tai") is an individual residing in Vietnam. Upon information and belief, Tai has used and can be contacted at several email accounts, including "nvt.kscntt@gmail.com."

13. As shown herein, Defendants have conspired with at least each other—and possibly others who have not yet been identified by Microsoft—to engage in a pattern of racketeering activity by and through the Fraudulent Enterprise, including by agreeing to commit and perpetrating millions of predicate racketeering acts of wire fraud since in or about 2021. Each of

them has participated in the operation or management of the Fraudulent Enterprise and has engaged in criminal acts causing harm to Microsoft, its customers, and countless others.

14. The Defendants and their Enterprise have perpetrated these crimes in part by abusing technological infrastructure and services provided by third parties, including the computer servers at the Internet domains listed in Appendix A.

15. On information and belief, the actions and omissions alleged herein to have been undertaken by Defendants were actions that they, and each of them, authorized, controlled, directed, or had the ability to authorize, control or direct, or were actions and omissions each Defendant assisted, participated in, or otherwise encouraged, and are actions for which each Defendant is liable. Each Defendant aided and abetted the actions and omissions of his co-Defendants set forth below, in that each Defendant had knowledge of those actions and omissions, provided assistance, and benefited from those actions and omissions, in whole or in part. Each Defendant was the agent of every remaining Defendant, and in doing the things hereinafter alleged, was acting within the course and scope of such agency and with permission and consent of the other Defendants.

JURISDICTION AND VENUE

16. This Court has jurisdiction over Microsoft's federal claims pursuant to 28 U.S.C. § 1331. This Court also has jurisdiction over Microsoft's federal Lanham Act claims under 28 U.S.C. § 1338 and 15 U.S.C. § 1121. This Court has supplemental jurisdiction over Microsoft's remaining state law claims pursuant to 28 U.S.C. § 1367 because those claims are so related to the federal claims asserted in this action that they form part of the same case or controversy under Article III of the United States Constitution.

17. Venue is proper in this Court under 28 U.S.C. § 1391(b) because a substantial part

of the events or omissions giving rise to Microsoft's claims has occurred in the Southern District of New York, because a substantial part of the property that is the subject of Microsoft's claims is situated in the Southern District of New York, and because a substantial part of the harm caused by Defendants has occurred in the Southern District of New York.

18. Venue is also proper in this Court under 28 U.S.C. § 1391(c) because Defendants are subject to personal jurisdiction in the Southern District of New York. Defendants have undertaken the acts alleged herein with knowledge that such acts would cause harm through domains located in and maintained through facilities in the Southern District of New York, and have targeted Microsoft's customers and their networks in the Southern District of New York and elsewhere in the United States, thereby injuring Microsoft, its customers, and the public. Furthermore, and as set forth herein, Defendants have utilized services provided by third parties located in the Southern District of New York, such as payment processors and Internet service providers, in carrying out their unlawful scheme. Therefore, this Court has personal jurisdiction over Defendants.

BACKGROUND

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

19. Microsoft is one of the leading computer technology companies in the world. The company's mission is to provide technology that empowers every person and every organization on the planet to achieve more.

20. Founded in 1975, Microsoft develops and supports market-leading computer software, services, and solutions that help its customers realize their full potential. Microsoft's globally-recognized products include the popular computer operating system Windows; the Microsoft 365 family of business productivity software, including Microsoft's Word processing,

Excel spreadsheet, and PowerPoint presentation software applications; Microsoft's Outlook software for managing email communications, calendaring, and tasks; Microsoft's Teams software for virtual collaboration; Microsoft's Skype instant messaging software; and Microsoft's LinkedIn social media platform for professional networking.

21. Microsoft's products and services are broadly used across the globe. Its customers include individual consumers, federal and state courts, law enforcement agencies, governments, hospitals, private businesses (ranging from small companies to global enterprises), manufacturers, non-profit organizations, and other public-sector institutions.

22. In fiscal year 2023, Microsoft earned over $200 billion in revenue, including billions of dollars from sales of subscriptions that grant licenses allowing Microsoft customers to use its products and services. For example, in recent years, Microsoft has earned revenue from subscriptions and licenses sold to individual and business customers to use Microsoft Office 365's suite of products (including Word, Excel, and Outlook).

23. Microsoft also offers widely-used emails 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 to form customer relationships with Microsoft.

24. Because the rate and pace of cybercrime threats have accelerated in recent years, Microsoft also provides comprehensive cybersecurity solutions powered by artificial intelligence to prevent cyberattacks. In fiscal year 2023, Microsoft's cybersecurity business surpassed $20 billion in annual revenue, which was earned from more than a million customer organizations that utilize Microsoft services to protect their digital estates.

25. Microsoft has invested billions of dollars in developing best-in-class products and services. 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 with its customers, and has built the brand names associated with Microsoft and its products into strong and famous worldwide symbols that are well-recognized within its channels of trade.

26. Microsoft has registered trademarks representing the quality of its products and services and its brand, including Outlook® and Hotmail®. Copies of the trademark registrations for these trademarks are attached as Appendix B to this Complaint.

B. Microsoft's Efforts to Prevent Cybercrime

27. Microsoft invests significant time and monies to deliver services to its customers in a safe and secure fashion, and on generating and sustaining overall consumer trust and confidence in the integrity of the digital economy and Internet. As a result, Microsoft undertakes costly, time-consuming, and labor-intensive efforts to secure its services to help ensure that its customers enjoy a positive, worry-free experience when they use its products. In recent years alone, Microsoft has spent tens of millions of dollars employing top-flight technical, legal, and business experts to prevent, disrupt, and deter cybercrime.

28. The measures that Microsoft takes to protect its customers from cybercrime include the following (among other things):

29. *First*, Microsoft requires everyone who wishes to use Microsoft services to agree that they will abide by a strict code of conduct, including by representing that they: (a) will not use any false, inaccurate, or misleading information when signing up for their 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 fake accounts, or automating inauthentic activity).

30. To use free or paid-subscription versions of Microsoft services, every customer must first sign up for their own personal Microsoft account. In doing so, every customer is required to agree to abide by Microsoft's Services Agreement (available at https://microsoft.com/en-us/servicesagreement) ("MSA"), which specify terms of service and a strict code of conduct aimed at preventing the misuse of Microsoft services for criminal ends.

