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.	**Case No.** **FILED UNDER SEAL** **PURSUANT TO LOCAL RULE 5**

COMPLAINT

Plaintiff Microsoft Corporation ("Microsoft") and Health-ISAC, Inc. ("Health-ISAC") (collectively "Plaintiffs"), by their attorneys, bring this action against Saad Fridi and John Does 1-4 (collectively "Tycoon 2FA Defendants"), who manufacture and sell illegal "phishing" kits, designed to steal sensitive information and perpetrate business email compromise, ransomware, and financial fraud against Microsoft customers, including Plaintiff Health-ISAC, and the public. Microsoft asserts claims based on (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.

Plaintiffs allege as follows:

NATURE OF THE ACTION

1. American companies are besieged daily by cybercriminals seeking to infiltrate or disrupt the vital technologies necessary for these businesses to operate, maintain and protect their confidential information, and communicate both internally and to the public. These cybercriminals target reputable organizations to steal and then leverage or sell their confidential information to commit further cybercrimes.

2. This action involves the relentless and persistent phishing attacks conducted and facilitated by a foreign cybercrime organization designated as "Tycoon 2FA Defendants," against Microsoft, its customers, including Plaintiff Health-ISAC, and the public, seeking to steal confidential personal and business information to compromise these businesses and perpetrate additional cybercrimes. Since 2023, Tycoon 2FA Defendants have been responsible for at least 96,000 successfully phished credentials globally and at least 55,000 successfully phished credentials in the United States (this number is reflective of all Tycoon 2FA activity, and isnot limited to Microsoft customers and represents validated instances where a victim was phished using the Tycoon 2FA phishing kit and were deceived to provide their login credentials).[1]

3. One of the most pernicious forms of cybercrime is known as "phishing," which entails luring online victims to open weaponized emails and attachments by tricking them to believe the emails come from a trusted and legitimate source.[2] Tycoon 2FA Defendants

[1] Microsoft collaborated with SpyCloud, a leading identity threat protection company, who provided this victimology data.

[2] The estimated financial impact of phishing in 2024 is over $3.5 billion US. Microsoft, *Microsoft Digital Defense Report 2024*, at p. 34, available at https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf (Oct. 2024) ("2024 *MDDR*").

manufacture, sell, and facilitate the deployment of pre-packaged phishing kits that enable other cybercriminals to launch phishing attacks with relative ease.

4. This action seeks to take down this technical infrastructure, render Tycoon 2FA Defendants incapable of continuing their attacks, and to transfer ownership and control of these domains to Microsoft.

5. The Tycoon 2FA Defendants develop, advertise, and sell Microsoft branded phishing kits (*i.e.*, kits that are advertised as being able to infiltrate Microsoft systems[3] and phish Microsoft customers)[4] to other cybercriminals, who use these kits to tailor their attacks to specific Microsoft customers using specialized messages and "subject" lines as bait. A cybercriminal can purchase the phishing kit that best serves its criminal objective, including selecting which companies' products and systems it wishes to infiltrate and the lure it wants to use. Tycoon 2FA targets Microsoft because it is a high-value, high-volume target, particularly due to Microsoft's enterprise customers (customers who are businesses or large organizations, rather than individual subscriptions). Microsoft has determined that approximately 87% of Defendants' attacks are directed at enterprise customers; the remaining 13% of the attacks are aimed at individual subscribers.

6. Tycoon 2FA's business model of selling phishing kits and services for use by other cybercriminals is also referred to as "Phishing-as-a-Service" or "PhaaS." These phishing kits include email templates, fake website templates, domains, and features designed to evade detection

[3] To be clear, Tycoon 2FA is not exploiting a Microsoft vulnerability. Rather these phishing kits rely on social engineering and deception to trick users into sharing credentials thereby bypassing Microsoft security measures and entering a victim's network as though they were an authorized user.

[4] The Defendants also design branded kits to target other companies' products such as Google, GoDaddy, and Adobe

and lead victims to believe they are dealing with legitimate products. The kits are essentially "how to" or "do it yourself" manuals for cybercriminals to develop and execute attacks on email systems through phishing campaigns, regardless of technical sophistication or capability. The Tycoon 2FA Defendants' phishing operation provides the gateway and know-how for cyber criminals to attack Microsoft customers and steal their personal and confidential business information.

7. Together with the purchasers and users of the Tycoon 2FA phishing kits, Defendants Saad Fridi and the John Does oversee the development, creation, and sale of the phishing kits and have collectively formed a criminal racketeering enterprise that works in tandem to carry out cyberattacks against Microsoft, its customers, and the public.

8. These Tycoon 2FA phishing kits are particularly destructive as they facilitate "adversary in the middle" ("AiTM") attacks whereby the attacker is allowed into the victim's system (through deception on the part of the attacker and affirmative actions by the victim, such as clicking a link and providing credentials), enabling the attacker to hide in the system and intercept communications and extract confidential information that can be further exploited by the cybercriminals.

9. Microsoft, without disclosing its identity, recently conducted a "test buy" of Tycoon 2FA phishing kits and purchased a subscription to the Tycoon 2FA phishing kit. With that subscription, Microsoft received instructions on how to use the phishing kit and access the dashboard that provides subscribers with the tools to launch phishing attacks. The Microsoft investigators received access to the infrastructure that allowed them to generate phishing templates and use the templates to conduct a test phish and see how the Tycoon 2FA kit works. The test buy and the test phish allowed Microsoft to observe the technical features of the Tycoon 2FA phishing kit, including the technical countermeasures Tycoon 2FA uses to avoid detection. The test buy

also allowed Microsoft to track the cryptocurrency transactions of the Tycoon 2FA Defendants, confirming the scope of Tycoon 2FA Defendants' phishing activities.

10. Through these test buys and Microsoft's ongoing investigation, Microsoft determined that Tycoon 2FA Defendants have established an infrastructure of websites, domains, and computers, which they use to target their victims. The website domains used by Tycoon 2FA Defendants to support their phishing operation are identified in **Appendix A**.[5] The domains set forth in **Appendix A** include both the domains that the sellers of the Tycoon 2FA kits use to support the control panel (a dashboard that purchasers of the kit can use to track efficacy and efficiency of the phishing campaigns, *i.e.*, numbers of phishing campaigns launched, the number of logins successfully stolen) and the domains that are provided with the Tycoon 2FA kits that are then used by the purchaser to carry out the phishing (*i.e.*, the domains that are included in the phishing lures and are designed to trick the victims). This aggregating of domains to launch attacks against Microsoft customers constitutes a racketeering enterprise.

11. To carry out their criminal racketeering enterprise, the Tycoon 2FA Defendants illegally use Microsoft's trademarks and logos. Microsoft has spent considerable time and resources developing goodwill and its reputation as a trusted brand, and owns the trademarks associated with the software and services it provides. The Tycoon 2FA Defendants have conspired to use and have illegally used the Microsoft name and logo to carry out their illegal phishing activities. They trick users by sending phishing emails that use Microsoft trademarks on the login screens deceiving victims into providing credentials to the attacker on the fake Microsoft login

[5] Microsoft collaborated with Proofpoint, a leading cybersecurity company that protects organization by securing email systems and enterprise applications from cyber threats. Microsoft leveraged domain information provided by Proofpoint to identify and validate domains that comprise Tycoon 2FA's technical infrastructure.

screen. Because a victim sees the Microsoft logo, he or she believes that the login page is protected by Microsoft's security measures. In reality, the login pages fraudulently use Microsoft's logos and branding and are actually controlled by the Tycoon 2FA Defendants, allowing them to steal the credential information from the login page.

12. In Fall 2025, Microsoft commenced an investigation into the Tycoon 2FA Defendants. Microsoft investigators determined that Tycoon 2FA Defendants' phishing operation was the most prolific threat actor imposing the greatest adverse impact on Microsoft customers of all the currently existing phishing threat actors. Based on its investigation, Microsoft discovered that Tycoon 2FA has operated since Fall 2023 (one of the primary domains associated with the operation was purchased in July 2023 and in October 2023, Tycoon 2FA launched the Telegram channel).[6] As other PhaaS operations have been subject to court order and injunctions (*infra*, ¶ 13), Tycoon 2FA's activity has increased, filling the void as the demand for these phishing kits remain. As part of Tycoon 2FA's operation, Defendant Fridi published a number of videos that functioned as tutorials for how to use his phishing kits. For example, on November 13, 2024 a video titled "How To Add Telegram API Key And Chat ID-VEED.mp4" was published on veed[.]io. This video provided a step-by-step demonstration of how to use the Tycoon 2FA kit. The video detailed the process of obtaining and inputting the Telegram API key and chat ID, which are used for enabling automated notifications and communications within the Tycoon 2FA PhaaS

[6] Based on Microsoft's investigation, Microsoft has been able to identify one of the individuals responsible for the Tycoon 2FA kit: Defendant Saad Fridi. Microsoft's investigation has revealed that Fridi was previously involved in cyber defacement, a form of cyber-vandalism similar to graffiti where attackers gain unauthorized access to a website to alter its visual appearance, replacing content with messages, images, or slogans. However, because phishing-as-a-service is more lucrative financially, Fridi focused his attention on selling his phishing kits.

ecosystem. Videos like these function as marketing and advertisement for the Tycoon 2FA kits, which causes more cybercriminals to purchase and use the kit.

13. 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.). 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.).

14. Tycoon 2FA Defendants have caused and will continue to cause irreparable injury to Microsoft, its customers, Health-ISAC, its members, and the public. Plaintiffs seek injunctive relief to take down the infrastructure developed and used by the Tycoon 2FA Defendants to perpetrate their crimes and other equitable relief and damages against Tycoon 2FA Defendants.

PARTIES

15. Microsoft is a corporation duly organized and existing under the laws of the state of Washington, having its headquarters and principal place of business in Redmond, Washington. Microsoft's Digital Crimes Unit ("DCU") is the Microsoft division responsible for protecting Microsoft and its customers against cybercrime threats. DCU is an international team of technical, legal, and business experts that has been fighting cybercrime, protecting individuals and

organizations, and safeguarding the integrity of Microsoft services since 2008.[7] One of DCU's responsibilities is to investigate cybersecurity threats and identify and attribute attacks, like it has done here with the Tycoon 2FA Defendants. DCU also collaborates with MSTIC, Microsoft's threat intelligence center, which is made up of thousands of world-class experts, security researchers, analysts, and threat hunters. MSTIC publishes a threat intelligence blog alerting customers and the public of cybersecurity threats.[8]

16. Health-ISAC is a non-profit corporation duly organized and existing under the laws of the State of Florida, having its headquarters and principal place of business in Ormond Beach, Florida. 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.

