UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

Microsoft Corporation, a Washington Corporation and Health-ISAC, INC., a Florida Corporation,

Plaintiff,

v.

Saad Fridi,

and

John Does 1-4, Controlling A Computer Network and Thereby Injuring Plaintiffs and Their Customers,

Defendants.

Civil Action No.

FILED UNDER SEAL PURSUANT TO LOCAL RULE 5

DECLARATION OF ERROL WEISS IN SUPPORT OF *EX PARTE* APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER

I, Errol Weiss, declare as follows:

1. I am the Chief Security Officer of the Health Information Sharing & Analysis Center ("Health-ISAC"), which is a Plaintiff in this action. I make this declaration in support of Plaintiffs' Application for an Emergency Temporary Restraining Order and Order to Show Cause re Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where noted. If called as a witness, I could and would testify to the truth of the matters set forth herein.

2. I have been employed by Health-ISAC since April 2019. In my role at Health-ISAC, I created and staffed Health-ISAC's Threat Operations Center in Orlando, Florida, providing global health organizations with meaningful and actionable threat intelligence relevant for information technology and information security professionals in the healthcare sector.

3. Health-ISAC is a non-profit industry organization that represents more than 1,100 member organizations both in the United States and globally including hospitals, medical device

manufacturers, pharmaceutical manufacturers, insurers, and health IT organizations.

4. I began my career with the National Security Agency (NSA) conducting vulnerability analyses and penetrations of highly classified U.S. Government systems and then spent ten years with consulting firms delivering information security services such as managed security services, security product implementations and secure network designs for Fortune 100 companies. A current version of my curriculum vitae is attached to this declaration as **Exhibit 1.**

5. I have over 30 years of experience in Information Security. Prior to joining Health-ISAC, I was the Senior Vice President at Bank of America (2016-2019), overseeing the Global Information Security and Cyber Threat Intelligence teams. I worked with internal partners to protect information, customers and staff by reducing the impact from cyber threats. From 2006 to 2016, I led Citigroup's Cyber Intelligence Center, a global organization that provides actionable intelligence to thousands of end-users across the entire enterprise. In 2012, I testified as an expert witness before the U.S. House Financial Services Committee's Subcommittee on Capital Markets and Government Sponsored Enterprises at the "Cyber Threats to Capital Markets and Corporate Accounts" hearing.

6. Since 2012, I have worked with Microsoft to disrupt criminal malware and botnets responsible for significant fraud losses impacting both healthcare and financial institutions and their customers, resulting in subsequent civil actions including successful disruptions of the malware families Zeus (2012), Citadel (2013) and Shylock (2014). Most recently, I was personally involved in Health-ISAC's efforts in connection with the successful disruption of the RaccoonO365 Operation in the Southern District of New York in 2025.

I. OVERVIEW OF TYCOON 2FA AND PHISHING

6. My declaration concerns Tycoon 2FA phishing kits that are advertised and

promoted as being able to circumvent the security features of Microsoft products, steal Microsoft 365 credentials and bypass multi-factor authentication. I received information from Microsoft in connection with its investigation of the Tycoon 2FA Defendants. Based on that information, I understand Tycoon 2FA Defendants have developed, sold, and facilitated the deployment of phishing kits that enable other cybercriminals to create and deploy phishing attacks with ease. The Tycoon 2FA business model of selling phishing kits and services to cybercriminals is known as Phishing-as-a-Service ("PhaaS"). Threat actors have been able to leverage Tycoon 2FA phishing kits to carry out credential theft, information exfiltration, and subsequent end-user terminal attacks.