31. Among the potential illegal uses of Microsoft's services is the malicious use of bots that fraudulently impersonate human users to open Microsoft Outlook email accounts in the names of fictitious individuals. The fraudulent accounts created by these bots are then sold to cybercriminals, who use them to perpetrate computer hacks or spread computer viruses anonymously. As noted, a bot is a software application that runs automated tasks on the Internet, usually with the intent to imitate human activity (such as messaging) on a massive scale. By leveraging their capacity to rapidly perform repetitive tasks, bots have been used to disseminate emails and other communications spreading computer viruses, spam communications, ransomware, and many other types of malware. Microsoft's CAPTCHA defenses help protect against these illicit ends by seeking to ensure that every would-be user who wishes to open a Microsoft email account is a human being rather than a bot.

32. To prevent the use of bots to obtain and abuse Microsoft accounts, Microsoft's Services Agreement provides that by using Microsoft services, each customer represents that they will comply with the following rules (among others):

- "Don't circumvent any restrictions on access to, usage, or availability of the Services" (MSA § 3(a)(vi)).
- "You agree not to use any false, inaccurate or misleading information when

signing up for your Microsoft account" (*id.* § 4(a)(i)).

- "You cannot transfer your Microsoft account credentials to another user or entity" (*id.*).
- "Don't 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)).
- "Don't do anything illegal, or try to generate or share content that is illegal" (*id.* § 3(a)(i)).
- "Don't send spam or engage in phishing, or try to generate or distribute malware" (*id.* § 3(a)(iii)).
- "Don't engage in activity that is harmful to you, the Services, or others" (*id.* § 3(a)(vii)).
- "Don't violate or infringe upon the rights of others" (*id.* § 3(a)(viii)).
- "Don't help others break these rules" (*id.* § 3(a)(x)).

33. *Second*, to deter the use of bots to create Microsoft accounts that could be abused by cybercriminals, Microsoft employs security measures to verify that each user attempting to open or use a Microsoft account is a human being. For example, Microsoft contracts with a leading cybersecurity vendor, namely Arkose Labs, to employ a state-of-the-art CAPTCHA defense service, which serves as a gatekeeper requiring every would-be user who wishes to open a Microsoft account to represent that they are a human being (not a bot), and verify the accuracy of that representation by solving several puzzles—which, if answered correctly, provide a high level of confidence that the user is, in fact, human. The user must then provide identifying information, including their birthday and name, so that Microsoft has additional data on file to confirm they are a real person.

34. *Third*, Microsoft uses a variety of internal tools that leverage artificial intelligence and machine learning to prevent bots and other malicious actors from entering its systems.

Microsoft employs engineers, data scientists, and other investigators to monitor its systems, such as Outlook and Skype, for signs of suspicious behaviors (such as indications of bots opening fraudulent Microsoft accounts in bulk) and suspends Microsoft accounts that are believed with a high degree of certainty to be acting in violation of Microsoft's terms of service.

35. *Fourth*, Microsoft maintains its own Digital Crimes Unit ("DCU"), which is an international team of technical, legal, and business experts—including former federal prosecutors and law enforcement agents—fighting cybercrime, protecting individuals and organizations, and safeguarding the integrity of Microsoft services since 2008. DCU investigators frequently uncover evidence of cybercrime that would not otherwise be detected by law enforcement. In appropriate cases, DCU brings that evidence to the attention of law enforcement for criminal prosecution. DCU also works to increase the operational cost of cybercrime by disrupting the infrastructure used by cybercriminals through civil lawsuits and technical measures.

36. For example, the DCU has, to date, disrupted the infrastructure of roughly 25 botnets—which are networks of malware-infected computers controlled by cybercriminals or nation-state actors—thereby preventing them from distributing additional malware, controlling victims' computers, and targeting additional victims. In partnership with governments and Internet service providers, the DCU has identified and shared information to remediate approximately 500 million botnet victims worldwide.

37. DCU has also invested in technical and legal resources to make ransomware less profitable and more difficult to deploy. Ransomware is a type of malware that encrypts a victim's computer system until a ransom is paid to the ransomware attacker in exchange for the password needed to access the system. In countless cases, DCU has disrupted

infrastructure and payment systems that enable ransomware attacks, preventing the use of Microsoft products and services to attack the company's customers.

THE DEFENDANTS' FRAUDULENT ENTERPRISE AND SCHEME

38. The Defendants are members of the Fraudulent Enterprise, a prolific crime-as-a-service provider. The Defendants and their Enterprise have developed CAPTCHA-defeating software bots which—by fraudulently impersonating millions of individual human computer users, and misrepresenting that they would abide by Microsoft's terms of service with the intent to do the exact opposite—have deceived and bypassed Microsoft's CAPTCHA-fortified security measures.

39. Since at least 2021, the Defendants and their Enterprise have been engaged in a scheme to procure millions of Microsoft Outlook email accounts in the names of fictitious users based on a series of false representations, and then sell these fraudulent accounts to malicious actors for use in various types of cybercrime. As part of the scheme, the Defendants have also sold digital CAPTCHA-solving tokens to cybercriminals allowing them to use their own bots to deceive Microsoft into furnishing fraudulent Microsoft Outlook accounts that the cybercriminals can then abuse for illegal ends.

40. Upon information and belief, evidence gathered to date by Microsoft's investigation in this case shows that Microsoft email accounts, which were fraudulently obtained by Defendants for resale, have been used to perpetrate cybercrime activity, including email phishing scams that were likely used to spread ransomware and other malware, including by the cybercrime groups known to Microsoft as Storm-0252, Storm-0455, and Octo Tempest, the latter of which recently brought ransomware attacks against flagship Microsoft customers. During these attacks, the computer systems of those customers were infected with ransomware that disabled

critical operational systems, resulting in service disruptions that inflicted hundreds of millions of dollars of damage.

41. From their criminal scheme, the Defendants and their Fraudulent Enterprise have earned millions of dollars in illicit revenue, caused tens of millions of dollars in damage to Microsoft and its customers, and irreparably harmed Microsoft's reputation, goodwill, and critical customer relationships. Unless enjoined and held accountable, Defendants will continue their campaign of fraud and destruction on Microsoft and its customers with impunity.

