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. -

Joshua Ogundipe,

and

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

Defendants.

Civil Action No. 25-cv-07111-JSR

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 certification of default against Defendants Joshua Ogundipe and John Does 1-4 (collectively, "RaccoonO365 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, RaccoonO365 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 conclusion on the fact that RaccoonO365 Defendants have engaged in sophisticated acts of

spear-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 based upon 28 U.S.C. § 1331 and 28 U.S.C. § 1367(a).

5. The Court has personal jurisdiction over the RaccoonO365 Defendants because the RaccoonO365 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. RaccoonO365 Defendants direct a significant amount of their cybercriminal activity to New York organizations and individuals.

6. This action was initiated on August 27, 2025 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 9, 11).

7. On August 27, 2025, the Court granted Plaintiffs' application for issuance of a TRO and authorized alternative service upon the RaccoonO365 Defendants, including by email and publication. Dkt. No. 21 at 11.

8. True and correct copies of the Summons, Complaint and the motion papers associated with Microsoft's TRO Motion were served upon RaccoonO365 Defendants on September 16, 2025. *See* Dkt. No. 28 (Saber Decl. describing service) ¶¶ 5-11. On September 23, 2025, 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 RaccoonO365 Defendants on or before October 7, 2025. To date,

RaccoonO365 Defendants have not responded to or answered Plaintiffs' Complaint and the time for RaccoonO365 Defendants to answer Plaintiffs' Complaint has expired.

10. This action seeks judgment against RaccoonO365 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, RaccoonO365 Defendants have been properly served with the Summons, Complaint, and all orders, pleadings and evidence in this action pursuant to the means which the Court expressly authorized in the Temporary Restraining Order (Dkt. 21) and Preliminary Injunction Order (Dkt. 32). The RaccoonO365 Defendants have failed to appear or otherwise defend the action.

12. As of April 1, 2026, I have not been contacted by any of the RaccoonO365 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 Jason Lyon and Nick Monaco (the DCU investigators responsible for to investigating RaccoonO365), 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. O. RaccoonO365 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 operation, target victims, gain unauthorized access to their accounts and information, and exfiltrate sensitive information. As attested, this 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 Jason B. Lyons in support of Plaintiffs' Applications For An Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction (Dkt. No. 17), ¶¶ 67-76. This effectively interrupted Defendants' attacks by severing communications between their technical control center and the victims of their phishing activities. 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. Indeed, following the seizure of the domains, the RaccoonO365 Defendants communicated to their users via the Telegram channel that a Microsoft legal action was responsible for the disruption of the RaccoonO365 infrastructure. Dkt. 28 ¶¶ 12-13.

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 (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. 21 at 11.

17. On September 16, 2025, 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 Joshua Ogundipe and John Does 1-4 associated with the RaccoonO365 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 RaccoonO365 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 RaccoonO365 Defendants have violated federal and state law by hosting a cybercriminal operation through these domains and selling, distributing, purchasing, and implementing the "RaccoonO365"-branded phishing kits that support a Phishing-as-a-Service enterprise. The phishing kits made and sold by the RaccoonO365 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. RaccoonO365 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/RaccoonO365.

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 September 24, 2025 at 2:00 p.m. in Courtroom 14B at the Daniel Patrick Moynihan Courthouse in the Southern District of New York before Judge Jed S. Rakoff.

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. Some of the registrant emails listed in Appendix A are proxy emails provided by the registrar. An example of this is "contact@idcprivacy.com." In emailing this address, I received instructions from IDCPrivacy providing the steps to obtain a temporary one-time use email that I would be able to use to email the registrant of a particular domain. I followed these steps, and emailed the one-time-use registrant email with a copy of the same documents described in Paragraph 18, *supra*, and used the same language described above. I also used

ReadNotify.com in connection with these emails.

20. Despite this robust notice and service, the RaccoonO365 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

21. 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. 21 at p. 10.

22. On September 16, 2025, 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 www.noticeofpleadings.com/RaccoonO365 is attached to my declaration as **Exhibit 1.**

