

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

Microsoft Corporation, a Washington State
Corporation and Health-ISAC, Inc., a Florida
non-profit organization,

Plaintiffs,

- v. -

Saad Fridi,

and

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

Defendants.

Civil Action No. 26-cv-01603-DLC

**DECLARATION OF ANNA Z. SABER
IN SUPPORT OF PLAINTIFFS'
REQUEST FOR CLERK'S
CERTIFICATE OF DEFAULT**

I, Anna Z. Saber, declare as follow:

1. I am an attorney duly admitted to practice in the State of California, and admitted *pro hac vice* in connection with this matter. I am a Counsel at the law firm of Crowell & Moring LLP, counsel of record for the plaintiffs in this matter, Microsoft Corporation ("Microsoft") and Health-ISAC, Inc. (collectively, "Plaintiffs").

2. I submit this declaration pursuant to Rule 55(a) of the Federal Rules of Civil Procedure, in support of Plaintiffs' application for certificate of default against Defendants Saad Fridi and John Does 1-4 (collectively, "Tycoon 2FA Defendants"). I have personal knowledge of the facts set forth in this declaration and, if called to testify as a witness, could and would testify to the following under oath.

3. Upon information and belief, Tycoon 2FA Defendants are (1) not currently in the military service of the United States, and (2) neither minors nor incompetent persons under Rule 55.2(a)(1)(C) of the Local Civil Rules for the Southern District of New York. I base this

statement on the fact that Tycoon 2FA Defendants have engaged in sophisticated acts of phishing, computer intrusion, and theft of sensitive information from computer networks and have operated and procured sophisticated cybercrime infrastructure.

4. The Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331 and 28 U.S.C. § 1367(a).

5. The Court has personal jurisdiction over the Tycoon 2FA Defendants because the Tycoon 2FA Defendants have engaged in tortious conduct in New York, have committed tortious acts causing injury to persons and property in New York and have utilized instrumentalities located in the State of New York and the Southern District of New York to carry out acts alleged herein. As set forth in Plaintiffs' Complaint, Tycoon 2FA Defendants direct a significant amount of their cybercriminal activity to New York organizations and individuals. Dkt. No. 4, ¶¶ 27-28, 76.

6. This action was commenced on February 26, 2026, when Plaintiffs filed, under seal, a Complaint and Emergency Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause ("TRO Motion") (Dkt. Nos 4, 16).

7. On February 26, 2026, the Court granted Plaintiffs' application for issuance of a TRO and authorized alternative service upon the Tycoon 2FA Defendants, including by email and publication. Dkt. No. 31 at 11.

8. True and correct copies of the Summons, Complaint and the motion papers associated with Microsoft's TRO Motion were served upon Tycoon 2FA Defendants on March 6, 2026. *See* Dkt. No. 21 (Saber Declaration describing service), ¶¶ 5-11. On March 10, 2026, Plaintiffs submitted the declaration of Anna Z. Saber detailing Plaintiffs' service efforts. *Id.*

9. Consequently, pursuant to Federal Rule of Civil Procedure 12(a)(1)(A)(i), an

answer was due from Tycoon 2FA Defendants on or before March 27, 2026 (21 days after service). To date, Tycoon 2FA Defendants have not responded to or answered Plaintiffs' Complaint and the time for Tycoon 2FA Defendants to answer Plaintiffs' Complaint has expired.

10. This action seeks judgment against Tycoon 2FA Defendants for liability and for entry of a permanent injunction. Plaintiffs are not seeking recovery of damages or fees.

Defendants Have Not Responded To This Action

11. As described more fully below, Tycoon 2FA Defendants have been properly served with the Summons, Complaint, and all orders, pleadings and evidence in this action pursuant to the means that the Court expressly authorized in the Temporary Restraining Order (Dkt. 31) and Preliminary Injunction Order (Dkt. 32). The Tycoon 2FA Defendants have failed to appear or otherwise defend the action.

12. As of September 29, 2026, I have not been contacted by any of the Tycoon 2FA Defendants regarding this case, or with respect to any other matter. I have also conferred with members of the Microsoft's Digital Crime Unit ("DCU," which is the division of Microsoft responsible for protecting Microsoft and its customers against cybercrime threats, investigating such threats and identifying and attributing attacks) and Derek Richardson (the DCU investigator responsible for investigating Tycoon 2FA), who both submitted Declarations in support of Plaintiffs' TRO Application and Preliminary Injunctions. DCU confirms that neither Microsoft, nor any party associated with it, has been contacted by any of the Defendants regarding this case, or with respect to any other matter. Tycoon 2FA Defendants have not objected to the relief obtained in the Temporary Restraining Order, the Preliminary Injunction Order, or any other order issued by this Court. Defendants have not objected to or disputed any pleading, declaration, fact, evidence or submission in this case.