A. Defendants' Use of Fraud to Breach Microsoft's Security Measures

42. The Defendants and their Fraudulent Enterprise have earned millions of dollars in illicit revenue by selling services to cybercriminals that involve the use of bots to breach Microsoft's security measures through fraudulent representations so that they can obtain Microsoft Outlook accounts, which are then turned into instruments of cybercrime.

43. ***The Hotmailbox Fraud.*** One of the criminal services provided by the Defendants and their Fraudulent Enterprise has been the fraudulent procurement and subsequent sale to cybercriminals of fraudulent Microsoft Outlook accounts via the website https://hotmailbox.me/home (the "Hotmailbox Website").

44. To facilitate this Hotmailbox service, the Defendants have sent their bots to Microsoft's website to create Microsoft Outlook accounts. Each time they did so, Microsoft's automated security measures asked the Defendants' bots to "Please solve the [following] puzzle so we know you're not a robot." Microsoft then presented a CAPTCHA challenge to solve, and asked them to certify they were a human user by clicking "next." On millions of occasions, the Defendants caused their bots to fraudulently impersonate individual human users by solving those CAPTCHA challenges, falsely representing they were "not a robot."

45. Each time the bots successfully completed a CAPTCHA test, the CAPTCHA software provided a unique digital token that allowed the bots to clear that CAPTCHA challenge. Much like a password to an encrypted computer file, such CAPTCHA tokens can—for a few seconds or less—also be recycled by the bots to clear other CAPTCHA challenges.

46. In the process of procuring fraudulent Outlook accounts, the Defendants also caused their bots to make numerous other false representations to break into Microsoft's security systems. For example, each time the Defendants' bots opened a Microsoft Outlook account, the bots agreed to abide by Microsoft's terms of service, including by:

- falsely representing that they would not "circumvent any restrictions on access to, usage, or availability of [Microsoft's] Services" (MSA § 3(a)(vi)), when, in fact, they had breached Microsoft's security restrictions against bots.

- providing false and fictitious identifying information, including fake names and birthdates for non-existent persons purporting to be real users of Microsoft services, in response to automated requests from Microsoft for such information as part of the account registration process.

- falsely representing that they would "not to use any false, inaccurate or misleading information when signing up for [their] Microsoft account" (*id.* § 4(a)(i)), when in fact, they had misrepresented that they were human users and provided fake identifying information in signing up for their Microsoft accounts.

- falsely representing that they would not "transfer [their] Microsoft account credentials to another user or entity" (*id.*), when in fact, the Defendants intended to and did sell such account credentials to customers of their criminal services.

- falsely representing that they would 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 did exactly those things in bypassing Microsoft's CAPTCHA challenges and opening Outlook email accounts in the names of fictitious users.

- falsely representing that they would not "help others break these rules" (*id.* § 3(a)(x)), when in fact, the bots were designed as part of the Defendants' scheme to help customers of the Defendants' criminal services break Microsoft's rules against doing "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)).

47. ***The 1stCAPTCHA Fraud.*** In addition to selling fraudulent Microsoft Outlook accounts via the Hotmailbox Website, the Defendants and their Fraudulent Enterprise have also been selling CAPTCHA-solving tokens procured by the Defendants' bots—through the fraudulent steps described above—to cybercriminals so that they can have their own bots deploy them to bypass Microsoft's CAPTCHA challenges and procure fraudulent Microsoft Outlook email accounts. Millions of fraudulent Microsoft Outlook email accounts have been opened via tokens that the Defendants' bots procured through deception, including the types of misrepresentations described above. The Defendants initially marketed this criminal service via websites available at https://anycaptcha.com (the "AnyCAPTCHA Website") and https://nonecaptcha.com (the "NoneCAPTCHA Website"), and later rebranded and moved it to a website available at https://1stcaptcha.com (the "1stCAPTCHA Website"). Since this rebranding, Internet users who attempt to visit the AnyCAPTCHA and NoneCAPTCHA Websites are automatically redirected to the 1stCAPTCHA Website.

B. The Defendants' Hotmailbox Website

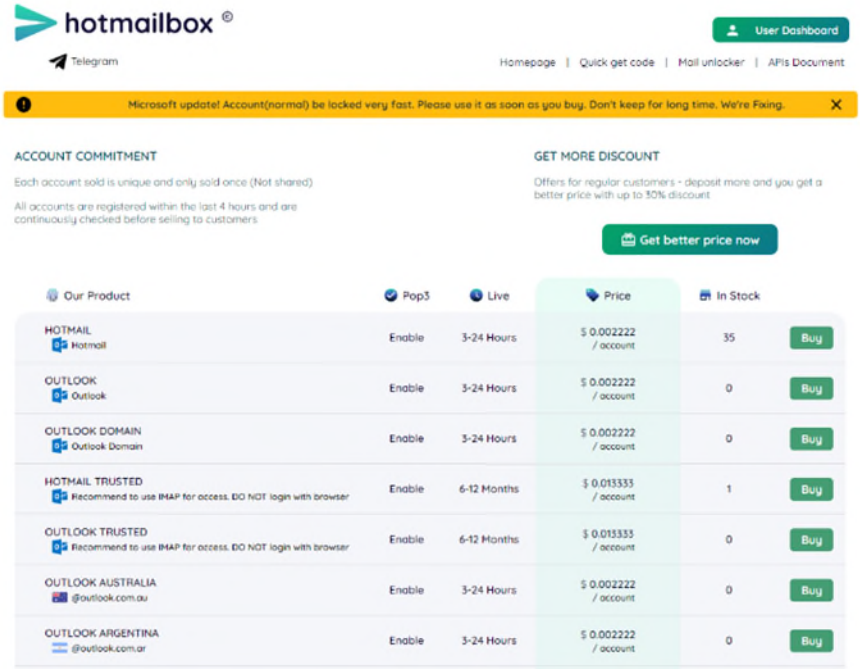
48. A screenshot of the Defendants' Hotmailbox Website is depicted in Figure 1 below.

49. The Hotmailbox Website offers customers of this illicit service a menu of fraudulent Microsoft email accounts procured through the illegal process described above. For example, as shown in Figure 1, a customer can purchase a Microsoft Outlook account registered in the name of a fictitious user that will be live for 3 to 24 hours for $0.002222. The fraudulent accounts sold by the Defendants are not useable for long because of Microsoft's continuous efforts to identify and suspend such accounts.