17. Defendant Saad Fridi is an individual residing in Pakistan who created the Tycoon 2FA-branded phishing kits and controls the Tycoon 2FA Defendants' technical infrastructure in furtherance of effectuating harm to Microsoft, its customers, including Health-ISAC, its member organization, and the public.

18. Plaintiffs are informed, believe, and thereupon allege that Defendant John Doe 1 provides administrative and/or technical support and assists in the marketing, advertising, and sale

[7] *Digital Crimes Unit: Leading the fight against Cybercrime, Microsoft*, available at https://news.microsoft.com/on-the-issues/2022/05/03/how-microsofts-digital-crimes-unit-fightscybercrime/ (May 3, 2022).

[8] *See* Microsoft, *Threat Intelligence Blog*, available at https://www.microsoft.com/en-us/security/blog/topic/threat-intelligence/ (last accessed Oct. 10, 2024).

of the Tycoon 2FA phishing kits as well as the maintenance of the technical infrastructure in furtherance of effectuating harm to Microsoft, its customers, and the public. Plaintiffs are informed, believe, and thereupon allege that John Doe 1 can likely be contacted directly or through third parties using the information set forth in **Appendix A**.

19. Plaintiffs are informed, believe, and thereupon allege that Defendant John Doe 2 provides financial support for the Tycoon 2FA Defendants' including by assisting the operation in leveraging various cryptocurrency wallets to conceal and convert funds in furtherance of effectuating harm to Microsoft, its customers, and the public. Plaintiffs are informed, believe, and thereupon allege that John Doe 2 can likely be contacted directly or through third parties using the information set forth in **Appendix A**.

20. Plaintiffs are informed, believe, and thereupon allege that Defendant John Doe 3 is a cybercriminal, who purchased the Tycoon 2FA-branded phishing kit and utilized the tools provided in the phishing kit to carry out phishing attacks against Microsoft, its customers, and the public. Plaintiffs are informed, believe, and thereupon allege that John Doe 3 can likely be contacted directly or through third parties using the information set forth in **Appendix A**.

21. Plaintiffs are informed, believe, and thereupon allege that Defendant John Doe 4 is a cybercriminal, who purchased the Tycoon 2FA-branded phishing kit and utilized the tools provided in the phishing kit to carry out phishing attacks against Microsoft, its customers, and the public. Plaintiffs are informed, believe, and thereupon allege that John Doe 4 can likely be contacted directly or through third parties using the information set forth in **Appendix A**.

22. Set forth in **Appendix A** are the identities of and contact information for third-party domain registries that control the domains used by the Tycoon 2FA Defendants.

23. Plaintiffs are informed, believe, and thereupon allege that Defendants Saad Fridi and John Does 1-4 jointly own, rent, lease, or otherwise have dominion over the technical infrastructure, including the domains identified in **Appendix A**, and through this technical infrastructure, control and operate the phishing operation by selling, distributing, implementing, and using the Tycoon 2FA-branded phishing kits. Plaintiffs will endeavor to amend this Complaint to allege the Doe Defendants' true names and capacities when and if ascertained. Plaintiffs will exercise due diligence to determine Doe Defendants' true names, capacities, and contact information, and to effect service upon those Doe Defendants.

24. Plaintiffs are informed, believe, and thereupon allege that the actions and omissions alleged herein undertaken by Defendants Saad Fridi and John Does 1-4 were authorized, controlled, and/or directed, by Tycoon 2FA Defendants for which each Defendant is liable. Each Defendant aided and abetted the actions of Tycoon 2FA Defendants and benefited from those actions and omissions, in whole or in part. Each Defendant acted as the agent of each of the remaining Tycoon 2FA Defendants and acted within the course and scope of such agency and with the permission and consent of other Tycoon 2FA Defendants.

25. Third party VeriSign Global Registry Services is the domain name registry that oversees the registration of all domain names ending in ".com" and ".net" and is located at 12061 Bluemont Way, Reston, Virginia 20190. As set forth in **Appendix A**, the Tycoon 2FA Defendants use ".com" and ".net" domains in connection with their cybercriminal operation.[9]

[9] None of the third-party registries has acted unlawfully; rather Tycoon 2FA Defendants simply register domains that are administered by these well-known registries with no knowledge of Defendants' criminal purpose.

JURISDICTION AND VENUE

26. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises out of Tycoon 2FA Defendants' violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962), the Racketeer Influenced and Corrupt Organizations Act (RICO) (18 U.S.C. § 1962(d)), the Electronic Communications Privacy Act (18 U.S.C. § 2701), and the Lanham Act (15 U.S.C. §§ 1114, 1125). Pursuant to 28 U.S.C. § 1367, the Court has supplemental jurisdiction over the common law claims of trespass to chattels, conversion, and unjust enrichment claims.

27. The Court has personal jurisdiction over Tycoon 2FA Defendants because they engage in conduct availing themselves of the privilege of conducting business in the State of New York, and utilize instrumentalities located in the State of New York and the Southern District of New York to carry out acts alleged herein. Specifically, as shown in **Figure 1**, *infra*, Tycoon 2FA Defendants direct a significant amount of their cybercriminal activity against New York organizations and individuals.

28. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Microsoft's claims has occurred in this judicial district, and because a substantial part of the harm caused by Tycoon 2FA Defendants has occurred in this judicial district. Tycoon 2FA Defendants engage in conduct availing themselves of the privilege of conducting business in the State of New York, and utilize instrumentalities located in the State of New York and the Southern District of New York to carry out acts alleged herein. **Figure 2** is a heatmap generated through DCU's investigation, showing the location of cybercriminal activity that DCU has attributed to Tycoon 2FA Defendants. As shown in the heatmap, a significant portion of this activity is directed at New York-based organizations and

individuals. Specifically, at least 623 Microsoft customers located in the State of New York were successfully phished by Defendants using the Tycoon 2FA phishing kit (a successful phish means that at least one individual located at the customer entity provided credentials to Defendants after receiving a phishing email). Of these 623 New York customers, 596 are located within the Southern District of New York. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because Tycoon 2FA Defendants are subject to personal jurisdiction in this judicial district.

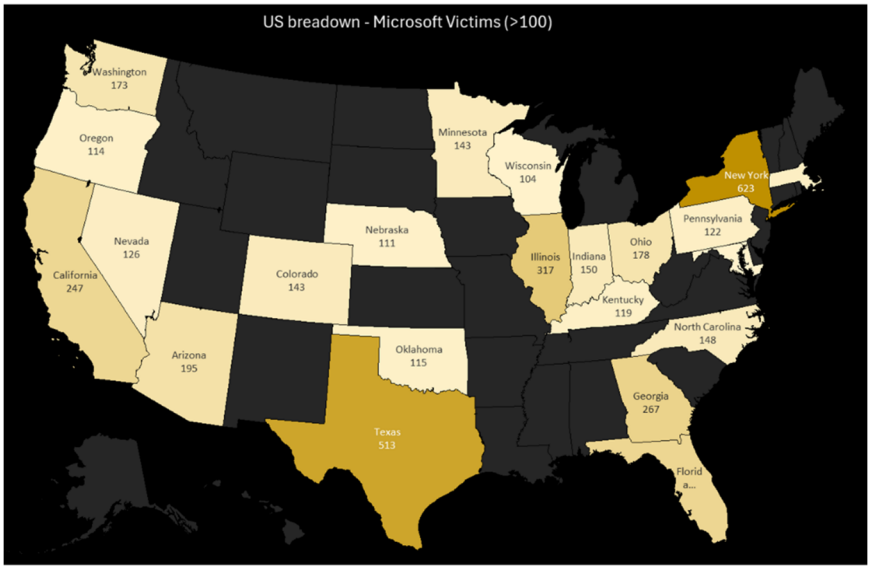


FIGURE 1

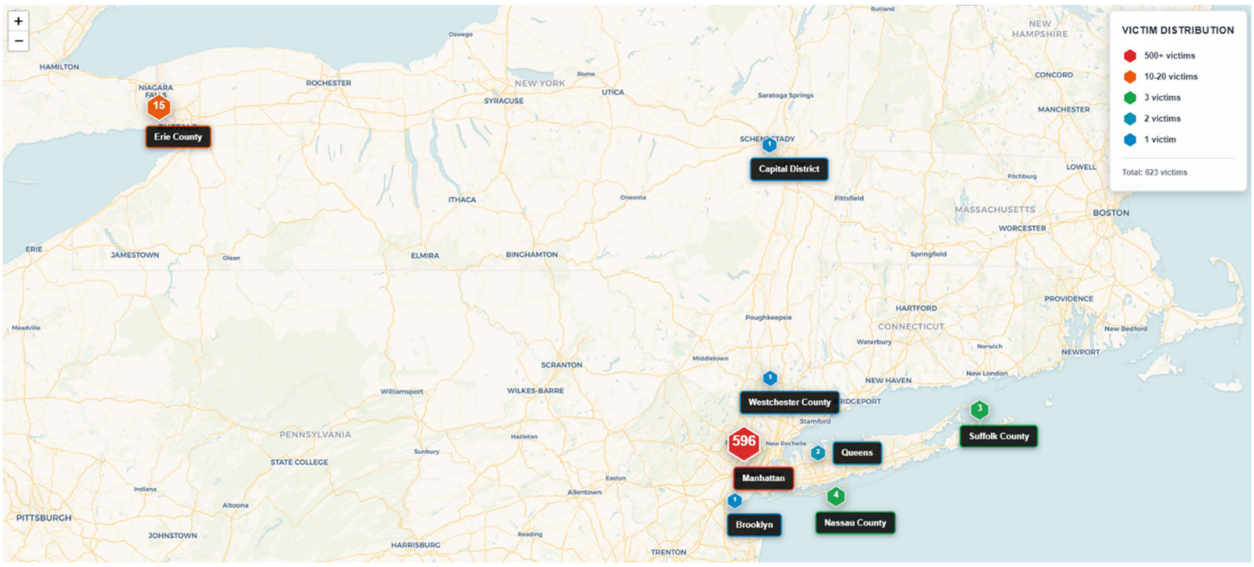


FIGURE 2

FACTUAL BACKGROUND

I. Microsoft's Services and Reputation

29. Microsoft is one of the world's leading technology companies, providing complete, open, and integrated computer software programs and hardware systems to individuals, businesses and governments. Microsoft is a provider of the Windows® computer operating system, and a variety of other software and services including Microsoft 365®, Office 365®, Outlook®, and Excel®.[10] Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, establishing a strong brand and world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including Microsoft®, Windows®, Microsoft 365®, Office365®, Office®, Microsoft Office®, SharePoint®, OneDrive®, Outlook®, and Excel®. Copies of the trademark registrations for these trademarks are attached as **Appendix B** to this Complaint.