7. Phishing attacks continue to be a major cybersecurity concern for Health-ISAC members and the broader health sector, with significant financial and operational consequences. Phishing schemes are a dominant attack vector in the healthcare sector, and they are involved in a significant percentage of cyberattacks. According to the IBM X-Force Threat Intelligence Index, phishing scams are the top infection vector in cyberattacks on healthcare organizations. This aligns with findings from the US Department of Health & Human Services, Health Sector Cybersecurity Coordination Center (HC3), which highlights phishing as a "common tactic" used against the health sector. According to the Health Industry Cybersecurity Practices (HICP) guidelines, phishing simulations conducted in healthcare organizations often reveal click rates between 10% and 30% for employees who fall for phishing emails during tests. HICP noted that healthcare employees are particularly vulnerable to phishing due to the high volume of emails they receive daily and the urgency often associated with their work. This makes them more likely to click on malicious links or attachments. The average downtime for a healthcare company successfully attacked by a cybercriminal is 19 days—during which time patient care can be severely impacted through canceled surgeries, diverted ambulances, and compromised medical

records. The average cost of ransomware in the healthcare sector is staggering, reflecting both the financial and operational toll these attacks impose. Here's a breakdown of the key figures:

- **Average Ransom Payment**: Healthcare organizations paid an average ransom of **$2.57 million** in 2024, according to the HIPAA Journal.
- **Recovery Costs (Excluding Ransom Payments)**: The average cost to recover from a ransomware attack in 2025 (excluding ransom payments) was **$1.53 million**, as reported by Sophos. This figure includes downtime, personnel time, device costs, network costs, and lost opportunities. For larger healthcare organizations with 1,000–5,000 employees, recovery costs can exceed **$1.83 million**.
- **Total Costs (Including Ransom Payments)**: When factoring in both ransom payments and recovery costs, the financial burden becomes even more severe. For example, in 2024, the average total cost of a ransomware attack on a healthcare organization was estimated at **$4.4 million**, with downtime alone costing up to **$900,000** per incident.
- **High-Profile Example**: The 2024 ransomware attack on Change Healthcare serves as a stark example of the potential financial impact. This attack exposed the personal health information of 190 million people and left numerous medical facilities unable to process claims or receive payments. The estimated direct costs associated with this attack reached **$1.15 billion**.

8. The Tycoon 2FA phishing kits make hospitals and other healthcare organizations vulnerable to ransomware attacks and the costs associated with defending against and remediating them.

9. Based on Microsoft's investigation, I understand that Tycoon 2FA Defendants sell

their phishing kits on a subscription basis making these phishing kits a low-cost, and potentially high-reward opportunity for cybercriminals. And because these kits are not designed for one-time use, they can be used repeatedly during the duration of the subscription. For several hundred dollars, a cybercriminal can launch thousands of phishing attacks against healthcare companies.

II. MY INVESTIGATION INTO TYCOON 2FA

10. I investigated the impact that the Tycoon 2FA Defendants and the phishing kits they sell have on the healthcare industry. I received threat intelligence data from the Microsoft DCU investigators regarding domains that they had identified and attributed to Tycoon 2FA phishing kits. I also received threat intelligence from SpyCloud[1] regarding victim information for entities that had been successfully phished (successfully phished means that Tycoon 2FA successfully intercepted the credentials for a user account). This victim information included identification of Health-ISAC member organizations where Microsoft and SpyCloud had observed phishing activity that was attributed to the Tycoon 2FA Defendants. Specifically, SpyCloud data has identified at least 261 user accounts associated with 92 Health-ISAC member organizations that were successfully phished by Tycoon 2FA Defendants. Two of these 92 member organizations are located within the Southern District of New York.

11. Microsoft does not have the ability to see the downstream effects of the observed phishing activity. For example, Microsoft cannot determine if a recipient of a phishing email opened the email, clicked on a link, or downloaded an attachment. Therefore, I provided this information to the impacted Health-ISAC organizations, so that they could investigate and remediate and update me as to what they learned. The additional information would allow me to investigate and verify whether anyone had opened the Tycoon 2FA phishing email and clicked on

[1] Microsoft and Health-ISAC collaborated with SpyCloud, a leading identity threat protection company, who provided victimology data.

the weaponized links or attachments, whether the attack resulted in credential theft or intrusion into the accounts, and whether the victim organization was subject to a ransomware or malware attack.