50. Given that bona fide consumers can open Microsoft Outlook accounts on their own

for free, it is hard to imagine a lawful purpose for buying a Microsoft Outlook account registered to a fake person in breach of Microsoft's terms of service. The brazenly criminal nature of the Hotmailbox scheme is also 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."

FIGURE 1



51. 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. As explained below, the Defendants sully Microsoft's valuable trademarks every time a cybercriminal uses a fraudulent Outlook account purchased from the Defendants to send seemingly innocuous emails to unwitting victims from what appears to be a legitimate Microsoft account, but is actually a Trojan horse used to spread malware capable of causing devastating harm.

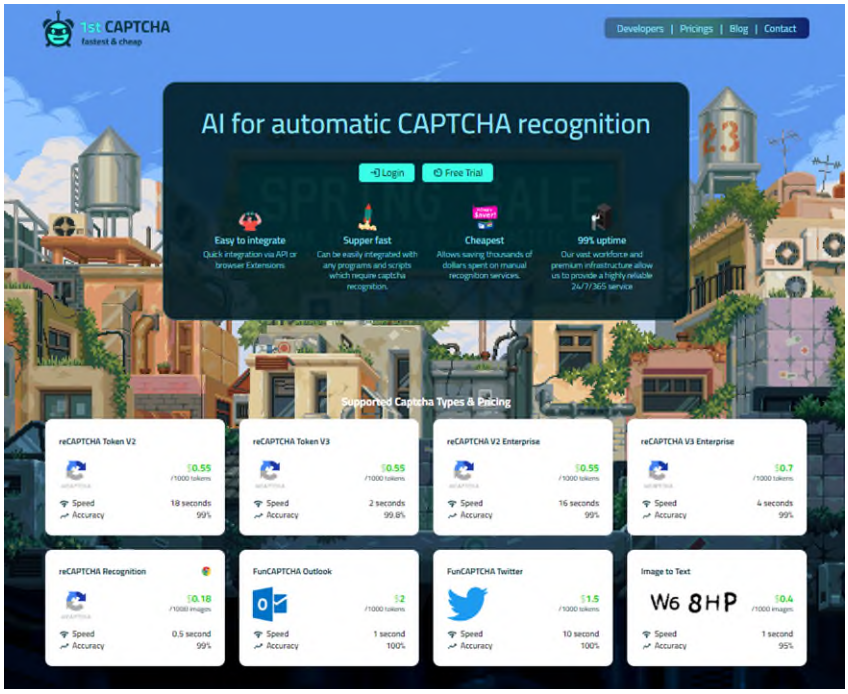
C. The Defendants' 1stCAPTCHA Website

52. A screenshot of the Defendants' 1stCAPTCHA Website is depicted in Figure 2

below.

53. This criminal service sells CAPTCHA-solving tokens—which the Defendants' bots procured fraudulently—to cybercriminals so that they can have their own bots deploy them to bypass Microsoft's CAPTCHA challenges and procure Microsoft Outlook email accounts. For example, as shown in Figure 2, a customer can purchase 1,000 CAPTCHA-solving tokens—each of which was procured by the fraudulent process described above—for $2, enabling them to obtain numerous fraudulent Microsoft Outlook accounts. 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.

FIGURE 2

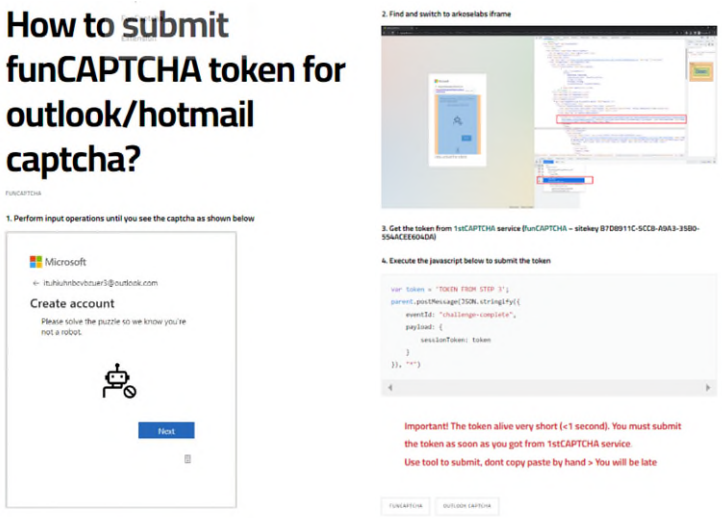


54. The 1stCAPTCHA Website also maintains a blog providing step-by-step guidance on how to use such tokens to bypass Microsoft's security systems to obtain fraudulent Outlook accounts.[3] Screenshots of this guidance are depicted in Figure 3 below. According to the

[3] *See How to submit funCAPTCHA token for outlook/hotmail captcha?*, 1STCAPTCHA (Sept. 6, 2023),

guidance, Step 1 is to undertake the process of opening a Microsoft account until Microsoft's security protocols present a CAPTCHA challenge. As shown in Figure 3, the CAPTCHA challenge is presented "so we know you're not a robot." Step 2 is to buy a CAPTCHA-solving token from 1stCAPTCHA—which the Defendants' bots procured through the fraudulent process described above. Step 3 is to submit the token to bypass Microsoft's security systems. The guidance then encourages the Defendants' customers to use bots of their own to open fraudulent Microsoft accounts with such tokens, noting that customers should "[u]se tool to submit" the tokens; "dont [*sic*] copy paste by hand > You will be late" as "[t]he token alive very short (< 1 second)."

FIGURE 3



55. Defendants do not merely sell services targeted at defrauding Microsoft. Defendants' blog also contains entries explaining how to defeat the CAPTCHA defenses employed by other technology companies, including Twitter (now known as X) and Google.[4]

https://1stcaptcha.com/blog/how-to-submit-funcaptcha-token-for-outlook-hotmail-captcha/.

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

D. The Defendants Adapt to Breach Microsoft's Evolving Security Measures

56. 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, including making its CAPTCHA challenges more difficult for bots to solve.

57. The Defendants have continually adapted in an attempt to overcome such measures. 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) at the top of the Website warning that each account will be "locked very fast," so "[p]lease use it as soon as you buy."