30. Health-ISAC is an industry organization that represents approximately 1,100 member organizations both in the United States and globally including hospitals, medical devices manufacturers, pharmaceutical manufacturers, insurers, and health IT organizations. It was established in 2010 to promote public trust by advancing the global health sector's cyber and physical security protection and resilience as well as enabling the ability to prepare for and respond

[10] Microsoft 365 and Office 365 are product families of productivity software, collaboration and cloud-based services owned by Microsoft. Microsoft 365 and Office 365 include Microsoft Office, which is a bundle of productivity applications that contains, among other things: a word processor (Word), a spreadsheet program (Excel), a presentation program (PowerPoint), and an email client (Outlook).

to cyber and physical threats and vulnerabilities. Health-ISAC's activities include sharing timely, actionable and relevant information with its members, including threat intelligence, involving indicators of compromise, tactics, techniques and procedures (TTPs) of threat actors.

31. Microsoft and Health-ISAC have coordinated together in connection with similar actions, successfully taking down cybercriminals who have launched attacks against Microsoft, its customers, and Health-ISAC member organizations.

II. The Tycoon 2FA Defendants

32. Tycoon 2FA Defendants are cybercriminals that manufacture and sell Tycoon 2FA phishing kits and provide PhaaS to other cybercriminals, who then launch phishing attacks against Microsoft customers across various industries. Tycoon 2FA Defendants first emerged in Fall 2023, but it was not until 2025 that the operation became one of the most prolific PhaaS operations. By August 2025, internal Microsoft telemetry revealed that 62 percent of the phishing attacks blocked by Microsoft involved the use of the Tycoon 2FA kit. Tycoon 2FA Defendants boast that their kits include multiple phishing templates (including Outlook, Excel, 365, SharePoint, Word), multiple distribution methods for the phishing emails (PDF attachments, QR codes, links included in the email), anti-detection features (including antibot detection and IP blocking), reverse proxy through the use of Cloudflare workers' deployment, credential/session cookie delivery, and end user analytics (the ability to track the efficacy of a particular phishing campaign). Through these offerings, the Tycoon 2FA platform is designed for large-scale credential theft operations.

33. The phishing operation is carried out by Defendants Saad Fridi and John Does 1-4. Microsoft was able to identify Fridi by using information from his Microsoft accounts, information Fridi provided in connection with his Telegram account, and open-source intelligence.

III. Tycoon 2FA's Cybercrime *Modus Operandi*

34. Much like how companies develop and sell all-in-one do-it-yourself kits to traditional customers for personal projects, Tycoon 2FA Defendants develop do-it-yourself phishing kits for cybercriminals to purchase and use for their cybercrime operations. The purchasers of these kits become part of the Tycoon 2FA Defendants' operation when they, in turn, use the Tycoon 2FA kit to create templates to conduct phishing and leverage the AiTM model[11] by positioning themselves between communications directed to and from Microsoft customers. **Figure 3** depicts the operational overview of how a Tycoon 2FA purchaser leverages the kits to engage in phishing attacks against a victim using the AiTM model, thus becoming part of Defendants' cybercriminal operation.

[11] The Tycoon 2FA-branded phishing kit allows cyber criminals to infiltrate the systems of Microsoft customers undetected and collect the usernames and passwords of the users of the infiltrated network. This is known as AiTM, which is a form of cyberattack where the malicious actor intercepts communications between two parties without their knowledge. It is particularly common for AiTM attacks to leverage PhaaS platforms given the high volume of phishing emails that these phishing kits make possible. This enables these criminals to then enter the system using these purloined credentials and remain undetected. Microsoft has identified AiTM attacks as one of the Top 5 PhaaS models by volume. 2024 MDDR at 34-35.

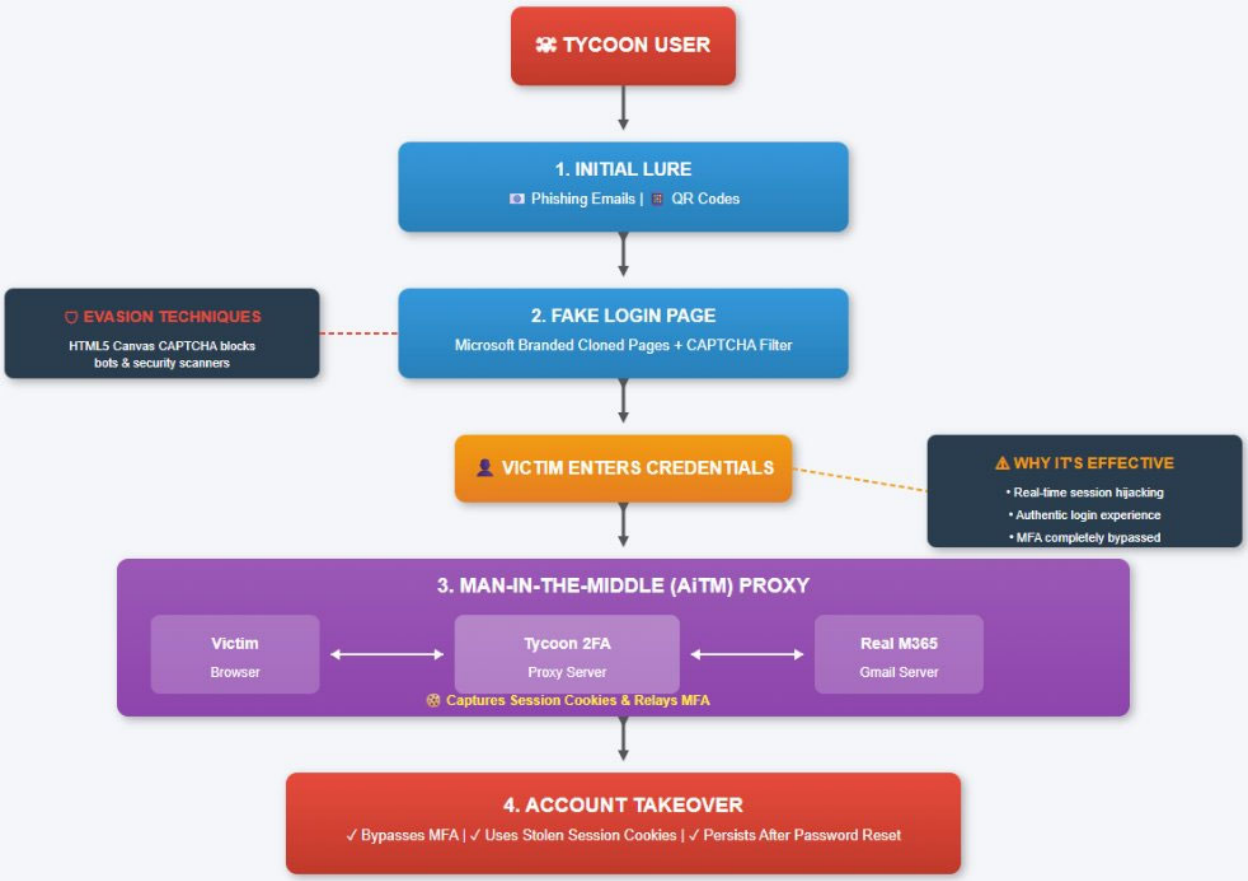


FIGURE 3[12]

[12] As described in greater detail herein (*see infra* ¶¶ 40-46, 52-55), an AiTM attack flow follows the following steps:

1. **Phishing Email**: Attacker sends a phishing email to the victim.
2. **Multiple Redirects:** When the victim clicks on the link in the email, the domain is redirected 3-4 times before landing on the login page. These redirects acts as a defensive countermeasure to further avoid detection.
3. **Fake Login Page**: Victim clicks the link and is directed to a fake login page.
4. **Credential Capture/Harvesting**: Victim enters credentials on the fake page, which are captured by the attacker. The victim is presented with a fake login page, where they enter their real Microfsoft credentials. These credentials are relayed to Microsoft's server, which causes a 2FA (two-factor authentication) or MFA (multi-factor authentication) prompt to be related back to the victim. When the victim enters the 2FA/MFA code, the authenticated session cookie is captured by Defendants.
5. **Account Compromise**: Defendants now possess the victim's authenticated session cookie, allowing them to access all Microsoft accounts associated with that credential, without having to do further 2FA/MFA.
6. **Date Exfiltration**: Defendants retrieve harvested credentials from the control panel. Because Defendants have access to the victims' accounts, they can conduct further exploitations (viewing files, downloading documents, changing account settings).

35. Phishing is the fraudulent practice of sending emails or other messages purporting to be from legitimate senders to induce recipients to reveal personal information, such as passwords or other credentials. It is a form of social engineering and a scam where the recipient-victim is convinced to interact with the correspondence (referred to as the "lure"). Tycoon 2FA Defendants develop and sell Tycoon phishing kits that are advertised and promoted as being able to circumvent the security features of Microsoft products, use Microsoft logos, and mimic the appearance of authentic communications to deceive victims into thinking that the email communication they receive, the files they are directed to open, or links to websites used to enter their personal credentials are authentic and Microsoft-approved. The Tycoon 2FA Defendants do not and cannot frontally target or compromise Microsoft's security features. Rather, Defendants avoid Microsoft's security features when a phishing recipient clicks on a weaponized link and ushers the attacker into the victim's system right through the front door negating the ability of Microsoft security to repel the attack.

36. A successful phishing attack relies on deceiving the victim that the email communication received or a website they are directed to is authentic. To perpetrate this deception, the communication they receive often appears to be from familiar contacts or organizations. Victims are directed to click on a link in the malicious email. The phishing websites connected with the link may appear authentic to a victim by using a company name, a well-known product, or some administrative service. As a result, the phishing domain may easily be misperceived as the authentic domain. When a phishing victim is deceived to visit a website and enter her credentials, Tycoon 2FA Defendants lie in wait to collect those credentials to subsequently access the account to further their cybercrime.

37. Tycoon 2FA Defendants' phishing kits are developed to target Microsoft 365 and Office 365 users (in addition to the customers of other companies such as Adobe, Google, and GoDaddy), and involve redirecting victims to fake login pages where the victims are deceived into entering their Microsoft credentials. These malicious phishing kits support credentials theft, information exfiltration, and subsequent end-user terminal attacks which include business email compromise, ransomware, and financial fraud. Tycoon 2FA Defendants execute these end-user terminal attacks more readily when they are able to access a victim's Microsoft platform, which serves as a gateway to other computer applications, and where these applications are connected by a global Microsoft network infrastructure. These features are the "selling points" of the phishing kits, and Tycoon 2FA Defendants advertise their ability to target Microsoft customers.

