

**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

[PROPOSED] ORDER AND JUDGMENT

This action having been commenced on August 27, 2025 by the filing of the Summons and Complaint, together with the filing of additional materials in support of Plaintiff Microsoft Corporation's ("Microsoft") and Plaintiff Health-ISAC, Inc.'s ("Health-ISAC") Ex Parte Application for an Emergency Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction (the "TRO Motion"); and copies of the Summons, Complaint and Plaintiffs' papers in support of their TRO Motion having been served on Defendants Joshua Ogundipe and John Does 1-4 on August 27, 2025 via e-mail and publication, as expressly authorized by this Court, and proof of service having been filed on September 23, 2025, and the Defendants not having answered the Complaint, and the time for answering the Complaint having expired;

And this matter having come before the Court on Plaintiffs Microsoft Corporation's ("Microsoft") and Health-ISAC, Inc.'s ("Health-ISAC") Motion for Default Judgment and Permanent Injunction. Plaintiffs have established the elements of their claims pursuant to: (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962; (3) Conspiracy to Violate the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(d); (4) the Electronic Communications Privacy Act, 18 U.S.C. § 2701; (5) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (6) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 et seq.; (7) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); (8) common law trespass to chattels; (9) conversion; and (10) unjust enrichment. Defendants have failed to appear, plead, or otherwise defend this action. Plaintiffs are entitled to default judgment under Fed. R. Civ. P. 55(b) and a permanent injunction pursuant to Fed. R. Civ. P. 65, the Lanham Act, and the All-Writs Act; it is ORDERED, ADJUDGED and DECREED as follows:

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiffs' Motion for Default Judgment and Permanent Injunction, the Court hereby makes the following findings of fact and conclusions of law:

1. Defendants Ogundipe and John Does 1-4 were properly served with Plaintiffs' Complaint and other pleadings in this action and were provided with adequate notice of this action through means authorized by law, satisfying Due Process, satisfying Fed. R. Civ. P. 4 and reasonably calculated to provide Defendants with notice. Specifically, Defendants have been served via e-mail at e-mail addresses associated with infrastructure used by Defendants to carry out the activity that is the subject of the complaint and by publication on the public website

<https://noticeofpleadings.com/raccoono365/>.

2. Defendants failed to appear, plead, or otherwise defend against the action.

3. The time for responding to Plaintiffs' Complaint was 21 days from service of the complaint, and more than 21 days have elapsed since Plaintiffs effected service. The Clerk entered default pursuant to Fed. R. Civ. P. 55(a) against Defendants for failing to appear after being properly provided notice of the proceedings under Fed. R. Civ. P. 4(f)(3) on April 3, 2026. *See* Dkt. No. 38.

4. This Court has jurisdiction over the subject matter of this case and venue is proper in this judicial district.

5. Plaintiffs are entitled to entry of judgment and a permanent injunction against Defendants.

6. The evidence of record indicates that no Defendant is an infant or incompetent.

7. Plaintiffs have established that RaccoonO365 Defendants manufacture and sell illegal phishing kits deceptively branded as "RaccoonO365," designed to steal sensitive information and perpetrate business email compromise, ransomware, and financial fraud against Microsoft customers, Health-ISAC member organizations, and the public.

8. Plaintiff have established that that RaccoonO365 Defendants targeted Microsoft's customers, Health-ISAC member organizations, and the general public. RaccoonO365 Defendants manufactured, sold, and facilitated the deployment of pre-packaged sets of tools ("phishing kits") that enable other cybercriminals to launch phishing attacks with relative ease. This business model of selling phishing kits and services for use by other cybercriminals is also referred to as "Phishing-as-a-Service" or "PhaaS."

9. Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962; (3) Conspiracy to Violate the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(d); (4) The Electronic Communications Privacy Act, 18 U.S.C. § 2701; (5) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (6) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.*; (7) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); (8) common law trespass to chattels; (9) conversion; and (10) unjust enrichment.

10. Microsoft owns the registered trademarks Microsoft®, Windows®, Microsoft 365®, Office365®, Office®, Microsoft Office®, SharePoint®, OneDrive®, Outlook®, and Azure® and numerous other trademarks used in connection with its services, software and products.

11. Health-ISAC is a membership organization comprised of public and private hospitals, ambulatory providers, health insurance payers, pharmaceutical/biotech manufacturers, laboratories, diagnostic, medical device manufacturers, medical schools, medical R&D organizations and other relevant health sector stakeholders. Health-ISAC represents the interests of its healthcare industry members in combating and defending against cyber threats that pose risk and loss to the industry.