A. Service Of Process And Notice Upon Defendants

13. It is reasonable to conclude that Defendants are aware of this proceeding given the significant impact of the TRO and preliminary injunction, in combination with the steps Plaintiffs took to serve process by email and through publication, discussed below.

14. As set forth and reflected in Plaintiffs' request for TRO and request for preliminary injunction, following execution of these orders, Microsoft seized the subject domain names that Defendants owned, operated, and controlled to conduct their spear phishing operations, target victims, gain unauthorized access to their accounts and information, and exfiltrate sensitive information. As attested, this seizure mechanism was designed to interrupt Defendants' attacks by removing infrastructure used to deceive victims of phishing emails and severing communications between the infected operating systems and devices of victims and the Defendants. *See* Declaration of Derek Richardson in support of Plaintiffs' Applications For An Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction (Dkt. No. 18), ¶¶ 56-64. This effectively interrupted Defendants' attacks by severing communications between their technical control center and the victims of their phishing activities. *Id.* Based on this disruption and impact on Defendants' infrastructure, I conclude that Defendants are very likely aware of the impact of the relief granted through the course of this action, and aware that the instant proceeding is the cause of that impact.

15. Additionally, in connection with effectuating the TRO and preliminary injunctions and effecting a transfer of the domains, the registries that administer the domains informed me that they had notified the impacted registrars of the transfer and advised the registrars that any future questions would be directed to counsel for Plaintiffs. In other words, in the event that the prior registrant (*i.e.*, the prior owner) of the domain had questions about why their domain was taken down, their questions would ultimately be directed to Plaintiffs' counsel.

To date, Plaintiffs' counsel have not received any correspondence from anyone claiming that their domain was improperly taken down. Nor have the registries or registrars alerted us to any user complaints or questions.

B. Service By Email

16. Plaintiffs have served process through email, as authorized by the TRO and Preliminary Injunction Order. The Court has authorized service by email, as follows: "the Complaint may be served by any means authorized by law, including (1) transmission by email . . . to the contact information provided by Defendants to Defendants' domain registrars and/or hosting companies and as agreed to by Defendants in the domain registration and/or hosting agreements." Dkt. No. 31 at 11.

17. On March 6, 2026, consistent with the TRO, I served copies of the Summons, Complaint and Plaintiffs' TRO Application upon the registrant emails identified in Appendix A to the Complaint. The service email contained the following language:

Plaintiffs Microsoft Corporation ("Microsoft") and Health-ISAC have sued Defendants Saad Fridi and John Does 1-4 associated with the Tycoon 2FA cybercriminal operation and domains listed in the documents set forth herein. You are receiving this email because you are the registrant of a domain that Tycoon 2FA Defendants use as part of their cybercriminal operation, and accordingly we have reason to believe that you are part of the cybercriminal operation and have violated federal and state law.

Plaintiffs allege that the Tycoon 2FA Defendants have violated federal and state law by hosting a cybercriminal operation through these domains and selling, distributing, purchasing, and utilizing the Tycoon 2FA phishing kits that support a Phishing-as-a-Service enterprise. The phishing kits made and sold by the Tycoon 2FA Defendants facilitate sophisticated spear phishing and are designed to steal sensitive information that is then used to perpetrate additional cybercrimes including business email compromise, financial fraud, and ransomware attacks. Tycoon 2FA Defendants have also committed intellectual property violations irreparably harming Plaintiffs' customers and member organizations. Plaintiffs seek a preliminary injunction directing the registrars associated with these domains to take all steps necessary to disable access to and operation of these domains and that all content and material associated with these domains are to be isolated and preserved pending resolution of the dispute. Plaintiffs seek a permanent injunction, other equitable relief and damages. Full copies of the pleading documents are available at www.noticeofpleadings.com/Tycoon2FA.

NOTICE TO DEFENDANT: READ THESE PAPERS CAREFULLY! You must “appear” in this case or the other side will win automatically. To “appear” you must file with the court a legal document called a “motion” or “answer.” The “motion” or “answer” must be given to the court clerk or administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on the Plaintiffs’ attorneys, Jeffrey L. Poston at Crowell & Moring LLP, 1001 Pennsylvania Avenue NW, Washington D.C. 20004, jposton@crowell.com. If you have questions, you should consult with your own attorney immediately.