38. Once a kit is purchased, cybercriminals can conduct their own phishing attacks using the templates and domains provided in the phishing kits. Because all the domains are registered, provided, and administered by the Tycoon 2FA Defendants, they are interconnected as part of a single technical infrastructure. These website domains are identified in **Appendix A** to the Complaint. Over the last 15 years, courts have frequently enjoined cybercriminals from attacking Microsoft and its customers, granting the relief Microsoft seeks against the Tycoon 2FA Defendants herein.[13]

[13] *See, e.g.*, *Microsoft and Health-ISAC v. Joshua Ogundipe and John Does 1-4*, 1:25-cv-07111 (S.D.N.Y. August 2025) (Rakoff, J.) ; *Microsoft and LF Projects v. Abanoub Nady and John Does 1-4*, 1:24-cv-2013-RDA (E.D. Va. Nov. 13, 2024) (Alston, J.); *Microsoft and NGO-ISAC v. John Does 1-2*, Case No. 1:24-cv-02719-RC (D.D.C. Sep. 24, 2024), (Contreras, J.); *Microsoft Corporation v. Tu et al.*, Case No. 23-cv-10685 (S.D.N.Y Dec. 13, 2023) (Engelmayer, J.); *Microsoft, Fortra, and Health ISAC v. John Does 1-16* Case No. 23-cv-2447 (E.D.N.Y. 2023); *Microsoft, FS-ISAC, Health-ISAC v. Denis Malikov and John Does 1-4*, Case No. 1:22-cv-1328-MHC (N.D. Ga. 2022); *Microsoft v. John Does 1-2*, Case No. 1:19-cv-00716-ABJ (D.D.C. 2019) (Berman-Jackson, J.); *Microsoft v. John Does 1-2*, Case No. 1:19-cv-01582 (E.D. Va. 2019) (O'Grady, J.); *Sophos v. John Does 1*-2, Case No. 1:20-cv-00502 (E.D. Va. 2020); *Microsoft v.*

39. Tycoon 2FA Defendants illegally use Microsoft systems and programs, such as Outlook and Microsoft 365, to further enhance the perceived legitimacy of the attack. In doing so, Tycoon 2FA Defendants capitalize on and misuse the brand recognition that Microsoft has cultivated, and the trust Microsoft has built with its customers. Defendants' use of Microsoft's trademarks in connection with their products and branding is false, deceptive and unauthorized.

a. Development and Sale of Tycoon 2FA-Branded Phishing Kits

40. Much like how an e-commerce business sells its products in online stores for consumers to purchase, Tycoon 2FA Defendants sell their Tycoon 2FA-branded online.

41. The phishing kits are promoted through Telegram Messenger, a cloud-based, cross-platform, instant messaging service. and **Figure 4** is the screenshot of the Telegram channel that the Tycoon 2FA Defendants operate. **Figure 5** is a screenshot reflecting the profile of Telegram user Mr._Spy0x0, which based on Microsoft's investigation is the account associated with Defendant Fridi and the account used to administer the Telegram account used by the Tycoon 2FA Defendants.

John Does 1-2, Case No. 1:20-cv-00730 (E.D. Va. 2020) (O'Grady, J.); *DXC Technology Company v. John Does 1-2,* Case No. 1:20-cv-00814 (E.D. Va. 2020) (Alston, J.); *Microsoft and FS-ISAC v. John Does 1-2,* Case No. 1:20-cv-1171 (E.D. Va. 2020) (Trenga, J.).

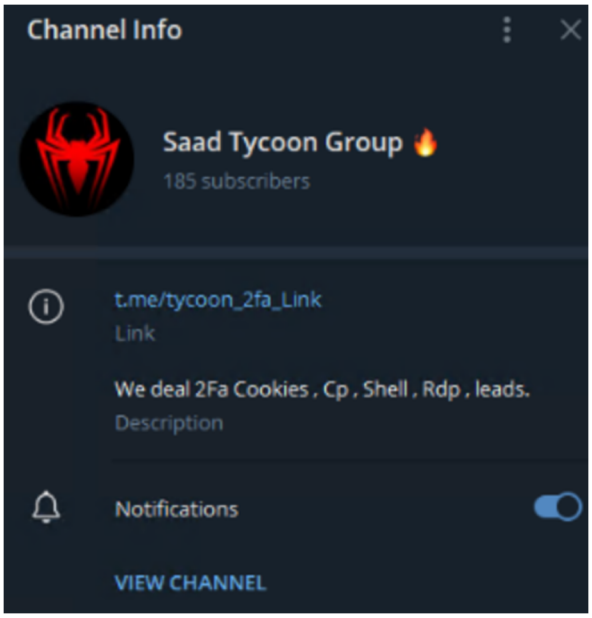


Figure 4

Figure 5

42. The phishing kits are offered as a monthly subscription, with different package options ranging in prices based on the number and type of domains provided as well as kit distinct package features, similar to the way the software subscription services offer different-priced subscription tiers. For example, **Figure 6** is a screenshot of a Telegram message offering different plans based on subscription duration and type of domain offered. As shown in the screenshot,

Tycoon 2FA Defendants charge more for a kit that includes .com domains (administered by a U.S. based registry) compared to .ru domains (Russia-based domains).

Figure 6

43. Once a cybercriminal purchases a subscription, the user can phish endlessly during the term of their subscription. The purchase of the subscription is conducted over Telegram, and that is how the purchaser receives access to the control panel.

b. DCU Purchases Tycoon 2FA Kit

44. In November 2025, DCU was involved in a test buy, where DCU purchased a one-month subscription to the Tycoon 2FA phishing kits from Tycoon 2FA Defendants.[14] For the one-

[14] In 2024, Sekoia, a security research company published an article which revealed operational details of Tycoon 2FA, *See* Sekoia TDR and Quentin Bourge, Quentin Bourge, *Tycoon 2FA: an in-depth analysis of the latest version of the AiTM phishing kit*, Sekoia, available at https://blog.sekoia.io/tycoon-2fa-an-in-depth-analysis-of-the-latest-version-of-the-aitm-phishing-kit/#88b42268-54a7-49a0-9ff6-3f3d363c41ea (Mar. 25, 2024). Following that, Defendant Fridi shut down his Telegram channel. Now, Defendant Fridi requires potential purchasers to

month subscription, Microsoft paid the subscription fee of $350 USD. To conduct the test buy, the referral source that DCU relied on communicated with Defendants via the Defendant Fridi's Telegram account. After expressing interest in purchasing a monthly subscription, Defendants provided cryptocurrency payment information, which Microsoft used to deliver payment.

45. Following payment, Microsoft obtained access to the control panel. **Figure 7** is a screenshot of the dashboard to which Microsoft received access. From the control panel, a purchaser of the Tycoon 2FA kit has access to customizable pre-configured templates (HTML links, PDFs, QR codes, etc.) with themes that a user can select for its phishing (for example, an email template containing a link to a "time sensitive" document). The user can also select the CAPTCHA that will be used as an anti-detection measure and the domain that will be incorporated into the phishing email. Unlike some phishing kits where cybercriminals are required to purchase their own domains to use in connection with their phishing, the Tycoon 2FA kit provides purchasers with pre-registered domains that are embedded in the templates from the control panel. These Tycoon 2FA users choose which domains they want to be included in each of their templates that they download from the control panel. Tycoon 2FA users then send customized and weaponized emails to victims designed to induce them to click on the malicious domains where they are redirected to a Tycoon 2FA-controlled webpage and then unknowingly provide their credentials to Defendants. Based on Microsoft's investigation, it appears that each Tycoon 2FA kit purchaser is allocated set of domains for use in launching these attacks. This test buy provided

communicate with him via Telegram direct messages and will not sell his phishing kits unless the potential customer is referred to Defendant Fridi and is vetted through the trusted referral. Because Defendant Fridi closed his Telegram channel and because Fridi no longer sells to unvetted purchasers, DCU relied on a security research company that had previously purchased a Tycoon 2FA kit for security research purposes to purchase a subscription to Tycoon 2FA on DCU's behalf.

Microsoft access to the same control panel infrastructure that is used by the Tycoon 2FA Defendants to launch phishing attacks.

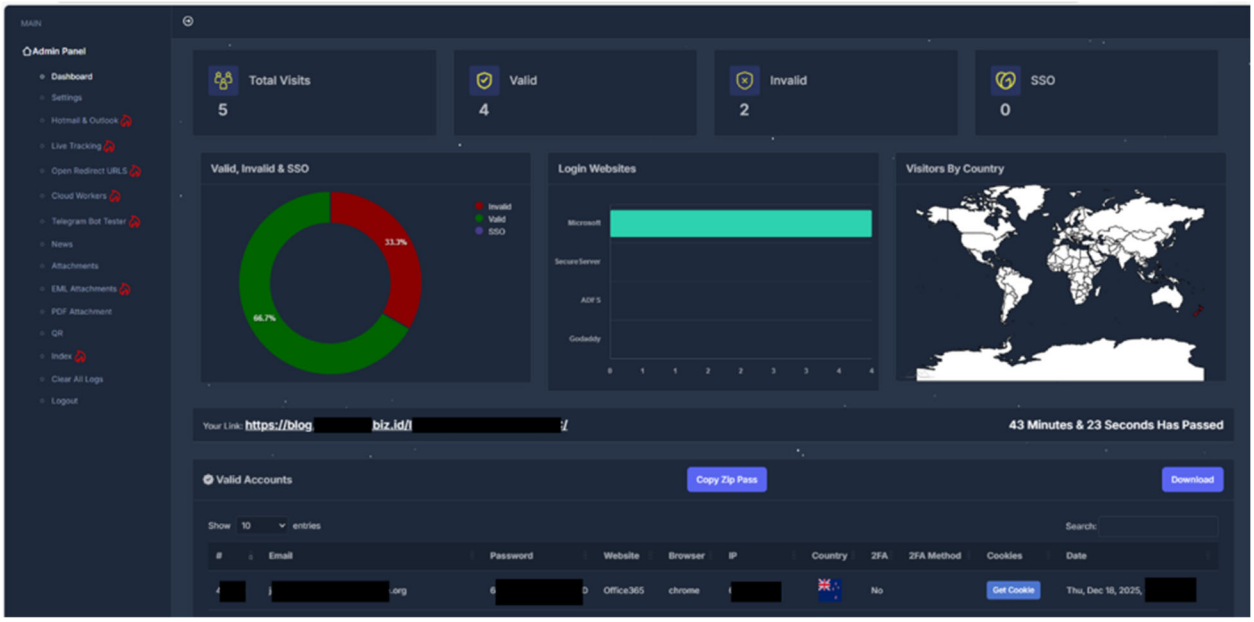


Figure 7

46. Following the test buy, Microsoft conducted a controlled phishing attack against a dummy account owned by Microsoft to learn the steps the Tycoon 2FA Defendants take to obscure their identity and conceal their cybercrimes. This allowed Microsoft to also see what a victim who was being phished would experience.