12. Plaintiffs have established that RaccoonO365 Defendants have engaged in violations of the foregoing law by:

- a. Intentionally accessing the protected computers and computer networks of Microsoft and the customers of Microsoft, without authorization or exceeding authorization, in order to steal and exfiltrate information from those computers and computer networks;
- b. Engaging in phishing operations to steal credentials from unsuspecting victims who are tricked into believing they are accessing legitimate websites;

- c. Developing mechanisms to circumvent technological security protocols;
- d. Intentionally accessing, without authorization, the email inboxes of Microsoft customers, to support credentials theft, information exfiltration, and subsequent end-user terminal attacks which include business email compromise, ransomware, and financial fraud;
- e. Operating a Racketeering Enterprise by leveraging each other's work to: (i) create, distribute, and operate the phishing technical infrastructure, (ii) sell, distribute, and use RaccoonO365 branded phishing kits, (iii) to steal credentials from victims, and (iv) gain access to victim computers to further additional criminal activities like financial fraud, business email compromise, and deploying ransomware.
- f. Infringing the protected marks of Plaintiffs for the purpose of causing confusion or mistake, whereby the victims of RaccoonO365 Defendants' attacks mistakenly associate such conduct with Plaintiffs.

13. Plaintiffs have established that unless Defendants are permanently restrained and enjoined and unless final relief is ordered to prevent Defendants from maintaining the registration of domains for such prohibited and unlawful purposes, that Defendants are likely to continue the foregoing conduct and to engage in the illegal conduct enjoined by the Preliminary Injunction.

14. There is good cause to believe that, unless Defendants are permanently restrained and enjoined and unless further relief is ordered to expeditiously prevent Defendants from maintaining the registration of domains for purposes enjoined by the Preliminary Injunction, immediate and irreparable harm will result to Microsoft, Microsoft's customers, Health-ISAC, its member organizations, and to the public, from Defendants' ongoing violations.

15. Plaintiffs have established that RaccoonO365 Defendants have operated their phishing operations through certain instrumentalities – specifically through the website domains identified in **Appendix A**. Plaintiffs have established that to halt the injury caused by Defendants, they must be prohibited from using domains, as set forth below. The hardship to Microsoft, its customers, Health-ISAC, and its member organizations that will result if a permanent injunction

does not issue weighs in favor of an injunction. Defendants will suffer no cognizable injury as a result of being enjoined from further illegal conduct.

16. There is good cause to permit notice of the instant Order and further orders of the court by formal and alternative means. The following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order: (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain registrars and hosting companies and (2) publishing notice on the publicly available website <https://noticeofpleadings.com/raccoono365/>.

FINAL JUDGMENT AND PERMANENT INJUNCTION

IT IS THEREFORE ORDERED that Defendants are in default and in accordance with Fed. R. Civ. P. 65(b) and 53(a)(1)(C), 15 U.S.C. § 1116(a), and 28 U.S.C. § 1651(a) and the court's inherent equitable authority, good cause and the interests of justice, Plaintiffs' Motion for Default Judgment and Permanent Injunction is Granted; and

IT IS HEREBY ORDERED, ADJUDGED AND DECREED that judgment is awarded in favor of Plaintiffs and against Defendants and that Plaintiffs have judgment against Defendants as demanded in the Complaint, including but not limited to the issuance of permanent injunctive relief enjoining Defendants from engaging in any of the wrongful activity set forth in the Complaint; and

IT IS FURTHER ORDERED that RaccoonO365 Defendants, their representatives, and persons who are in active concert or participation with RaccoonO365 Defendants and associated criminal operation, are permanently restrained and enjoined from: (1) intentionally accessing the protected computers without authorization, (2) engaging in phishing campaigns, (3) stealing

credentials from victims of phishing campaigns, (4) using the credentials to access the email inboxes of victims, (4) unlawfully accessing, viewing, exfiltrating, or otherwise stealing the contents of the compromised email inboxes, (5) capitalizing on the trademarks of Plaintiffs to fabricate legitimacy of the phishing campaign, (6) misappropriating that which rightfully belongs to Microsoft, its customers, or in which Microsoft or its customers have a proprietary interest; (7) destroying the goodwill and reputation of Plaintiffs, (8) impersonating Plaintiffs, their systems, products, and services, (9) configuring, deploying, operating, or otherwise participating in or facilitating infrastructure described in the TRO Application, including but not limited to the Internet domains set forth in **Appendix A** and through any other component or element of RaccoonO365 Defendants' illegal infrastructure at any location, including infrastructure RaccoonO365 Defendants may attempt to rebuild, and (10) undertaking any similar activity that inflicts harm on Microsoft, Microsoft's customers, Health-ISAC member organizations, or the public.