NOTICE TO DEFENDANTS: The Court has ORDERED that the Show Cause Hearing re Plaintiffs’ Motion for Preliminary Injunction will be SCHEDULED for March 13, 2026 at 10:30 a.m. in Courtroom 18B at the Daniel Patrick Moynihan Courthouse in the Southern District of New York before Judge Denise L. Cote.

18. In connection with sending the service email to the registrant emails as identified in Appendix A, I used Readnotify.com to track the email correspondence. By appending “.readnotify.com” to the end of each of the registrant’s emails, I was able to track the correspondence, including when the email was received and when it was opened (to the extent the recipient opens the email). I have reviewed the ReadNotify.com records, and have confirmed that successful delivery (*i.e.*, no bounce back) of the emails and have confirmed that in many instances the service email was opened by the recipient.

19. Despite this robust notice and service, the Tycoon 2FA Defendants have not contacted me, anyone at my firm, Plaintiffs Microsoft or Health-ISAC, nor have they otherwise appeared, objected to or disputed any pleading, declaration, fact, evidence or submission in this case.

C. Service By Internet Publication

20. Plaintiffs have served process by Internet publication, as authorized by the TRO and Preliminary Injunction Order. The Court has authorized service by Internet publication, as follows: “the Complaint may be served by any means authorized by law, including . . . publishing notice on a publicly available Internet website.” Dkt. No. 31 at p. 10.

21. On March 4, 2026, the “Notice of Pleadings” website, which is hosted by Crowell & Moring, went live. This website contains copies of the pleadings filed in this case to date, including all Orders issued by this Court, and information regarding the preliminary injunction hearing. I visited the Notice of Pleadings website and confirmed that all the posted documents were in fact accessible to the public. A true and accurate copy of the homepage for <https://noticeofpleadings.com/tycoon2FA/> is attached to my declaration as **Exhibit 1**. I receive regular updates from Crowell IT department regarding internet traffic to the Notice of Pleadings website. To date, I have received no indication that any of the Tycoon 2FA Defendants have attempted contact or to respond via the Notice of Pleadings website.

22. The Notice of Pleadings website contains the case caption as well as the following language:

Plaintiffs Microsoft Corporation (“Microsoft”) and Health-ISAC have sued Defendants Saad Fridi and John Does 1-4 associated with the Tycoon 2FA cybercriminal operation and domains listed in the documents set forth herein. Plaintiffs allege that the Tycoon 2FA Defendants have violated federal and state law by hosting a cybercriminal operation through these domains and selling, distributing, purchasing, and utilizing the Tycoon 2FA phishing kits that support a Phishing-as-a-Service enterprise. The phishing kits made and sold by the Tycoon 2FA Defendants facilitate sophisticated spear phishing and are designed to steal sensitive information that is then used to perpetrate additional cybercrimes including business email compromise, financial fraud, and ransomware attacks. Tycoon 2FA Defendants have also committed intellectual property violations irreparably harming Plaintiffs’ customers and member organizations. Plaintiffs seek a preliminary injunction directing the registrars associated with these domains to take all steps necessary to disable access to and operation of these domains and that all content and material associated with these domains are to be isolated and preserved pending resolution of the dispute. Plaintiffs seek a permanent injunction, other equitable relief and damages. Full copies of the pleading documents are available at www.noticeofpleadings.com/Tycoon2FA.

NOTICE TO DEFENDANT: READ THESE PAPERS CAREFULLY! You must “appear” in this case or the other side will win automatically. To “appear” you must file with the court a legal document called a “motion” or “answer.” The “motion” or “answer” must be given to the court clerk or administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on the Plaintiffs’ attorneys, Jeffrey L. Poston at Crowell & Moring LLP, 1001 Pennsylvania Avenue NW, Washington D.C. 20004, jposton@crowell.com. If you have questions, you should consult with your own attorney immediately.

NOTICE TO DEFENDANTS: The Court has ORDERED that the Show Cause Hearing re Plaintiffs’ Motion for Preliminary Injunction will be SCHEDULED for March 13, 2026 at 10:30 a.m. in Courtroom 18B at the Daniel Patrick Moynihan Courthouse in the Southern District of New York before Judge Denise L. Cote.