IV. Tycoon 2FA Kits Features Are Designed to Streamline Phishing Process

47. Once a cybercriminal purchases the Tycoon 2FA phishing kit, it can immediately launch phishing attacks. The control panel provides the template files, including model phishing emails, that can be easily configured to match the cybercriminals[15] phishing objective. For example, the template could include messaging that suggests the recipient needs to open an

[15] Cybercriminal customers become part of the cybercriminal organization as John Does 3-4 once they have purchased a Tycoon 2FA-branded phishing kit from Defendants.

important document immediately. Additionally, each purchaser of the kit is allocated multiple domains which will be embedded in the templates. For example, the template could include a what appears to be a link to the "important document" which when selected by the victim, opens to a Defendant-controlled website.

48. When a Tycoon 2FA Defendant launches a phishing attack it will appear in the victim's inbox as an authentic email, inducing the victim to open the email and complete a particular action *e.g.* open a document to review edits, provide a response on an online form, or validate credentials. When the victim clicks on the link contained in the email, she is taken to a webpage that looks like a legitimate login page for a Microsoft product. What the victim does not see is that the webpage is fraudulent and controlled by Defendants. The victims are deceived by Defendants use of Microsoft's branding and logos, which makes the website look legitimate and lures Defendants' victims into a false sense of security into providing information allowing Tycoon 2FA Defendants to further their criminal activities.

V. Tycoon 2FA Defendants Use Cloudflare Infrastructure to Cover Their Tracks

49. The Tycoon 2FA Defendants leverage legitimate Cloudflare infrastructure to further evade detection. Cloudflare is a company that provides a variety of legitimate network services and security features to protect websites from various online cyberthreats. The Cloudflare infrastructure hosts Defendants' phishing sites and powers the redirection of the domains when the victim clicks on the link in the phishing emails.

50. There are two main Cloudflare services that are used by Tycoon 2FA Defendants: reverse proxying[16] and a CAPTCHA[17] service to authenticate that a website link is legitimately clicked by a human.

(a) *Reverse IP proxying*. Cloudflare provides an IP proxy feature that acts like a middleman to protect the privacy of domain owners. An IP proxy allows legitimate, honest users to have an intermediary in place to protect the privacy of the domain by shielding it from public view. When used by the Tycoon 2FA Defendants, this prevents security researchers or law enforcement from being able to identify the real IP address associated with the infrastructure. This allows Tycoon 2FA Defendants to hide their location, making it more difficult for their infrastructure to be taken down.

(b) *CAPTCHA*. CAPTCHAs allow websites to discern if it is interacting with a human user rather than a bot. Ordinally, CAPTCHAS are designed to protect consumers; Tycoon 2FA Defendants, however, use a CAPTCHA feature to prevent email security programs that would deploy automated programs (bots) to check if an email has malicious content or links to malicious websites. By using the CAPTCHAS (whether those that are offered as part of the kit or if the Tycoon 2FA user configures a Cloudflare one), Tycoon 2FA Defendants can block security scanning bots from running the scan of the websites controlled by Tycoon 2FA Defendants. This

[16] IP proxying is where a proxy server acts as an intermediary between the user and the web server. Proxy servers use a different IP address on behalf of the user, concealing the user's real address from web servers.

[17] CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) has been widely used as a means of protection against bots. It is a type of challenge – response test used to determine whether the user trying to access a website is human in order to deter bot attacks and spam. Tycoon 2FA kits provide users with CAPTCHAS to user. Tycoon 2FA users, if they want, can also configure Cloudflare-based CAPTCHAS within they Tycoon 2FA control panel.

prevents the websites controlled by 2FA Defendants from being flagged as "malicious" or "suspicious," which further ensures success of the phishing attack.

51. Both the misuse of Cloudflare's IP proxying and CAPTCHA services allow Tycoon 2FA Defendants to conduct their phishing attacks with little/lower risk of being discovered or being blocked by using the legitimate services as a technical countermeasure against detection.

VI. Tycoon 2FA Defendants' Attack Chain

52. To commence an attack, a phishing email is sent to a victim that prompts the victim to click on a link connected to the malicious domain. These phishing emails use, without authorization, Microsoft's logos and format to lull the victim into believing the email is legitimate and the attachments are benign. *See* **Figure 8** (referencing a SharePoint file). When the victim downloads the file and attempts to open the document, they see that the document is titled "Important Update Immediate Review," prompting the victim to open the file and interact with the document. *See* **Figure 9**.

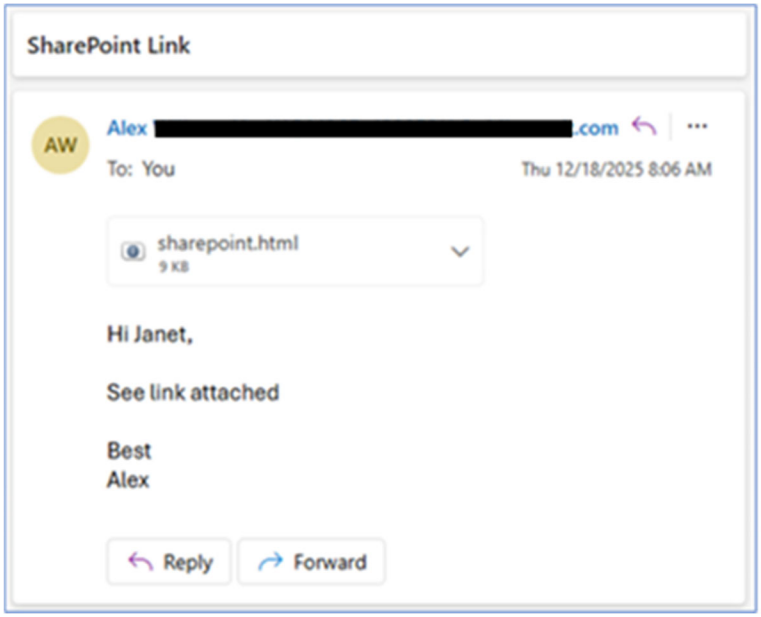


Figure 8

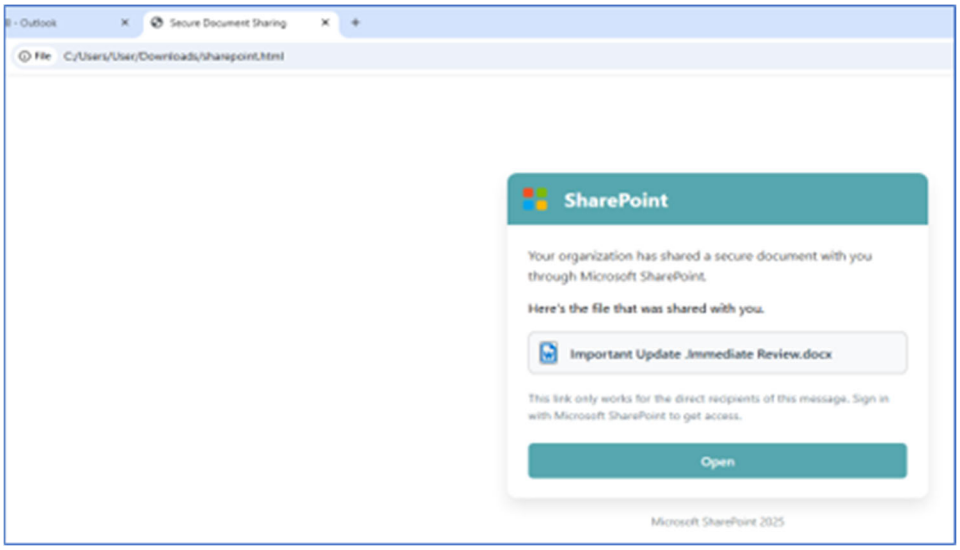


Figure 9

53. Once a victim clicks on the link, the victim is redirected 3-4 times, including through a legitimate domain (i.e., a domain that is owned by a legitimate third party and not connected to Defendants' operation) before ending on a page controlled by Tycoon 2FA Defendants. This redirection through a legitimate website serves to undermine security features that are designed to block suspicious websites. One of the features of the Tycoon 2FA kit is the sophistication of its redirection process, whereby instead of having a single level of redirection, this infrastructure allows for 3-4 redirects. This allows for greater concealment of the cybercriminal activity. **Figures 10-12** demonstrate the redirection process.

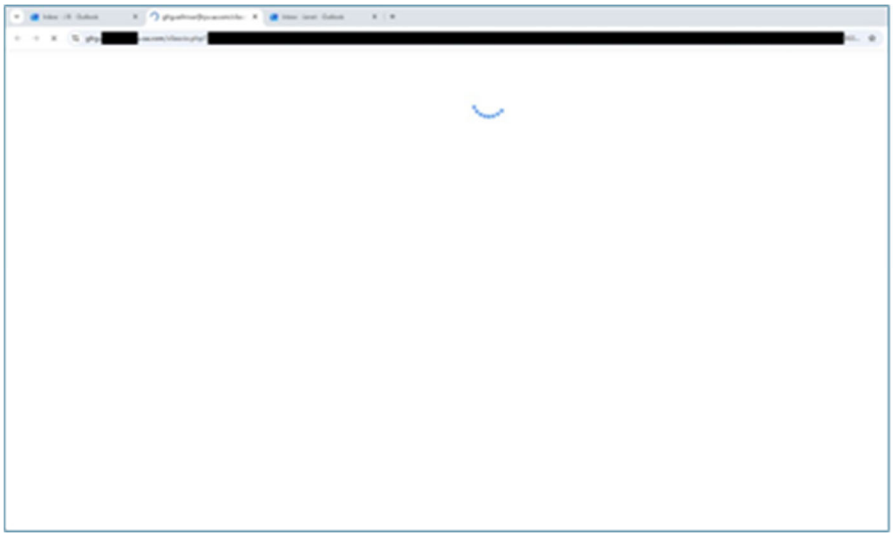


Figure 10

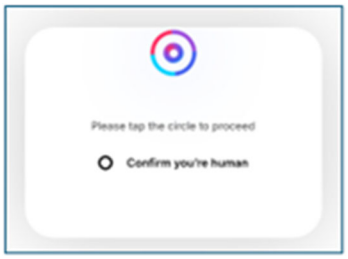


Figure 11

Figure 12

54. Once all the security measures have been disabled or circumvented, the victim is presented with a login page with Microsoft branding. Because Tycoon 2FA Defendants control the fake login page, once the victim enters their credentials the Tycoon 2FA Defendants are able to capture the credentials and they have completed their goal of credential theft. This process is shown in **Figure 13** and **14**.