EVIDENCE LINKING DEFENDANTS TO THE FRAUD

58. As shown below, Defendants Duong Dinh Tu (Tu), Linh Van Nguyen (a/k/a Nguyen Van Linh) (Linh), and Tai Van Nguyen (Tai) are members of and have been operating the Fraudulent 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 their criminal conspiracy to do so.

A. Defendant Duong Dinh Tu

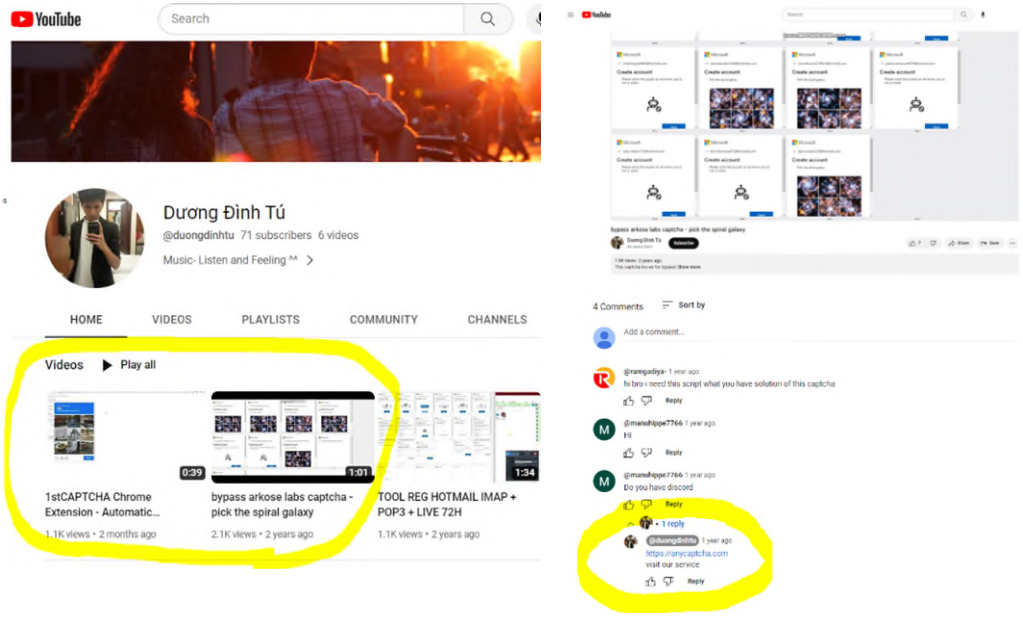
59. According to a search of publicly available Internet domain registration data using a domain name lookup (also called a WHOIS lookup), Defendant Duong Dinh Tu of Vietnam has been the registrant of the Hotmailbox Website from at least in or about November 2021 through in or about July 2023.

60. Defendant Duong Dinh Tu has a YouTube channel—under the YouTube handle "@duongdinhtu"—on which he publicizes the Fraudulent Enterprise's Hotmailbox and

https://1stcaptcha.com/blog/how-to-distinguish-recaptcha-v2-v3-enterprise/.

1stCAPTCHA services. His YouTube channel includes YouTube videos showing recordings of a computer running bots to defraud Microsoft and bypass its CAPTCHA challenges. A screenshot of Tu's YouTube channel is depicted in Figure 4 below. As shown in Figure 4, Tu's YouTube channel includes a YouTube 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."

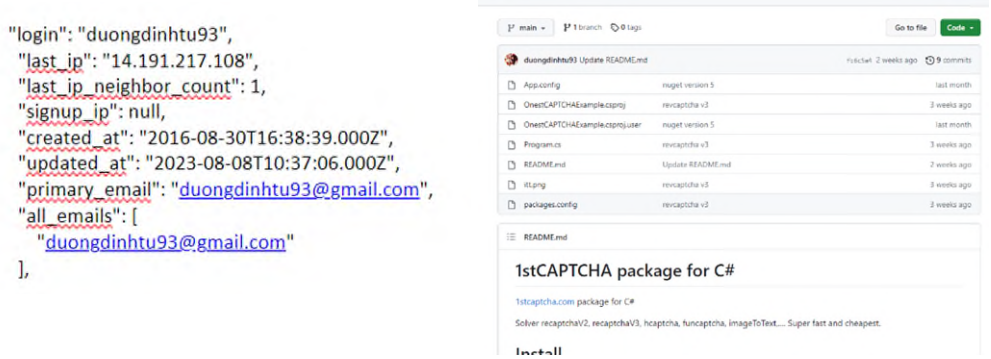
FIGURE 4



61. Defendant Duong Dinh Tu has also edited the source code for the 1stCAPTCHA service via the GitHub website at https://github.com/1stcaptcha (the "1stCAPTCHA GitHub Page"). 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. The 1stCAPTCHA GitHub Page houses the software code necessary to utilize the CAPTCHA-solving tokens sold on the 1stCAPTCHA Website. Screenshots of the 1stCAPTCHA GitHub Page are depicted in Figure 5 below. 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").

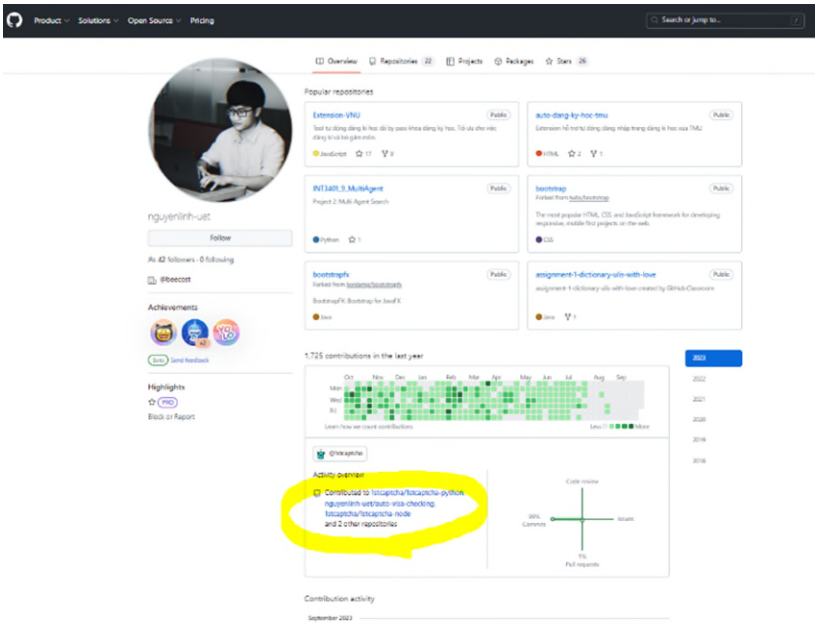
FIGURE 5



B. Defendant Linh Van Nguyen

62. Defendant Linh Van Nguyen has edited the source code for the 1stCAPTCHA service via the 1stCAPTCHA GitHub Page on over 100 occasions during the period from in or about October 2020 through in or about July 2023. A screenshot of his GitHub account page is depicted in Figure 6 below. Figure 6 indicates that Linh has "[c]ontributed" to the 1stCAPTCHA GitHub Page.

