UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

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

DECLARATION OF SHINESA CAMBRIC IN SUPPORT OF PLAINTIFF MICROSOFT'S MOTION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

I, Shinesa Cambric, declare as follows:

1. I am the Principal Product Manager of the Anti-Abuse and Fraud Defense Team at Microsoft Corporation. I respectfully submit 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 Microsoft, I assess whether malicious actors or their "bots"[1] are creating accounts in the ecosystem of Microsoft software and services offered to Microsoft customers, or are otherwise violating Microsoft's terms of service.[2] I am also a member of a task

[1] Internet bots are software programs that simulate human user behavior and perform repetitive, automated tasks.

[2] A true and correct copy of Microsoft's Services Agreement detailing its terms of service, published July 30, 2023 and effective September 30, 2023, is attached to this declaration as Exhibit 1, and is also available online at https://www.microsoft.com/en-us/servicesagreement/.

force of Microsoft employees that has been assembled to address the cybersecurity threats presented by the illicit online criminal enterprise referred to herein as the "Fraudulent Enterprise."

3. Prior to joining Microsoft, I held various roles in the cybersecurity departments of several major corporations, including Vistra Corp., Fossil Group Inc., Rockwell Collins, NewellRubbermaid, MedQuist, Inc., and International Paper. In each role, I focused on using state-of-the-art technology to prevent malicious actors from penetrating company security systems. I am a Certified Cloud Security Professional (CCSP), a Certified Information Security Manager (CISM), and a Certified Data Privacy Solutions Engineer (CDPSE). A true and correct copy of my curriculum vitae and certifications is attached to this declaration as Exhibit 2.

4. Since in or about June 2022, I have been investigating the structure and function of the Fraudulent Enterprise, which is in the business of using fraud and deception to breach Microsoft's security systems, open Microsoft accounts in the names of fictitious users, and then sell these fake Microsoft accounts to cybercriminals for use in a wide variety of internet-based crimes (the "Fraudulent Scheme").

5. Through this scheme, the Fraudulent Enterprise has created and sold millions of fake Microsoft accounts. Microsoft has incurred tens of millions of dollars in expenses to abate the threats caused by the Fraudulent Enterprise, including millions of dollars on upgrades to adapt to its evolving fraud. The Fraudulent Enterprise has also caused irreparable damage to Microsoft's reputation, goodwill, and relationships with key customers and will continue to do so absent injunctive and other relief to disrupt the scheme.

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

I. Microsoft's Efforts to Protect Customers

7. Microsoft invests significant time and money to deliver services to its customers in a safe and secure fashion, and to generate and sustain 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 software ecosystem to help ensure that its customers enjoy a positive, worry-free experience when they use Microsoft's services. 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.

8. As the Principal Product Manager of Microsoft's Anti-Abuse and Fraud Defense Team, I participate directly in these efforts, some of which are summarized below.

A. Prevention

9. Because bots can perform repetitive tasks rapidly, they are frequently used by cybercriminals for a wide array of illegal ends, including to spray emails and other communications across the Internet to disseminate computer viruses, such as "ransomware" used to extort payments from victims, and other types of malicious software ("malware").

10. To prevent bots controlled by malicious actors from opening Microsoft accounts, Microsoft contracts with a leading vendor called Arkose Labs, which employs a state-of-the-art CAPTCHA defense service that 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 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, in fact, human. CAPTCHA stands for "Completely Automated Public Turing test to tell Computers and Humans Apart."

11. Microsoft also 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 its Outlook and Skype platforms) for signs of suspicious behavior (such as indications of bots opening fake 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.

B. Detection and Suspension

12. Microsoft also employs in-house-developed algorithms that leverage artificial intelligence, machine learning, and heuristics to aggregate and assess signals related to suspicious behaviors, attributes, and patterns for users and devices that would indicate the presence of a bot or other malicious actor.

13. To identify these activities and actors, Microsoft classifies users according to a ranking system based on signal combinations. This ranking system—which ranks accounts as (i) unknown, (ii) basic, (iii), preferred, (iv) suspicious, (v) or abusive—is crucial because Microsoft suspends accounts only when it has high confidence, based on the algorithms and signals being shared, that the account deserves suspension.

II. Discovery of the Fraudulent Enterprise

14. In 2021, Microsoft's Identity Organization and Security Research teams initially detected the Fraudulent Enterprise after noticing suspicious patterns of Microsoft accounts being opened by overlapping Internet Protocol (IP) addresses.[3]

15. After conducting an investigation into the source of these suspicious patterns, Microsoft determined that the Fraudulent Enterprise had been causing bots to use fraud and

[3] An IP address is a unique identifying number that is assigned to every device connected to the internet.

deception to bypass Microsoft's CAPTCHA challenges, open Microsoft accounts in bulk in the names of fictitious users, and sell these fake Microsoft accounts to cybercriminals.

16. From April 2023 through June 2023, to stem the harm caused by the Fraudulent Enterprise, Microsoft systematically identified and suspended up to 200,000 fake Microsoft accounts per day that were opened by bots controlled by the Enterprise.

17. In response, the Fraudulent Enterprise adapted its methods and tactics and managed to continue breaching Microsoft's security systems and opening substantial volumes of fake Microsoft accounts. Microsoft's Identity Organization and Security Research teams then introduced two new cybersecurity algorithms, which utilized insights from past data studies as well as ongoing investigations of the Fraudulent Enterprise. These algorithms were integrated into Microsoft's production systems for the purpose of identifying fake Microsoft accounts that met the Fraudulent Enterprise's new patterns even faster and with high levels of precision. These algorithms continue to seek out potentially problematic accounts, using a combination of account features and logs derived from Identity Organization data sources, including domain features, recovery data, and alias features.

18. To further address the issues caused by the Fraudulent Enterprise, Microsoft formed a task force of roughly twenty investigators and engineers. The task force continues to confer on a regular basis for the purpose of attempting to abate the threats caused by the Fraudulent Enterprise.

III. Harm to Microsoft, Its Customers and the Public

19. Despite Microsoft's best efforts at warding off the Fraudulent Enterprise, it has nonetheless continued its misconduct on a massive scale, creating a substantial risk that Microsoft, its customers, and the public will be harmed by malware spread using fake Microsoft accounts

sold by the Fraudulent Enterprise. Based on our analysis of internal Microsoft data pertaining to the scheme, we estimate that the Fraudulent Enterprise has created and sold roughly 750 million fake Microsoft accounts to date.

20. Microsoft has incurred tens of millions of dollars in expenses to abate the threats caused by the Fraudulent Enterprise, including millions of dollars on upgrades to CAPTCHA challenges to adapt to its evolving scheme. The Fraudulent Enterprise has also caused irreparable damage to Microsoft's reputation, goodwill, and relationships with key customers.

21. For example, in or about March 2023, a major Microsoft customer experienced attacks arising out of the actions of the Fraudulent Enterprise. Specifically, fake Microsoft Outlook and Hotmail accounts purchased from the Fraudulent Enterprise were reaping the benefits of the customer's services provided as test trials to prospective users, even though these fake accounts had no intention of ever paying for those services. These 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 and harming countless legitimate Microsoft customers.

22. The Fraudulent Enterprise's 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 Fraudulent Enterprise absent injunctive and other relief to disrupt their scheme.

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 30 day of November, 2023 in Sachse, Texas.

Shinesa Cambric

Shinesa Cambric