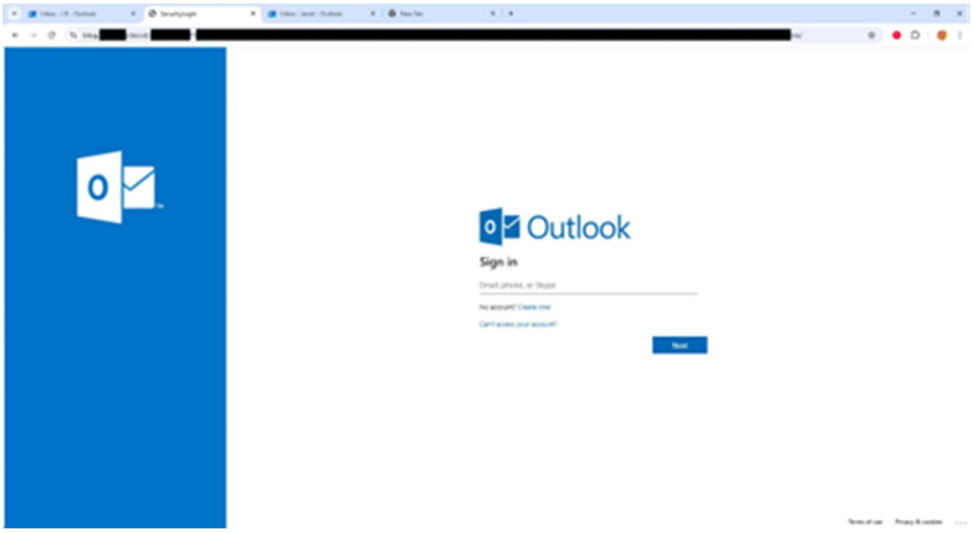


Figure 13

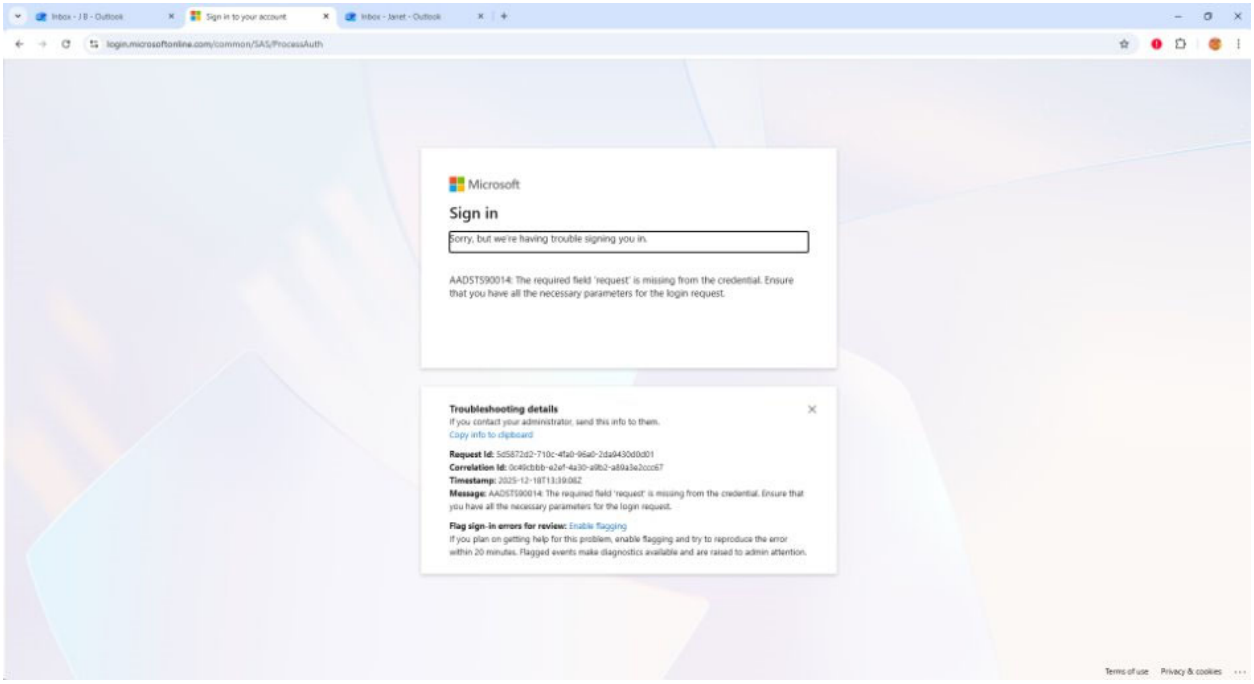


Figure 14

55. After the victim enters the username and password, the victim is directed to a genuine Microsoft website. At this point the credentials and cookies are captured via AiTM. From the control panel, the cybercriminals can download a text file that allows the cybercriminal to log into all Microsoft services that share the phished credentials. *See* **Figure 15**. Tycoon 2FA

Defendants subsequently can exploit the credentials to access their victim's services to perpetrate further cybercrime such as ransomware, business email compromise, and financial fraud.

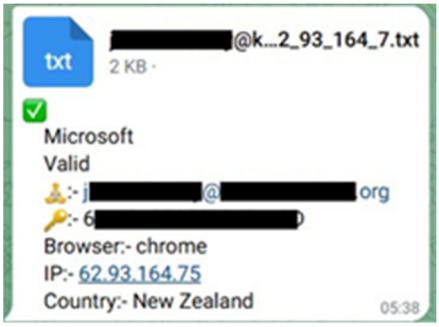


FIGURE 15

VII. Tycoon 2FA Defendants' Victimology

56. Since 2023, Tycoon 2FA Defendants have been responsible for over 96,000 individual, successfully phished credentials in globally and over 55,000 in the United States (this number is not limited to Microsoft customers and represents validated instances where a victim was phished using the Tycoon 2FA phishing kit and were deceived to provide their login credentials). Approximately 87% of Defendants' phishing activity is directed towards enterprise accounts (i.e., employee's work emails).

57. While Tycoon 2FA Defendants do not single out any particular sector to target, most of the victims are from entities that operate in the Real Estate, Health, Consumer Goods, Education and IT Services & Business Advisory sectors, targeting American companies across crucial, data-rich sectors. *See* **Figure 16** (sector breakdown of victims).

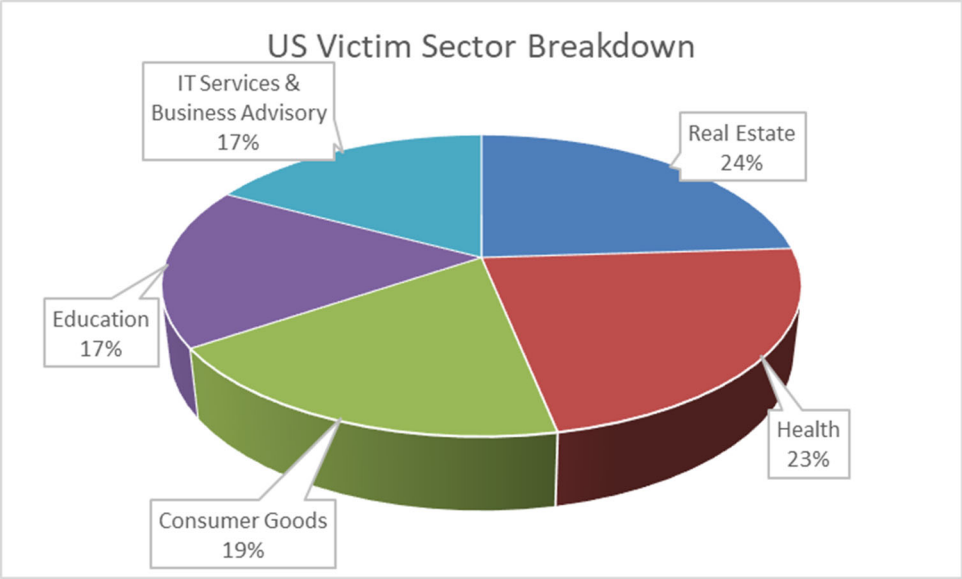


Figure 16

VI. Tycoon 2FA Jointly Leverage the Racketeering Enterprise to Commit Cybercrime

58. Defendants Saad Fridi and John Does 1-4 constitute a group of criminals engaged in a common course of conduct, as part of an ongoing organization and functioning as a continuing unit (hereinafter the "Racketeering Enterprise").

59. The Racketeering Enterprise causes significant harm to Microsoft, its customers, Health-ISAC, its member organizations, and the public. The Tycoon 2FA Defendants cooperate and collude in the sale, distribution, deployment, or use of the phishing kits, the control of the phishing operation, the importing of domains for use in the phishing operation, the provision of technical support to cybercriminals, the multi-tier subscription of phishing operation services, circumvention of technical security measures to gain access to victim computers and information, and the unauthorized use and dissemination of Microsoft's and Health-ISAC's intellectual property.

60. The relationships among Tycoon 2FA Defendants allow them to collectively pursue the criminal purpose of the Racketeering Enterprise. As **Chart 1** below demonstrates, Saad Fridi

and John Does 1-4 each have specialized roles in the Racketeering Enterprise, on which the success and furtherance of the Racketeering Enterprise is entirely dependent. Namely, the Tycoon 2FA Defendants leverage each other's work to: (i) create, distribute, and operate the phishing technical infrastructure, (ii) sell, distribute, and use Tycoon 2FA-branded phishing kits, (iii) 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. The Tycoon 2FA Defendants' ongoing association with one another and reliance on each other's contributions, allows the Racketeering Enterprise to function as a continuing unit and within a lucrative operational structure.

TYCOON 2FA DEFENDANTS	FUNCTION
Saad Fridi	Develops the Tycoon 2FA-branded phishing kit and controls the Tycoon 2FA Defendants' criminal phishing organization and the technical infrastructure.
John Doe 1	Provides administrative and technical support for the Tycoon 2FA Defendants' criminal phishing organization and the technical infrastructure.
John Doe 2	Provides financial support for the Tycoon 2FA Defendants' criminal phishing organization.
John Does 3-4	Customers of Tycoon 2FA kits, who utilize the phishing kits to conduct phishing attacks against Microsoft and its customers. Microsoft is informed, believes, and thereupon alleges that based on its investigation of the cryptocurrency wallet associated with Defendant Fridi that there are hundreds of individuals who have purchased a Tycoon 2FA kit.

Chart 1. Tycoon 2FA Defendants' Division of Labor.

61. Plaintiffs are informed, believe, and thereupon allege that Defendants Fridi and John Does 1-2, the creators, sellers, and distributors of the Tycoon 2FA-branded phishing kits, work together with the cybercriminals, who purchase and use the phishing kits, and leverage the technical infrastructure to engage in phishing attacks.