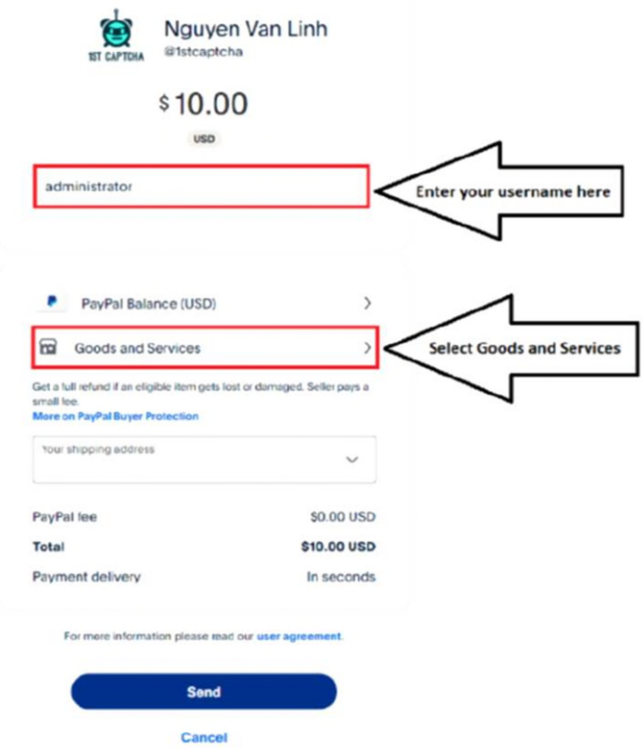
FIGURE 6



63. In addition, payments to purchase services from the 1st CAPTCHA Website via the

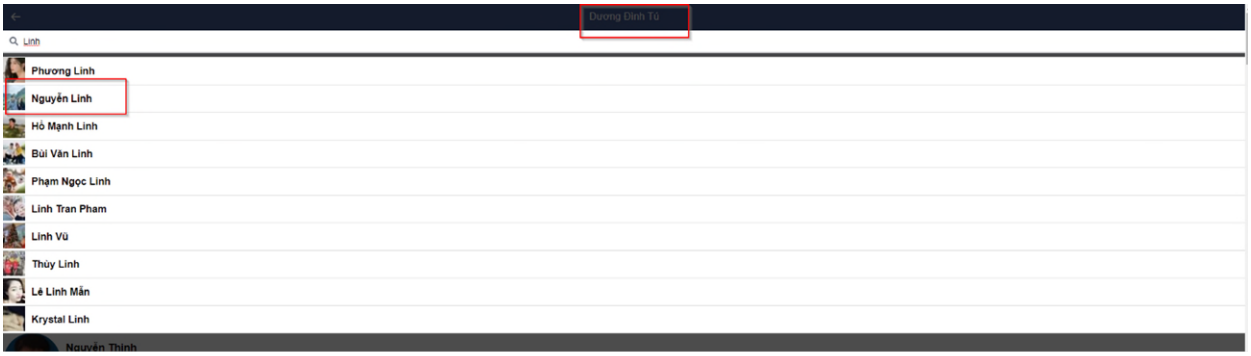
payment processing service PayPal are directed to a 1stCAPTCHA account at PayPal (with the account name "@1stcaptcha") associated with Defendant Linh Van Nguyen. A screenshot of the user interface to submit a PayPal payment to 1stCAPTCHA—noting Linh's association with 1stCAPTCHA's PayPal account—is depicted in Figure 7 below.

FIGURE 7



64. Defendants Linh Van Nguyen (a/k/a Nguyen Van Linh) and Duong Dinh Tu are "friends" on Facebook, according to Duong Dinh Tu's Facebook "friends" lists. A screenshot from the Facebook account of Duong Dinh Tu, showing that Tu is "friends" with "Nguyen Linh," is depicted in Figure 8 below.

FIGURE 8



C. Defendant Tai Van Nguyen

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

HARM TO MICROSOFT, ITS CUSTOMERS, AND THE PUBLIC

66. Despite Microsoft's best efforts at protecting itself against infiltration by the Defendants' Fraudulent Enterprise, the Defendants' bots have repeatedly and persistently used fraud to bypass Microsoft's security measures and CAPTCHA challenges, procure millions of fraudulent Microsoft Outlook email accounts, and sell them to cybercriminals. As set forth above, fraudulent accounts sold by the Defendants can be used, and are believed to have been used, to perpetrate cybercrime activity and inflict severe harm on Microsoft customers.

67. Through their Fraudulent Enterprise, the Defendants have caused tens of millions of dollars in damage to Microsoft and have irreparably harmed its reputation, goodwill, and critical customer relationships.

68. For example, in or about March 2023, a major Microsoft customer experienced

attacks arising out of the Defendants' Fraudulent Enterprise. Specifically, fraudulent Outlook and Hotmail accounts that were purchased from the Defendants' Enterprise were reaping the benefits of the customer's services provided as test trials to prospective users, even though these fraudulent accounts had no intention of ever paying for those services. These Enterprise-originated accounts also caused outages in the customer's systems. Due to these difficulties, the customer blocked all new account sign-ups from Microsoft Outlook and Hotmail, thus irreparably harming Microsoft's business relationship with this major customer as well as countless legitimate Microsoft customers.

69. 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 their criminal scheme.

DEFENDANTS' EXPLOITATION OF MICROSOFT'S TRADEMARKS

70. In selling fraudulent Microsoft accounts and CAPTCHA-defeating tools through the Hotmailbox and 1stCAPTCHA Websites, Defendants misuse several Microsoft trademarks without Microsoft's authorization, including its Outlook launch icon trademark, its Outlook word mark, and its Hotmail word mark.

