

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

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

**DECLARATION OF PATRICE BOFFA IN SUPPORT OF
PLAINTIFF MICROSOFT’S MOTION FOR AN EMERGENCY *EX PARTE*
TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE**

I, Patrice Boffa, declare as follows:

1. I am the Chief Customer Officer of Arkose Labs, a global cybersecurity company focused on detecting, preventing, and eliminating cyber fraud and other cyber threats for prominent institutional clients such as Microsoft Corporation. Arkose has approximately 200 employees across offices in the United States, Australia, Spain, England, Costa Rica, India, and Argentina. I make this declaration in support of Microsoft’s motion for an emergency *ex parte* temporary restraining order and order to show cause why a preliminary injunction should not be entered in the above-captioned case.

2. In my role at Arkose, I advise our customers, including Microsoft, on the use of Arkose cybersecurity and antifraud products and services. Prior to joining Arkose in October 2021, I held various roles within the security departments of two major technology companies

where I had a considerable focus on cybersecurity threats. A true and correct copy of my curriculum vitae is attached to this declaration as Exhibit 1.

3. Since in or about August 2021, I have been investigating the structure and function of a criminal organization referred to herein as the “Fraudulent Enterprise” (or the “Enterprise”). The Enterprise is a group of individuals in the business of using fraud and deception to breach Microsoft’s security systems, procuring Microsoft accounts in the names of fictitious users, and selling these fake accounts to cybercriminals for a wide variety of internet-based crimes (the “Fraudulent Scheme”).

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

I. Background on CAPTCHA

5. The cybersecurity services that Arkose provides to Microsoft include so-called “CAPTCHA” security measures. The term “CAPTCHA” stands for “Completely Automated Public Turing Test to tell Computers and Humans Apart.” CAPTCHA is a security measure used to verify that someone attempting to enter a particular service or ecosystem over the Internet is actually a human being, as opposed to an Internet “bot.” CAPTCHA tests do so by presenting different types of challenges that, if answered correctly, provide a high level of confidence that the apparent user solving the challenge is, in fact, a human being. Such challenges may include, for example, (i) re-typing a code appearing in an image, (ii) selecting the images that display a certain type of object (e.g., streets or cars), or (iii) rotating a figure a particular way as requested. When a CAPTCHA challenge is successfully solved, a unique digital “token” is created, which may then be used for a very short period of time (before “timing out”) to gain access to a particular service

or ecosystem. Each unique token is supposed to grant access one time only, but can be exploited to bypass other CAPTCHA challenges until the token “times out.”

6. Because of the high incidence of cybercrime associated with the use of bots, Microsoft utilizes CAPTCHA challenges powered and operated by Arkose as an antifraud tool to help ensure, among other things, that only real human beings are permitted to obtain Microsoft accounts.

7. While CAPTCHA has been widely acclaimed for its success in defeating fraud, some bad actors (including the Fraudulent Enterprise) have found ways to misuse CAPTCHA tokens by harvesting them in bulk through the use of bots and then selling them to customers, who may then quickly utilize the tokens for improper purposes before they expire. Such improper purposes include the bulk creation of fake Microsoft accounts for later use in cyberattacks and other misconduct.

II. History of the Fraudulent Enterprise

8. Arkose first discovered signs of the Fraudulent Enterprise in or about August 2021, when my team 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).

9. Arkose conducted various initial mitigation efforts in and around August 2021, including by enhancing existing CAPTCHA challenges, verifying timeouts (in order to limit the lifetime of a solved puzzle token so it would have little or no value to the Enterprise or its criminal customers), and blocking verifications on any challenges that we understood to be coming from the Enterprise’s website, which we eventually learned was called “AnyCAPTCHA.com” (the “AnyCAPTCHA Website”). By November 2021, however, the sophisticated cybercriminals

operating the AnyCAPTCHA Website began defeating the challenges again, suggesting that they had adapted to Arkose's enhancements.