62. Plaintiffs are informed, believe, and thereupon allege that Defendants John Does 3-4 are cybercriminals who utilize the Tycoon 2FA phishing kit to conduct cybercrimes, thus expanding the reach of the Tycoon 2FA infrastructure and criminal organization. This allows the prolific expansion of the Tycoon 2FA Defendants' phishing operation, which leads to the increase of downstream criminal activities including financial fraud, business email compromise, and ransomware attacks. This level of continuous and coordinated activity allows for the success of the operation.

63. The Racketeering Enterprise has continuously and effectively carried out its purpose of developing and operating a global technical infrastructure that facilitates phishing attacks leading to credentials theft and allowing for the unauthorized access to a victim's email account or Microsoft services.

64. The relationship between the Tycoon 2FA Defendants is proven by: (i) development and repeated sale of the Tycoon 2FA-branded phishing kit, (ii) the subsequent development and operation of the technical infrastructure to proliferate the phishing operation and leveraging of the infrastructure to facilitate further criminal activities, and (iii) Tycoon 2FA Defendants' respective and interrelated roles in the sale, operation of, and profiting from the Tycoon 2FA-branded phishing kits in furtherance of Tycoon 2FA Defendants' common financial interests.

65. Plaintiffs are informed, believe, and thereupon allege that Tycoon 2FA Defendants have conspired to, and have, knowingly with intent to defraud, facilitated phishing attacks against victims to steal credentials and gain unauthorized access to a victim's computer and have impersonated Microsoft and lured victims to divulge login credentials to non-public personal

accounts. These acts are continuing and will continue unless and until this Court grants Plaintiffs' request for a temporary restraining order.

66. As set forth in detail herein, Tycoon 2FA Defendants have used the technical infrastructure to steal, intercept, and obtain credentials and other device access information from countless individuals, including 2FA authentication tokens.

67. Plaintiffs are informed, believe, and thereupon allege that Tycoon 2FA Defendants have also conspired to, and have knowingly and with intent to defraud, possessed and do possess, thousands of unauthorized access devices[18] fraudulently obtained as described herein.

68. Each of the foregoing illegal acts perpetrated by the Tycoon 2FA Defendants was conducted using interstate Automated Clearing House (ACH, a U.S. electronic network for direct bank-to-bank transfers), cryptocurrency exchanges whereby the funds are transferred via the internet—an instrumentality of interstate commerce, and/or interstate and/or foreign wires as described herein and therefore affected interstate and/or foreign commerce.

VIII. Harm to Microsoft and Microsoft's Customers

69. Microsoft has determined that Tycoon 2FA Defendants used the domains identified in **Appendix A** in their technical infrastructure and have actively and affirmatively targeted Microsoft customers in the United States. The Tycoon 2FA Defendants disguise their technical infrastructure obfuscating their criminality through the use of Microsoft products, services, branding, and logos.

[18] An unauthorized access device, as defined under the CFAA (which is one of the predicate offenses for Plaintiffs' RICO claim), includes credentials, cookies, and two-factor authentication codes (18 U.S.C. § 1029(e)(1)), all of which Tycoon 2FA Defendants steal in connection with their cybercriminal organization.

70. Because these are the webpages that a victim is redirected to when they interact with a phishing email, the use of Microsoft branding in connection with the webpage will further trick the victim into believing that the login page is legitimate and that Microsoft has endorsed the email. Tycoon 2FA Defendants rely on the Microsoft brand and trademark to perpetrate their phishing and malware attacks by leveraging and misusing the trust Microsoft has obtained from its customers.

71. Microsoft determined that Tycoon 2FA Defendants also cause great harm to the company and its customers through the unauthorized access of Microsoft enterprise platforms. An enterprise platform is a cloud platform that grants access to a victim's other computer applications and information. When the Tycoon 2FA Defendants access the Microsoft enterprise platforms, they move through other computer applications and can facilitate additional criminal activities like ransomware, financial fraud, and business email compromise.

72. Tycoon 2FA Defendants irreparably harm Microsoft by damaging its reputation, brands, and customer goodwill. Tycoon 2FA Defendants' misuse of Microsoft brands and trademarks is meant to confuse Microsoft's customers into clicking on malicious links that they believe are associated with and owned by Microsoft. Because Tycoon 2FA Defendants impersonate Microsoft platforms and logins, victims will believe that they are protected. When the victim realizes that they have been attacked, he will believe that Microsoft is responsible for or complicit in the attack and customers may incorrectly attribute these problems to Microsoft's products and services, thereby diluting and tarnishing the value of these trademarks and brands.

73. Microsoft has invested considerable resources in developing high-quality products and services, including significant resources to combat Tycoon 2FA Defendants and other cybersecurity threats. Microsoft spent at least $925,000 and 5,000 hours investigating and

remediating Tycoon 2FA Defendants' activities, including engaging teams across the country. Through the development of flagship products used by millions of customers, Microsoft has thereby cultivated significant customer goodwill and globally recognized trademarks. Trademark registrations for marks infringed by Tycoon 2FA Defendants are attached as **Appendix B**.

74. A phishing attack where customers blame Microsoft involves a risk that customers may move from Microsoft's products and services because of the Tycoon 2FA Defendants and their activities. For customers who leave, there may be significant challenges to having such customers return, given the cost they bear to switch to new products and perceived risks. This causes injury to Microsoft.

IX. Harm to Health-ISAC and its Member Organizations

75. Health-ISAC has invested considerable resources in developing high-quality products and services, including significant resources to combat Tycoon 2FA Defendants and other cybersecurity threats. Health-ISAC and its member organizations spent at least $350,500 investigating and remediating Tycoon 2FA Defendants' activities.

76. SpyCloud data has identified at least 261 user accounts associated with 92 Health-ISAC member organizations that were successfully phished by Tycoon 2FA Defendants (successful phishing means that the credentials were captured by Defendants). At least two of the identified Health-ISAC organizations are located in the Southern District of New York.

77. As part of its investigation, Health-ISAC obtained data from 15 of the 92 member organizations. This data confirmed that 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. Of that, 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 users provided their credentials, which were successfully captured by Tycoon 2FA Defendants, before the accounts were locked to block any further malicious activity. The Health-ISAC member organizations subsequently detected this activity and were able to successfully reset the credentials before further malicious activity could occur.

78. Even where the employees of the member organization did not interact with the phishing emails, the Health-ISAC members' receipt of Tycoon 2FA phishing emails is a precursor to subsequent cybercriminal activity. 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.

79. When hospitals are attacked by ransomware, critical IT systems become unavailable and hospital services begin to decline rapidly, causing devastating consequences, including:

- 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 have led to the breach of sensitive health information; and

- Financial losses, including ransom payments to cybercriminals, legal fees, and regulatory fines.

COUNT I

Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030

(Microsoft; Health-ISAC)

80. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 79 above.

81. Tycoon 2FA Defendants knowingly and intentionally accessed and continue to access protected computers without authorization and through the use of stolen credentials, and knowingly caused the transmission of a program, information, code, and commands, resulting in damage to the protected computers of Microsoft, its customers, Health-ISAC, and its member organizations' including damage to the software and operating systems residing on the protected computers.

82. Tycoon 2FA Defendants' conduct involved interstate and/or foreign communications.

83. Tycoon 2FA Defendants' conduct has caused a loss to Plaintiffs during a one-year period aggregating at least $5,000. Specifically, Microsoft has incurred damage in excess of $925,000. The same harm has caused Health-ISAC members damage in excess of $350,400.

84. Microsoft and Health-ISAC seek injunctive relief and compensatory and punitive damages under 18 U.S.C. § 1030(g) in an amount to be proven at trial.

85. As a direct result of Tycoon 2FA Defendants' actions, Microsoft and Health-ISAC have suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Tycoon 2FA Defendants' actions are enjoined.

COUNT II

Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962

(Microsoft; Health-ISAC)

86. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 85 above.

87. Beginning in August 2023 and continuing up through the filing of this Complaint, Tycoon 2FA Defendants Saad Fridi and John Does 1-2 were and are associated in fact with the Racketeering Enterprise and have conducted their affairs through a pattern of racketeering activity, with such conduct and activities affecting interstate and foreign commerce. At various dates thereafter and continuing through the filing of this Complaint, Tycoon 2FA Defendants John Does 3-4 also became associated in fact with the Racketeering Enterprise and have conducted their affairs through a pattern of racketeering activity that affects interstate and foreign commerce.

88. Tycoon 2FA Defendants conduct their affairs through a pattern of racketeering activity affecting interstate and foreign commerce involving thousands of predicate acts of fraud including violations of (i) the Computer Fraud and Abuse Act (18 U.S.C. § 1030(a)(5)(A)), incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(G) and 18 U.S.C. § 2332b(g)(5)(B), and (ii) wire fraud (18 U.S.C. § 1343), incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(B).

89. Tycoon 2FA Defendants manufacture malicious phishing kits and operate a global technical infrastructure that supports credentials theft, information exfiltration, and subsequent end-user terminal attacks including business email compromise, ransomware, and financial fraud.

90. Tycoon 2FA Defendants, as members of the Racketeering Enterprise, share the common purpose of developing and operating a malicious technical infrastructure that proliferates

phishing attacks through the sale, distribution, deployment, and use of the Tycoon 2FA-branded phishing kits.

91. Tycoon 2FA Defendants have knowingly and with intent to defraud, possessed, and do possess, thousands of unauthorized access devices, including specifically credentials, 2FA tokens, and cookies, fraudulently obtained as described above, in violation of 18 U.S.C. § 1029.

92. Tycoon 2FA Defendants have knowingly and with intent to proliferate phishing kits used to steal, intercept and obtain credential information through access devices (including credentials, 2FA tokens, and cookies) defrauded Microsoft customers, including Health-ISAC member organization by sending emails impersonating Microsoft and its customers in order to lure victims to unknowingly providing login credentials to Tycoon 2FA Defendants, in violation of 18 U.S.C. § 1343. Tycoon 2FA Defendants have captured login credentials from victims with the intent to defraud, itself a predicate offense for a RICO action.

93. Microsoft and Health-ISAC have been and continues to be directly injured by Tycoon 2FA Defendants' conduct. But for the alleged pattern of racketeering activity, Microsoft and Health-ISAC would not have incurred harm.

94. Microsoft and Health-ISAC seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

COUNT III

Conspiracy to Violate the Racketeer Influenced and Corrupt Organizations Act (RICO), 18 U.S.C. § 1962(d)

(Microsoft; Health-ISAC)

95. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 94 above.

96. Beginning in or before August 2023 and continuing up through the filing of this Complaint, Tycoon 2FA Defendants, Saad Fridi and John Does 1-4, conspired to associate in fact with the Racketeering Enterprise and conduct its affairs through a pattern of racketeering activity, with such conduct and activities affecting interstate and foreign commerce. Tycoon 2FA Defendants further conspired to engage in an unlawful pattern of racketeering activity involving thousands of predicate acts of violations of (i) the Computer Fraud and Abuse Act (18 U.S.C. § 1030(a)(5)(A)), incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(G) and 18 U.S.C. § 2332b(g)(5)(B), and (ii) wire fraud (18 U.S.C. § 1343), incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(B).