71. Cybercriminals who purchase fraudulent Microsoft Outlook email accounts from the Defendants' criminal services abuse Microsoft's trademarks to cause their victims to open emails containing computer viruses, ransomware, and other malware. Because the emails appear to have been sent from legitimate Microsoft Outlook accounts, victims trust that they can safely open emails from them, but instead are attacked by malware that installs itself on their computers. Moreover, because of the similarities between Microsoft's registered trademarks and the misappropriated versions utilized by Defendants, consumers seeking legitimate Microsoft

accounts may accidentally arrive on Defendants' Hotmailbox and 1stCAPTCHA Websites.

UNDERCOVER PURCHASES IN NEW YORK

72. To investigate the Defendants' criminal activities, Microsoft retained external cybercrime experts at the Berkeley Research Group ("BRG"). From August through October 2023, BRG made several undercover purchases of fraudulent 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. These undercover purchases confirmed that the Hotmailbox and 1stCAPTCHA Websites provide fraudulent Microsoft Outlook accounts and CAPTCHA-defeating tokens to obtain fraudulent Outlook accounts in exchange for payment, and that those tools successfully bypass Microsoft's CAPTCHA security measures.

73. 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 their Enterprise's criminal services. For example, 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.

FIRST CAUSE OF ACTION
(Violations of the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. §§ 1962(c)-(d)))

74. Plaintiff incorporates by reference each and every allegation set forth above.

75. Defendants are a group of persons associated together in fact for the common purpose of carrying out an ongoing criminal enterprise, namely the Fraudulent Enterprise, and have conducted its affairs through a pattern of racketeering activity, with such conduct and

activities affecting interstate and foreign commerce.

76. At all relevant times, the Defendants conducted or participated, directly or indirectly, in the conduct, management, or operation of the Fraudulent Enterprise's affairs through a pattern of racketeering activity in violation of 18 U.S.C. §§ 1961(5) and 1962(c), with such conduct and activities affecting interstate and foreign commerce.

77. Defendants have conducted their and the Enterprise's affairs through a pattern of racketeering activity affecting interstate and foreign commerce, including millions of predicate acts of wire fraud in violation of 18 U.S.C. § 1343—incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(B)—that have affected and continue to affect interstate and foreign commerce.

78. The Defendants, with intent to defraud and obtain money or property by means of false or fraudulent pretenses, have committed wire fraud in violation of 18 U.S.C. § 1343 by transmitting or causing to be transmitted, by means of wire communication in interstate or foreign commerce, writings, signs, and signals for the purpose of executing fraudulent schemes. Defendants have violated and continue to violate the wire fraud statute in several ways, each instance of which constitutes a separate RICO predicate offense.

79. For example, the Defendants' and their Fraudulent Enterprise commit wire fraud, in violation of 18 U.S.C. § 1343, each time one of their bots falsely represents that it is a human to open a Microsoft account, provides a fictitious user name for a Microsoft account, or falsely represents that it will abide by Microsoft's terms of service in using a Microsoft account.

80. In violation of 18 U.S.C. § 1962(d), each Defendant unlawfully, knowingly, and willfully agreed and conspired together and with others to violate 18 U.S.C. § 1962(c) as described above.

81. The Defendants knew they were engaged in a conspiracy to commit multiple predicate RICO offenses, including millions of acts of wire fraud, and they knew the predicate offenses were part of such racketeering activity, and that their participation and agreement was necessary to allow the commission of this pattern of racketeering activity.

82. Microsoft has been injured in its business and property by reason of Defendants' violations of 18 U.S.C. §§ 1962(c) and (d), as described herein. These injuries are direct, proximate, and reasonably foreseeable results of these violations, which continue to harm Microsoft.

83. Under 18 U.S.C. § 1964(c), Microsoft is entitled to recover and seeks treble damages plus costs and attorneys' fees from the Defendants.

84. Microsoft also seeks injunctive relief and compensatory, treble, and punitive damages in an amount to be proven at trial, including without limitation disgorgement of Defendants' ill-gotten gains.

85. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SECOND CAUSE OF ACTION
(Trademark Infringement in Violation of the Lanham Act (15 U.S.C. § 1114 *et seq.*))

86. Microsoft incorporates by reference each and every allegation set forth above.

87. Defendants have used Microsoft's trademarks in interstate commerce without Microsoft's permission.

88. Defendants and their Enterprise have generated and used unauthorized copies of Microsoft's trademarks in selling fraudulent versions of Microsoft Outlook email accounts to cybercriminals, including by making unauthorized uses of Microsoft's word marks, design marks,

and federally registered trademarks associated with Microsoft software and services. Defendants make use of these Microsoft trademarks without Microsoft's permission in interstate commerce, including Microsoft's federally registered trademarks for Microsoft Outlook. By doing so, Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the fraudulent and unauthorized versions of the Microsoft Outlook email accounts that the Defendants have been selling to cybercriminals.

89. As a result of their wrongful conduct, Defendants are liable to Microsoft for their violations of the Lanham Act.

90. Microsoft seeks injunctive relief and compensatory, treble, and punitive damages in an amount to be proven at trial, including without limitation disgorgement of Defendants' ill-gotten gains.

91. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

92. Defendants' wrongful and unauthorized use of Microsoft's trademarks to promote, market, or sell products and services constitutes trademark infringement pursuant to 15 U.S.C. § 1114 *et seq.*

THIRD CAUSE OF ACTION
(False Designation of Origin, Federal False Advertising, and Federal Unfair Competition in Violation of the Lanham Act (15 U.S.C. § 1125(a)))

93. Plaintiff incorporates by reference each and every allegation set forth above.

94. Microsoft's trademarks are distinctive marks that are associated with Microsoft and exclusively identify its businesses, products, and services.

95. Defendants make unauthorized use of Microsoft's trademarks. By doing so,

Defendants create false designations of origin as to tainted Microsoft products that are likely to cause confusion, mistake, or deception.

96. As a result of their wrongful conduct, Defendants are liable to Microsoft for their violations of the Lanham Act, 15 U.S.C. § 1125(a).