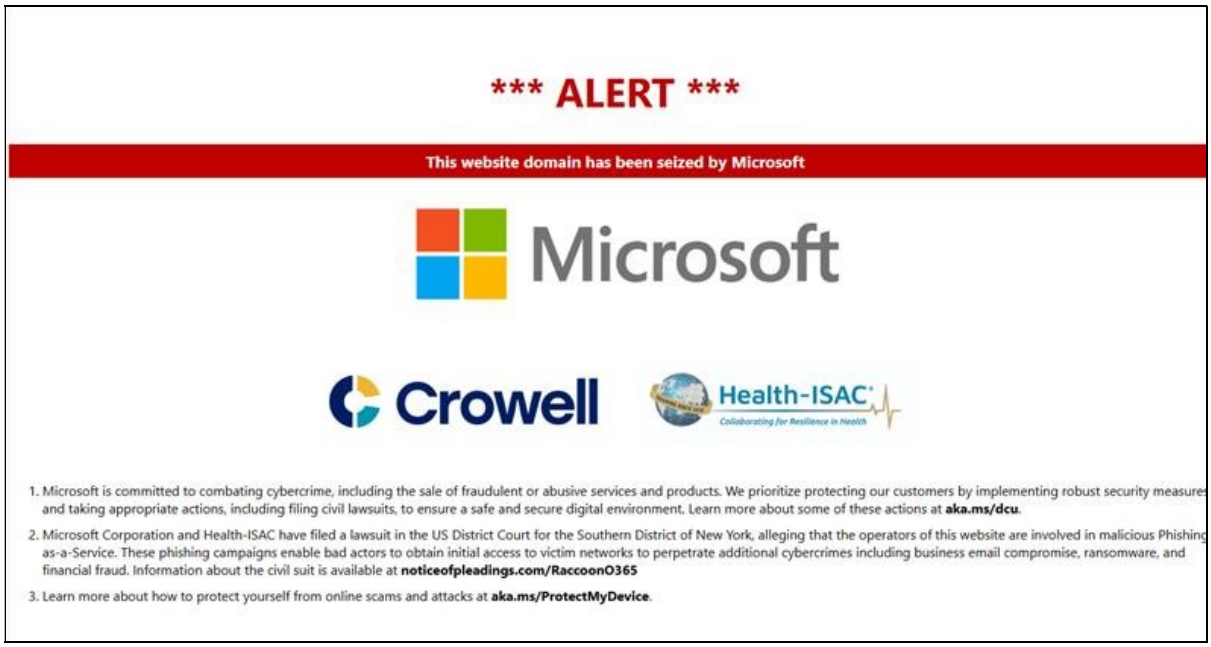
23. The Notice of Pleadings website contains the case caption as well as the following language:

> Plaintiffs Microsoft Corporation ("Microsoft") and Health-ISAC have sued Defendants Joshua Ogundipe and John Does 1-4 associated with the RaccoonO365 cybercriminal operation and domains listed in the documents set forth herein. Plaintiffs allege that the RaccoonO365 Defendants have violated federal and state law by hosting a cybercriminal operation through these domains and selling, distributing, purchasing, and implementing the "RaccoonO365"-branded phishing kits that support a Phishing-as-a-Service enterprise. The phishing kits made and sold by the RaccoonO365 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. RaccoonO365 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/RaccoonO365.
>
> 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 September 24, 2025 at 2:00 p.m. in Courtroom 14B at the Daniel Patrick Moynihan Courthouse in the Southern District of New York before Judge Jed S. Rakoff.

24. 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, *Microsoft seized 338 websites to disrupt rapidly growing 'Raccoon O365' phishing service*, Microsoft Blog, available at https://blogs.microsoft.com/on-the-issues/2025/09/16/microsoft-seizes-338-websites-to-disrupt-rapidly-growing-raccoono365-phishing-service/ (Sept. 16, 2025).[1] Microsoft included a link to the Notice of Pleadings website in connection with its press release, and shared this link with other news publications. To the extent that RaccoonO365 Defendants were made aware of the action via Microsoft's media activity or third-party news publications, RaccoonO365 Defendants were able to access the Notice of Pleadings website and access the pleadings.

25. Additionally, if the public or RaccoonO365 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.

[1] *See also* Ravie Lakshmana, *RaccoonO365 Phishing Network Dismantled as Microsoft, Cloudflare Take Down 338 Domains*, The Hacker News, available at https://thehackernews.com/2025/09/raccoono365-phishing-network-shut-down.html (Sept. 17, 2025); *Threat Brief – Cloudflare participates in global operations to disrupt RaccoonO365*, available at https://www.cloudflare.com/en-in/threat-intelligence/research/report/cloudflare-participates-in-global-operation-to-disrupt-raccoono365/ (Sept. 10, 2025).



D. Attempted Notice And Service By Mail Or Personal Delivery

26. To the extent that the records obtained in response to the third-party subpoenas included physical addresses purportedly associated with the registrants of the RaccoonO365 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.

27. 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 Made Substantial but Unsuccessful Efforts to Discover and Investigate Defendants' Particular Identities, Which Leaves Service Via Email the Best Means to Serve Process in This Case

28. On behalf of Plaintiffs, I endeavored to identify additional contact information through which Defendants could be served, as well as more specific identities. I served subpoenas upon 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.

29. Based on my review of the responses and documents provided by these registrars, as well as Microsoft's technical analysis of the information provided, Microsoft has not been able to identify Defendants with any greater particularity through the subpoena responses.

30. 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 1st day of April, 2026 in San Francisco, California.

Anna Z. Saber