12. 15 of the 92 organizations provided me with additional information, which I used to validate the victimology information that Microsoft and SpyCloud provided. With each of the 15 organizations, there were multiple instances of both attempted phishing (that was ultimately blocked by the organization) and successful phishing. We know from the data provided by SpyCloud, at least 261 users clicked on malicious links in the Tycoon 2FA emails, were redirected to a Defendant-controlled phishing website, and provided their username/password credentials. Each of those 261 instances of credential theft represent an opportunity for the cybercriminals to launch further attacks such as ransomware, or business email compromise. Ultimately, at some point, the account compromise will be detected by the end user or information security team at the respective organization, requiring an incident response and investigation.

13. Through the malicious Tycoon 2FA domain information provided by Microsoft, I identified another 16 Health-ISAC member organizations that were targeted by the phishing attacks. I was able to confirm that these 16 member organizations were able to successfully block phishing emails associated with Tycoon 2FA in 148 instances, but in 62 instances, Tycoon 2FA phishing emails were delivered to employees of the member organizations.

14. In the instances where the phishing email was successfully delivered, 34 users clicked on the links contained in the Tycoon 2FA phishing emails, were redirected to the fraudulent Tycoon 2FA-controlled login pages, and 11 recipients of the phishing emails provided their credentials.

15. The credentials that the 11 recipients provided were successfully captured by Tycoon 2FA Defendants. Subsequently, the member organizations detected this activity and were able to lock the accounts to block any further malicious activity. Based on my 30 years of information security experiences, on average, I estimate that for each individual that gave up their credentials, the member organization had to expend significant time responding to these incidents, , including time from the response team, investigators, systems administrators, human resources (HR), company managers and individual employees.

16. When considering the incident response and remediation costs of these 261 attacks and the 11 cases of stolen credentials, Health-ISAC member organizations have incurred at least $326,400 in damages. Health-ISAC had incurred at least $24,000 in connection with its investigation and remediation efforts.

III. PHISHING ATTRIBUTED TO TYCOON 2FA WILL LIKELY ESCALATE TO OTHER CYBERCRIME

17. In general, ransomware is a form of malicious software (malware) designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Because a ransomware attack on a hospital can result in delayed medical procedures, disruption of life-saving surgeries, or taking the entire system offline, the consequences of these attacks can have devastating consequences and endanger people's lives.

18. Health-ISAC has been tracking ransomware attacks since 2020 and has identified over 30,000 incidents impacting all critical infrastructures listed in our database (as of December 2025). Of these, 1,935 attacks, or 6.5%, were in the health sector.

19. For the calendar year 2025, Health-ISAC observed 8,903 ransomware cases and 575 in the health sector. The total number of incidents in 2025 (8,903) surpassed that of 2024

(5,744) representing an increase of 55%. Health-sector-specific incidents also increased, but not as sharply, with 476 incidents in 2024 rising to 575 in 2025, for a 21% increase.

20. When hospitals get attacked by ransomware, critical IT systems become unavailable and hospital services decline rapidly.

21. In my experiences as Health-ISAC's Chief Security Officer since 2019, I am aware of the consequences of ransomware attacks on healthcare companies such as hospitals. I have personally investigated ransomware attacks that have caused the following harm:

- Ambulances forced to divert from hospitals;
- Delays in providing emergency patient services, delays or cancellation of providing treatments for cancer patients, delays in receiving lab results, delays in scheduling appointments;
- Hospitals forced to cancel elective procedures;
- Electronic Health Record systems being taken offline, which prevent hospitals, doctors, and providers from accessing any portion of the patient's electronic file.
- Malware and ransomware attacks that have crippled IT systems and led to the breach of sensitive health information; and
- Financial losses, including ransom payments to cybercriminals, legal fees, and regulatory fines.