10. Through queries on the "WHOIS.com" database (which contains public information about website domains and registration), we learned that in addition to operating the AnyCAPTCHA.com website (which, as noted, sold only the tokens to defeat CAPTCHA tests for the purpose of creating a Microsoft account), the Fraudulent Enterprise also began operating a website known as "Hotmailbox.me," which sells pre-authorized Microsoft accounts that the Fraudulent Enterprise procured itself by using its own bot-harvested CAPTCHA-defeating tokens (the "Hotmailbox Website").

11. The fact that the same cybercriminals operated both the AnyCAPTCHA and Hotmailbox Websites is evidenced by a chat, which occurred on January 14, 2022, between a member of my team at Arkose and the "help desk" function of the AnyCAPTCHA website. A screenshot of this chat is depicted in Figure 1 below.¹

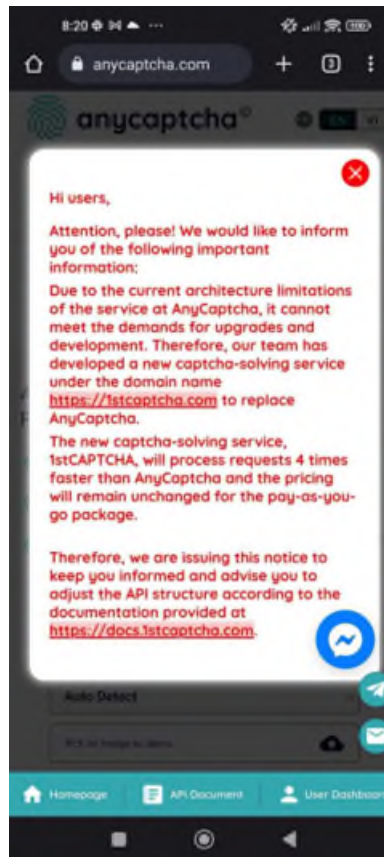
¹ A redaction has been made to information within Figure 1 that, if revealed, would identify the undercover methods and means used to investigate the Fraudulent Enterprise's ongoing criminal activity. An unredacted version of Figure 1 will be made available during discovery in this action assuming that an appropriate protective order is entered.

FIGURE 1



12. In or about December 2022, the Fraudulent Enterprise appeared to migrate its criminal services from the AnyCAPTCHA Website to a similar but revamped site known as 1stCAPTCHA.com (“1stCAPTCHA Website”), from which they claimed to process fraudulently-obtained CAPTCHA tokens four times faster than on the prior site. Figure 2 below is a screenshot of a message displayed on July 4, 2023 on the AnyCAPTCHA Website, directing customers to the 1stCAPTCHA Website.

FIGURE 2



13. Based on my investigation, the Fraudulent Enterprise attempts to avoid detection and disguise itself by using proxy services and recycling their U.S. Internet protocol (“IP”) addresses and Autonomous System Numbers (“ASNs”) through products offered by companies known as ColoCrossing, Cloudflare, Bright Data and Proxyrack. In total, the Fraudulent Enterprise has utilized at least 2.6 million IP addresses across 16,000 ASN numbers.

III. Connections to Defendants

14. Arkose’s investigation of the Fraudulent Enterprise has determined that one of the individuals involved in the Enterprise is Linh Van Nguyen, who is named as a Defendant in the above-captioned case. This is based in part on the fact that when someone attempts to purchase the CAPTCHA-defeating tool provided by the 1stCAPTCHA Website using PayPal or

Vietcombank, the 1stCAPTCHA Website directs them to make the payment directly to this individual.

15. Furthermore, WHOIS search results verify that the AnyCAPTCHA, 1stCAPTCHA, and Hotmailbox Websites were all registered by registrants in Vietnam. Specifically, the AnyCAPTCHA and 1stCAPTCHA Websites were registered by the same corporation in Vietnam, and the Hotmailbox Website was registered by Duong Dinh Tu, who is also named as a Defendant in the above-captioned case. Figure 3 below depicts a screenshot of the WHOIS results for the Hotmailbox Website reflecting that it was registered by Tu.