97. The members of the Racketeering Enterprise conspired for the common purpose of developing malicious phishing kits and operating a global technical infrastructure that supports credential theft, information exfiltration, and subsequent end-user terminal attacks which include business email compromise, ransomware, and financial fraud.

98. Microsoft and Health-ISAC have been and continue to be directly injured by Tycoon 2FA Defendants' conduct. But for the alleged conspiracy to conduct a pattern of racketeering activity, Microsoft would not have incurred damages. Specifically, Microsoft has incurred over $925,000 in damages as a direct result of Tycoon 2FA Defendants' racketeering activity. Health-ISAC and its member organizations have incurred over $350,400 in damages as a direct result of the same racketeering activity.

99. Microsoft and Health-ISAC seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

COUNT IV

Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2701

(Microsoft; Health-ISAC)

100. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 99 above.

101. Microsoft's Windows operating system software and Microsoft's customers' computers running such software are facilities through which electronic communication services are provided to users and customers.

102. Tycoon 2FA Defendants knowingly and intentionally accessed the Windows operating system and Health-ISAC members network infrastructure and associated software, services, and computers upon which this software and services run without authorization or in excess of any authorization granted by Microsoft, including through the use of stolen credentials. Tycoon 2FA Defendants relentlessly attack Health-ISAC members through phishing campaigns and have knowingly and intentionally accessed the networks of Health-ISAC member organizations.

103. Through this unauthorized access, Tycoon 2FA Defendants intercepted, had access to, obtained and altered, and/or prevented legitimate, authorized access to, wire and electronic communications transmitted through the computers and infrastructure of Microsoft and its users.

104. Microsoft and Health-ISAC seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

105. As a direct result of Tycoon 2FA Defendants' actions, Plaintiffs have suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Tycoon 2FA Defendants' actions are enjoined.

COUNT V

False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a)

(Microsoft)

106. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 106 above.

107. Microsoft's trademarks are distinctive marks that are associated with Microsoft, and exclusively identify Microsoft's businesses, products, and services.

108. Tycoon 2FA Defendants make unauthorized use of Microsoft's trademarks. By doing so, Tycoon 2FA Defendants create false designations of origin as to tainted Microsoft's products and projects that are likely to cause confusion, mistake, or deception.

109. Because of their wrongful conduct, Tycoon 2FA Defendants are liable to Microsoft for violation of the Lanham Act, 15 U.S.C. § 1125(a).

110. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

111. As a direct result of Tycoon 2FA Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which it has no adequate remedy at law, and which will continue unless Tycoon 2FA Defendants' actions are enjoined.

COUNT VI

Trademark Infringement Under the Lanham Act, 15 U.S.C. § 1114 *et seq.*

(Microsoft)

112. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 111 above.

113. Tycoon 2FA Defendants have used Microsoft's trademarks in interstate commerce, including Microsoft's federally registered trademarks for the word marks Microsoft®, Windows®, Microsoft 365®, Office365®, Office®, Microsoft Office®, SharePoint®, OneDrive®, Outlook®, and Excel®. By doing so, Tycoon 2FA Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake and unauthorized versions of the Windows operating system and software. As a result of their wrongful conduct, Tycoon 2FA Defendants are liable to Microsoft for violations of the Lanham Act.

114. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

115. As a direct result of Tycoon 2FA Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which it has no adequate remedy at law, and which will continue unless Tycoon 2FA Defendants' actions are enjoined.

116. Tycoon 2FA Defendants' wrongful and unauthorized use of Microsoft's trademarks to promote, market, or sell products and services constitutes trademark infringement pursuant to 15 U.S.C. § 1114 *et seq*.

COUNT VII

Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c)

(Microsoft)

117. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 116 above.

118. Microsoft's trademarks are famous marks that are associated with Microsoft, and exclusively identify its businesses, products, and services.

119. Tycoon 2FA Defendants make unauthorized use of Microsoft's trademarks. By doing so, Tycoon 2FA Defendants are likely to cause dilution by tarnishment of Microsoft's trademarks.

120. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

121. As a direct result of Tycoon 2FA Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which it has no adequate remedy at law, and which will continue unless Tycoon 2FA Defendants' actions are enjoined.

COUNT VIII

Common Law Trespass to Chattels

(Microsoft; Health-ISAC)

122. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 121 above.

123. Tycoon 2FA Defendants have used a computer and/or computer network, without authority, with the intent to cause physical injury to the property of another.

124. Tycoon 2FA Defendants have, without authority, used a computer or computer network, without authority, with the intent to trespass on the computers and computer networks of Microsoft and its customers, including when Tycoon 2FA Defendants uses stolen credentials to access the account, spy on the account's content, and steal other sensitive information.

125. Tycoon 2FA Defendants' actions in offering the phishing kits result in unauthorized access through the use of stolen credentials to Microsoft's Windows operating system and the computers on which such programs run, and result in unauthorized intrusion into those computers and theft of information, account credentials, and funds.

126. Tycoon 2FA Defendants' actions in offering the phishing kits result in unauthorized access to Health-ISAC and its member organizations' email accounts and other non-public resources, and result in an unauthorized intrusion into those computers and theft of information and account credentials for the purpose of extracting sensitive information.

127. Tycoon 2FA Defendants intentionally caused this conduct, and this conduct was unlawful and unauthorized.

128. Tycoon 2FA Defendants' actions have caused injury to Microsoft and Health-ISAC and have interfered with the possessory interests of Microsoft over its software.

129. Microsoft and Health-ISAC seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

130. As a direct result of Tycoon 2FA Defendants' actions, Microsoft and Health-ISAC have suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Tycoon 2FA Defendants' actions are enjoined.

COUNT IX

Conversion

(Microsoft; Health-ISAC)

131. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 130 above.

132. Microsoft owns all right, title, and interest in its Windows software and the Microsoft 365, Outlook, and Azure software and services. Microsoft licenses its software to end-users. Tycoon 2FA Defendants have interfered with, unlawfully and without authorization, and dispossessed Microsoft of control over its Windows software and its Outlook, OneDrive, and Microsoft 365 software and services. Tycoon 2FA Defendants have also deprived Health-ISAC's

member organizations of control over their network infrastructure, as Tycoon 2FA has been able to use the ill-gotten sensitive information they received through their phishing operation to infiltrate the systems belonging to Health-ISAC's member organizations.

133. Defendants interfered with and converted computers running Windows operating systems and deprived Microsoft and its customers of possession and use of their property and systems.

134. Tycoon 2FA Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to remove, halt, or otherwise disable computer data, computer programs, and computer software from a computer or computer network.

135. Tycoon 2FA Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to cause a computer to malfunction.

136. Microsoft and Health-ISAC seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including without limitation the return of Tycoon 2FA Defendants' ill-gotten profits.

137. As a direct result of Tycoon 2FA Defendants' actions, Microsoft and Health-ISAC suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Tycoon 2FA Defendants' actions are enjoined.

COUNT X

Unjust Enrichment

(Microsoft; Health-ISAC)

138. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 137 above.

139. The acts of Tycoon 2FA Defendants complained of herein constitute unjust enrichment of the Tycoon 2FA Defendants at Plaintiffs' expense, in violation of the common law.

140. Tycoon 2FA Defendants used, without authorization or license, software belonging to Plaintiffs to facilitate unlawful conduct inuring to the benefit of Tycoon 2FA Defendants.

141. Tycoon 2FA Defendants profited unjustly from their unauthorized and unlicensed use of Microsoft's intellectual property.

142. Plaintiffs are informed, believe, and thereupon allege that Tycoon 2FA Defendants had an appreciation and knowledge of the benefit they derived from their unauthorized and unlicensed use of Microsoft's intellectual property and Health-ISAC's members' stolen information.

143. Retention by the Tycoon 2FA Defendants of the profits they derived from their malfeasance would be inequitable and unjust.

144. Microsoft and Health-ISAC seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including without limitation disgorgement of Tycoon 2FA Defendants' ill-gotten profits.

145. As a direct result of Tycoon 2FA Defendants' actions, Microsoft and Health-ISAC suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Tycoon 2FA Defendants' actions are enjoined.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that the Court enter judgment in their favor and against Defendants, as follows:

1. Awarding judgment in favor of Microsoft and against Defendants, for Plaintiffs' actual damages from Tycoon 2FA Defendants' activity complained of herein

and for any injuries complained of herein, including but not limited to interest and costs, in an amount to be proven at trial.

2. Declaring that Tycoon 2FA Defendants' conduct has been willful, and that Tycoon 2FA Defendants have acted with fraud, malice, and oppression.

3. Issuing a temporary restraining order and preliminary and permanent injunction enjoining Tycoon 2FA Defendants and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injuries complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activities complained of herein or from causing any of the injuries complained of herein.

4. Issuing a preliminary and permanent injunction giving Microsoft control over the domains used by Tycoon 2FA Defendants to cause injury and enjoining Tycoon 2FA Defendants from using such instrumentalities.

5. Entering judgment disgorging Tycoon 2FA Defendants' profits.

6. Entering judgment awarding enhanced, exemplary, and special damages, in an amount to be proved at trial.

7. Entering judgment awarding attorneys' fees and costs, and

8. Awarding such other relief that the Court deems just and proper.

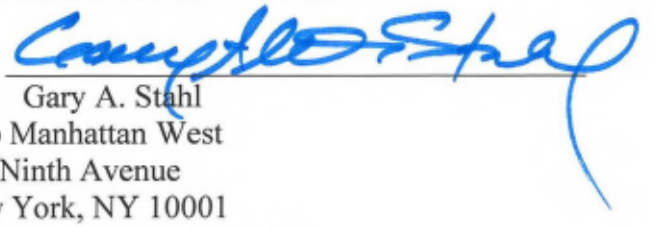
DEMAND FOR JURY TRIAL

Plaintiffs respectfully request a trial by jury on all issues so triable in accordance with Fed. R. Civ. P. 38.

Dated: February 24, 2026

Respectfully submitted,

CROWELL & MORING LLP

By: 

Gary A. Stahl
Two Manhattan West
375 Ninth Avenue
New York, NY 10001
Telephone: (212) 223-4000
Fax: (212) 223-4134
gstahl@crowell.com

Jeffrey L. Poston (*pro hac vice* forthcoming)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington, DC 20004
T: 202-624-2500
F: 202628-5116
JPoston@crowell.com

Amanda (Anna) Z. Saber (*pro hac vice* forthcoming)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
T: 415-986-2800
F: 415-986-2827
ASaber@crowell.com

Attorneys for Plaintiffs Microsoft Corporation and Health-ISAC