22. Although I have observed attacks from the Tycoon 2FA Defendants on Health ISAC members, I have not yet observed subsequent ransomware or malware attacks that can be directly linked or attributed to the Tycoon 2FA Defendants. That does not mean that there is no risk of such attacks. Additionally, that the member organizations have been able to thwart further activity by locking down compromised accounts, does not mean that future compromised will be

similarly detected. Given that Tycoon 2FA Defendants have successfully captured credentials, it is inevitable that if allowed to continue, Tycoon 2FA will continue to launch their phishing attacks, some of those attacks will be undetected, and Tycoon 2FA Defendants will ultimately escalate to ransomware and malware attacks.

23. Additionally, according to DCU's investigation, Tycoon 2FA first emerged in August 2023 and has been expanding their cybercriminal operations since. Successful phishing attacks are a precursor to ransomware and malware attacks. Once the cybercriminal has successfully intruded into the system (such as when a Health-ISAC member organization's employee interacts with the link contained in the phishing email), it is not a question of if there will be subsequent attacks, it is a question of when. It is very common for cybercriminals to escalate from phishing to more crippling forms of cybercrime. Phishing attacks are a critical precursor to ransomware attacks in healthcare organizations because threat actors, like Tycoon 2FA Defendants, exploit human vulnerabilities to gain initial access to systems, which attackers can then leverage to deploy ransomware payloads. Unless Tycoon 2FA is stopped, consistent with the relief requested in Plaintiffs' Temporary Restraining Order, Tycoon 2FA Defendants will continue their attacks.

24. I understand, based on the collaboration and information sharing between Microsoft and Health-ISAC, that the Tycoon 2FA Defendants operate in a fashion similar to other threat actors that have been enjoined by U.S. federal courts such as the "RaccoonO365 Defendants" and the "Fake ONNX Defendants." Both sold do-it-yourself phishing kits and operated as a PhaaS. In November 2024, Microsoft filed a lawsuit in the Eastern District of Virginia and obtained injunctive relief effectively crippling Fake ONNX's cybercriminal operations. *See Microsoft Corporation and LF Projects LLC v. Abanoub Nady and John Does 1-*

4, Civil Action No. 1:24-cv-2013-RDA (E.D. VA. Nov. 12, 2024) (Alston, J.). Although Health-ISAC was not involved with this action, I am familiar with Microsoft's takedown of the Fake ONNX Defendants and understand that there are many operational and technical similarities between Fake ONNX and Tycoon 2FA Defendants and the phishing kits sold. In August 2025, Microsoft and Health-ISAC filed a lawsuit in the Southern District of New York and obtained injunctive relief, effectively crippling RaccoonO365's cybercriminal operation. *Microsoft and Health-ISAC v. Joshua Ogundipe and John Does 1-4*, 1:25-cv-07111 (S.D.N.Y. Aug. 2024) (Rakoff, J.). Based on my investigation into the RaccoonO365 and Tycoon 2FA, I am aware of the similarities between both operations.

IV. MALWARE AND RANSOMWARE ATTACKS CAUSE FURTHER IRREPARABLE HARM

25. Tycoon 2FA-branded phishing kits harm the brand reputation of Health-ISAC's member organizations. For example, given that Tycoon 2FA kits offer the ability to customize the phishing attacks to target specific victims, the emails that Tycoon 2FA Defendants send to Health-ISAC members are customized to appear as legitimate communications from or concerning the Health-ISAC member organization. Because Health-ISAC member organizations are under attack, they are forced to expend tremendous resources to defend themselves. When member organizations are attacked, their brand and reputation are irreparably harmed, because patients are no longer able to rely on their healthcare providers, including calling into question the trust, safety and security of patient data and the healthcare network system as a whole.

26. As a result of Defendants' attacks, Health-ISAC's member organizations have experienced harm to their brand and reputation. Given the amount of publicity that attacks on healthcare organizations receive, this reputational harm is significant. Additionally, member organizations that are victims of attack face a loss of goodwill, members of the public incorrectly

attribute the source of the emails to the member organizations (rather than attributing the harms to the malicious actors who are deploying Tycoon 2FA-branded phishing kits).

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

Executed this 24th day of February, 2026, in New York, New York.

Errol S. Weiss