IT IS FURTHER ORDERED that RaccoonO365 Defendants, their representatives, and persons who are in active concert or participation with RaccoonO365 Defendants and associated criminal operation are permanently restrained and enjoined from (1) using and infringing Plaintiffs' trademarks, including specifically Microsoft's registered trademarks Microsoft®, Windows®, Microsoft 365®, Office365®, Office®, Microsoft Office®, SharePoint®, OneDrive®, Outlook®, and Azure®, and/or other trademarks, trade names, service marks, or Internet domain addresses or names containing or infringing such trademarks, trade names or service marks, as set forth in **Appendix B** to the Complaint; (2) using in connection with RaccoonO365 Defendants' activities, products, or services any false or deceptive designation, representation or description of RaccoonO365 Defendants or of their activities, whether by

symbols, words, designs or statements, which would damage or injure Plaintiffs or give RaccoonO365 Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that RaccoonO365 Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Plaintiffs, or passing off RaccoonO365 Defendants' activities, products or services as Plaintiffs'.

IT IS FURTHER ORDERED that Defendants shall forfeit ownership and control of all domains used to carry out the activities enjoined herein, including the domains identified at Appendix A. With respect to any currently registered Internet domains set forth in **Appendix A** to this Order, the domain registries located in the United States shall take the following actions:

A. Within **three (3) business days** of receipt of this Order, shall unlock and change the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. To the extent the registrar of record does not assist in changing the registrar of record for the domain under its control, the domain registry for the domain, or its administrators, including backend registry operators or administrators, within three (3) business days of receipt of this Order, shall change, or assist in changing, the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. The purpose of this paragraph is to ensure that Microsoft has control over the hosting and administration of the domain in its registrar account at MarkMonitor or such other registrar specified by Microsoft. Microsoft shall provide to the domain registry or registrar of record any requested information or account details necessary to effectuate the foregoing.

B. The domain registries shall be made active and shall resolve in the manner set forth in this order, or as otherwise specified by Microsoft, upon taking control of the domain.

C. The domain registries shall take reasonable steps to work with Microsoft to ensure the transfer of the domain and to ensure that RaccoonO365 Defendants cannot use it to make unauthorized access to computers, infect computers, compromise computers and computer networks, monitor the owners and users of computers and computer networks, steal information from them, or engage in any other activities prohibited by this Order;

D. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following, or other information as may be specified by Microsoft:

Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
United States
Phone: +1.4258828080
Facsimile: +1.4259367329
domains@microsoft.com
Name Server Information: ns2246a.microsoftinternetsafety.net,
ns2246b.microsoftinternetsafety.net

E. Prevent transfer, modification or deletion of the domain by RaccoonO365 Defendants and prevent transfer or control of the domain to the account of any party other than Microsoft;

F. Take all steps required to propagate the foregoing changes through the Domain Name System (“DNS”), including domain registrars.

With regard to the domain registries and registrars located outside of the United States, the Court respectfully requests, but does not order, that they take the same or substantially similar actions as the foregoing so as to neutralize the threat posed by RaccoonO365 Defendants to the citizens of all countries, including their own. RaccoonO365 Defendants, their representatives and persons who are in active concert or participation with them are ordered to consent to whatever

actions are necessary for non-United States registries, registrars and registrants or hosts, set forth in **Appendix A** to this Order, to effectuate this request.

IT IS FURTHER ORDERED that copies of this Order may be served by any means authorized by law, including (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by RaccoonO365 Defendants to their domain registrars and/or hosting companies and as agreed to by RaccoonO365 Defendants in the domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent RaccoonO365 Defendants provided accurate contact information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon RaccoonO365 Defendants, to the extent they provided accurate contact information in foreign countries that are signatories to such treaties.

IT IS SO ORDERED

Entered this ____ day of May, 2026

HON. JED S. RAKOFF
UNITED STATES DISTRICT JUDGE

This document was entered on the docket
on _____, 2026.