23. Following execution of the TRO and the unsealing of the record in this action, Plaintiffs also engaged in widespread press relations and media activity announcing this action. See Steven Masada, Defending the gates: How a global coalition disrupted Tycoon 2FA, a major driver of initial access and large-scale online impersonation, *Microsoft Blog*, available at <https://blogs.microsoft.com/on-the-issues/2026/03/04/how-a-global-coalition-disrupted-tycoon/> (Mar. 4, 2026).¹ Microsoft included a link to www.noticeofpleadings.com/Tycoon2FA in

¹ In addition to Microsoft’s own publication, other news outlets published their own reports regarding this takedown.

connection with its press release, and shared this link with other news publications. To the extent that Tycoon 2FA Defendants were made aware of the action via Microsoft's media activity or third-party news publications, Tycoon 2FA Defendants would have been able to access the Notice of Pleadings website and access the pleadings.

24. Additionally, if the public or Tycoon 2FA Defendants visited the URL of the seized domains, they were shown the following page, alerting them to this action and directing them to the Notice of Pleading page.



D. Attempted Notice And Service By Mail Or Personal Delivery

See, e.g., Christopher Boyton, Mayra Rosario Fuentes, Stephen Hilt, Europol, Microsoft, TrendAI™ and Collaborators Halt Tycoon 2FA Operations, *TrendMicro*, available at <https://www.trendaisecurity.com/en-us/resources-insights/trendai-security-blog/tycoon2fa-takedown> (Mar. 4, 2026); Press Release, Global phishing-as-a-service platform taken down in coordinated public private action, *Europol Newsroom*, available at <https://www.europol.europa.eu/media-press/newsroom/news/global-phishing-service-platform-taken-down-in-coordinated-public-private-action> (Mar. 4, 2026); Angus Loten, Microsoft Helps Bust Global Hacking Service, *The Wall Street Journal*, available at https://www.wsj.com/articles/microsoft-helps-bust-global-hacking-service-2d1a4bbc?gaa_at=eafs&gaa_n=AWetsqeszx8880GCg3NcNAOi_pNRUSTN4Dn3retTiAnJCc6E0NUh7bvrw2NYYXZAIQ%3D&gaa_ts=69af0ab9&gaa_sig=FvRvvrgmiQONf0rCof72FLPjOBu2vZIS6orcg4wPUBzE9fkQwNI_HuONwXOnYFMXdkRrIhkUmm0MayEtuERGA%3D%3D&mg=pr_od/com-wsj (Mar. 4, 2026).

25. To the extent that the records included physical addresses purportedly associated with the registrants of the Tycoon 2FA domains, I have investigated these addresses, and have concluded that these addresses reflected: (1) incomplete addresses, such as only the names of cities without further detail, (2) addresses that are artificial and do not exist at all, (3) street names that exist but not do properly correlate with other address information and/or are associated with individuals or companies that do not exist, and (4) city names that are not properly correlated with the listed country or which combine elements of different cities in different countries.

26. From the foregoing, I conclude that the email addresses associated with the domain names, and which are described further above, are the most reliable way to communicate with the Defendants in this action. As noted above, Defendants provided these email addresses when registering the domain names used in the infrastructure of their cybercrime operations, making it likely that Defendants monitor messages sent to those addresses.

E. Plaintiffs Have Been Unsuccessful in Investigating The Identities of the Remaining Doe Defendants, Which Leaves Service Via Email the Best Means to Serve Process in This Case

27. Although Plaintiffs are aware that Saad Fridi (the named Defendant) is located in Pakistan, they have not been able to determine a more specific location that would allow for direct service. Additionally, for Doe Defendants 1-4, Plaintiff have endeavored to identify additional contact information through which Defendants could be served, as well as more specific identities. Through discovery efforts, Plaintiffs have sought from the U.S.-based domain registrars seeking account information, identifying information, payment information, device information, and communications with the account holders in an effort to obtain additional information regarding Defendants' identities. Given the information provided by the third-party registers and Plaintiffs' analysis of the information provided, Plaintiffs have not been able to

identify the Defendants with greater particularity.

28. Based on (a) Defendants’ use of aliases and false information; (b) use of anonymous proxy computers or anonymization networks to create and maintain the infrastructure at issue in the case; (c) the absence of or limitations on the ability to carry out U.S.-style civil discovery outside of the U.S.; (d) the ease with which anonymous activities can be carried out through the Internet; and (e) Defendants’ sophisticated use of tools to conceal more specific indicia of their identities or further contact information, I have been unable to specifically and definitively determine Defendants’ “real” names and physical addresses at which they might be served by personal service.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge. Executed on this 30th day of September, 2026 in San Francisco, California.

A handwritten signature in black ink, appearing to read "Anna Z. Saber", is written over a horizontal line.

Anna Z. Saber