Figure 3

WHOIS search results

Domain Name: hotmailbox.me
Registry Domain ID:
ba9177103c3c459ebe5a6ac360215082-DONUTS
Registrar WHOIS Server:
www.onlinenic.com/domain-whois/
Registrar URL: <https://www.onlinenic.com/signup/>
Updated Date: 2022-09-29T02:52:33Z
Creation Date: 2021-11-03T02:21:41Z
Registry Expiry Date: 2023-11-03T02:21:41Z
Registrar: OnlineNIC, Inc.
Registrar IANA ID: 82
Registrar Abuse Contact Email:
complaints@onlinenic.com
Registrar Abuse Contact Phone:
Domain Status: ok <https://icann.org/epp#ok>

Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: **Duong Dinh Tu**
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: **Ho Chi Minh**
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: **VN**
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the
Registrar of Record identified in this output for
information on how to contact the Registrant, Admin, or
Tech contact of the queried domain name.

IV. Damage Caused by the Fraudulent Enterprise

16. Based on our assessment of dedicated IP addresses used by the Fraudulent Enterprise and Password Unique Identifiers with sign-ins from these accounts,² we estimate that the Fraudulent Enterprise has created and sold roughly 750 million fake Microsoft accounts to date.

17. According to its websites, the Fraudulent Enterprise sells such fake Microsoft accounts for an average sale price of roughly \$0.004 per account, meaning that the Enterprise


² Every Microsoft account has its own unique Password Unique Identifier code.

would have collected an unlawful profit of roughly \$3 million as a result of the Fraudulent Scheme victimizing Microsoft and its customers.

18. Arkose has undertaken resource-intensive efforts—at millions of dollars in expense to Microsoft—to identify and disrupt the Fraudulent Enterprise. Indeed, since approximately August 2021, when Arkose first discovered the threat that became known as the Fraudulent Enterprise, we have assigned as many as 30 employees, working 24 hours per day, each day of the week (24/7), to a team focused on abating these efforts. As a result, Microsoft has incurred millions of dollars in fees and costs for Arkose services relating to disrupting the Fraudulent Enterprise.

19. Based on my experience, the Fraudulent Enterprise currently poses the largest danger to Microsoft of any cyber threat actor. Specifically, according to Arkose’s traffic categorization statistics, which are shown in Figure 4 below, as compared to other attackers, 1stCAPTCHA has the highest percentage of verified sessions, nearly doubling other attackers. This demonstrates the level of sophistication of the Fraudulent Enterprise and its ability to constantly adapt to avoid Arkose’s and Microsoft’s detection and prevention efforts.

FIGURE 4

Traffic categorisation: session counts 28/09 - 11/09 					
Attacker / Category	#sessions (millions)	#verifies (millions)	%verified	%attempted	%solved (per attempt)
1stCaptcha	68.3	45.7	67.0	83.0	92.2
High Wall	109.0	33.8	31.1	33.3	94.8
Other attackers	94.1	30.8	32.7	62.7	66.8
Legit users	33.5	22.8	68.2	76.1	95.4

20. In February 2023, Arkose experienced a distributed denial-of-service (“DDoS”) attack on its systems.³ Arkose has attributed this DDoS attack, based on a root cause analysis, to the AnyCAPTCHA Website and the Fraudulent Enterprise as its operator.

V. Defendants’ Scheme is an Industry-Wide Problem

21. The Enterprise’s CAPTCHA-defeating tools are used against a host of technology companies that employ CAPTCHA challenges provided by Arkose to secure their systems. In other words, the Enterprise’s Fraudulent Scheme is a significant issue not only for Microsoft, but for numerous other Arkose clients and the technology industry as a whole.

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

Executed on this 30th day of NOVEMBER, 2023 in Mountain View, CA.



Patrice Boffa

³ DDoS attacks disrupt the traffic of a network, service, or sever by overwhelming it or its surrounding infrastructure with irregularly large amounts of internet traffic.