97. Microsoft seeks injunctive relief and compensatory, treble, and punitive damages in an amount to be proven at trial, including without limitation disgorgement of Defendants' ill-gotten gains.

98. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

FOURTH CAUSE OF ACTION
(Trademark Dilution in Violation of the Lanham Act (15 U.S.C. § 1125(c)))

99. Plaintiff incorporates by reference each and every allegation set forth above.

100. Microsoft's trademarks are famous marks that are associated with Microsoft and exclusively identify its businesses, products, and services.

101. Defendants make unauthorized use of Microsoft's trademarks. By doing so, Defendants are likely to cause dilution by tarnishment and/or dilution by blurring of Microsoft's trademarks.

102. Microsoft seeks injunctive relief and compensatory, treble, and punitive damages in an amount to be proven at trial, including without limitation disgorgement of Defendants' ill-gotten gains.

103. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

FIFTH CAUSE OF ACTION
(Tortious Interference with Business Relationships)

104. Plaintiff incorporates by reference each and every allegation set forth above.

105. Microsoft has valid and subsisting contractual relationships, including with licensees of its Outlook products. Microsoft's contracts confer economic benefits on Microsoft.

106. Defendants' conduct interferes with Microsoft's contractual relationships by impairing, and in some instances destroying, the quality and value of the products and services Microsoft provides to its customers. On information and belief, Defendants know that their conduct is likely to interfere with Microsoft's contracts and to deprive Microsoft of the attendant economic benefits.

107. On information and belief, Microsoft has lost business, including from licensees, due to Defendants' conduct.

108. Microsoft seeks injunctive relief and compensatory, treble, and punitive damages in an amount to be proven at trial, including without limitation disgorgement of Defendants' ill-gotten gains.

109. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SIXTH CAUSE OF ACTION
(Conversion)

110. Microsoft incorporates by reference each and every allegation set forth above.

111. Microsoft owns all right, title, and interest in its Outlook services. Defendants have interfered with, unlawfully and without authorization, and dispossessed Microsoft of control over its Outlook services.

112. Defendants have unlawfully and without authorization taken and converted for their own purposes confidential data from Microsoft computer systems, including digital CAPTCHA-solving tokens that represent passkeys to Microsoft services that they were not entitled to access.

113. Defendants have, without authority, used a Microsoft computer or computer network, with the intent to remove, halt, or otherwise disable computer data, computer programs, or computer software from a Microsoft computer or computer network.

114. Defendants have, without authority, used a Microsoft computer or computer network with the intent to cause a computer to malfunction.

115. Microsoft seeks injunctive relief and compensatory, treble, and punitive damages in an amount to be proven at trial, including without limitation disgorgement of Defendants' ill-gotten gains.

116. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SEVENTH CAUSE OF ACTION
(Trespass to Chattels)

117. Microsoft incorporates by reference each and every allegation set forth above.

118. Defendants' activities resulted in unauthorized access to the computers and servers of Microsoft and its customers that resulted in an intrusion without permission into those computers and servers.

119. Defendants have used a computer or computer network, without permission, with the intent to cause physical injury to the property of another.

120. Defendants intentionally caused this conduct, which was unlawful and unauthorized.

121. Defendants' actions have caused injury to Microsoft and its customers and have interfered with the possessory interests of Microsoft over its software.

122. Microsoft seeks injunctive relief and compensatory, treble, and punitive damages in an amount to be proven at trial, including without limitation disgorgement of Defendants' ill-gotten gains.

123. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

EIGHTH CAUSE OF ACTION
(Unjust Enrichment)

124. Plaintiff incorporates by reference each and every allegation set forth above.

125. The acts of Defendants complained of herein constitute unjust enrichment of the Defendants at the expense of Microsoft, in violation of the common law. Defendants used, without authorization or license, software and trademarks belonging to Microsoft to facilitate unlawful conduct inuring to the benefit of Defendants.

126. Defendants profited unjustly from their unauthorized and unlicensed use of Microsoft's property.

127. Upon information and belief, Defendants had an appreciation and knowledge of the benefit they derived from their unauthorized and unlicensed use of that property.

128. Retention by the Defendants of the profits they derived from their malfeasance would be inequitable.

129. Plaintiff seeks injunctive relief and compensatory, treble, and punitive damages in an amount to be proven at trial, including without limitation disgorgement of Defendants' ill-gotten gains.

130. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

PRAYER FOR RELIEF

WHEREFORE, Microsoft respectfully requests that this Court enter judgment in Microsoft's favor and against Defendants and grant the following relief:

A. Enter judgment in favor of Microsoft against the Defendants;

B. Declare that Defendants have violated RICO and the Lanham Act, and are therefore liable to Microsoft;

C. Declare that Defendants have tortiously interfered with Microsoft's business relationships, converted and trespassed upon the property and chattels of Microsoft, and have been unjustly enriched, and are therefore liable to Microsoft;

D. Declare that Defendants have infringed and diluted Microsoft's trademarks;

E. Declare the substantial likelihood that Defendants will continue to infringe and dilute Microsoft's intellectual property unless enjoined from doing so;

F. Declare that Defendants' conduct has been willful and that Defendants have acted with fraud, malice, and oppression;

G. Order that all copies made or used in violation of Microsoft's trademarks, and all means by which such copies may be reproduced, be impounded and destroyed or otherwise reasonably disposed of;

H. Enter a temporary restraining order and preliminary and permanent injunction enjoining Defendants and their Enterprise's officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or

participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein;

I. Enter a temporary restraining order and preliminary and permanent injunction giving Microsoft control over the Internet domains listed in Appendix A that are used by Defendants to cause injury and enjoining Defendants from using such domains and other similar instrumentalities;

J. Enter an award of appropriate equitable relief under available law, including injunctive relief and an accounting of profits;

K. Enter judgment awarding Microsoft actual damages from Defendants adequate to compensate Microsoft for Defendants' activity complained of herein and for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial;

L. Enter judgement awarding Microsoft treble and punitive damages;

M. Enter judgment for Microsoft disgorging Defendants' profits;

N. Enter judgment awarding enhanced, exemplary, and special damages, in an amount to be proved at trial;

O. Enter judgment awarding attorneys' fees and costs; and

P. Order such other relief that the Court deems just and reasonable.

DEMAND FOR JURY TRIAL

Microsoft respectfully requests a trial by jury in this action of all issues so triable.

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