

SEALED

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

MICROSOFT CORPORATION and
HEALTH-ISAC, INC.,

Plaintiffs,

v.

YANG JIAN d/b/a YAM STORE, INC., and
DOES 1-10,

Defendants.

Case No. 1:26-cv-26998-JEM

FILED UNDER SEAL



COMPLAINT

Plaintiffs Microsoft Corporation (“Microsoft”) and Health-ISAC, Inc. (Health-ISAC) bring this action pursuant to the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (“CFAA”); the Stored Communications Act (18 U.S.C. § 2701 *et seq.*); the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and Florida common law. Defendants are a group of cybercriminals abusing Microsoft technology and services to commit a wide range of crimes against Microsoft customers, Health-ISAC members, and other victims around the world.

Defendant JIAN procures and resells fraudulent Microsoft cloud services accounts to Defendants like DOES 1-10. DOES 1-10 then use these fraudulent accounts in connection with Chinese language phishing kits like “CoGUI” and “Iron Man” to steal login credentials and commit financial fraud. The phishing kits Defendants host, distribute, and use are designed to deceive victims by generating at scale malicious emails that appear to come from legitimate companies, non-profit organizations, and governmental entities. Through this action, Plaintiffs aim to disable core elements of Defendants’ technical infrastructure and to obtain discovery designed

to help identify the individuals responsible for operating a transnational criminal enterprise, referred to in this Complaint as the Transnational Chinese Cybercrime Enterprise, or “TCC Enterprise.”

NATURE OF THE ACTION

1. This action arises under the Computer Fraud and Abuse Act (CFAA 18 U.S.C. §§ 1030 *et seq.*); the Stored Communications Act (18 U.S.C. § 2701 *et seq.*); the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); and the Racketeer Influenced Corrupt Organizations Act (the RICO Act, 18 U.S.C. §§ 1961 *et seq.*). This action also arises under the common law of Florida with respect to Plaintiffs’ state law tort claims.

2. Plaintiffs seek compensatory damages and injunctive relief needed to disrupt Defendants’ unlawful conduct and operation of the global criminal conspiracy described in this complaint.

THE PARTIES

3. Plaintiff 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 is a leading provider of technology products and services, including computer software, internet services, websites, and email services.

4. Plaintiff Health-ISAC, also known as the Health Information Sharing and Analysis Center, is a non-profit corporation duly organized and existing under the laws of Florida, having its principal place of business in Orlando, Florida. Health-ISAC provides situational awareness around cyber and physical security threats to the Health Sector so that companies can detect, mitigate, and respond to ensure operational resilience. Health-ISAC connects thousands of health security professionals globally to share peer insights, real-time alerts, and best practices in a

trusted, collaborative environment.

5. Defendant YANG JIAN is a natural person doing business under the fictitious business names “Yam Store Inc.” and “YAM Store.” JIAN controls the website [yam\[.\]ink](http://yam[.]ink), which hosts a storefront through which JIAN sells unauthorized access to Microsoft and Google cloud environments. JIAN has sold unauthorized access to Microsoft Azure cloud tenants to cybercriminals like DOES 1-10. JIAN also has access to and/or control over the Telegram handles used to advertise and sell Microsoft Azure access through the Yam Store. JIAN also controls the domains used to operate the Yam Store website and back office functions (“Yam Store Domains.”). The Yam Store Domains are listed in **Appendix A** to this Complaint. JIAN is believed to be a resident of the People’s Republic of China (“PRC”) but his current address is unknown to Plaintiffs.

6. Plaintiffs are uncertain of the true names of the ten (10) DOE Defendants whose conduct is described in this Complaint and Plaintiffs accordingly sue them under the fictitious names DOES 1-10. Plaintiffs will amend this pleading to allege Defendants’ true names once they are ascertained with reasonable certainty through civil discovery and the exercise of due diligence.

7. A first group of “Infrastructure Provider Defendants” consists of the persons who provide the software, hosting environments, payment accounts, distribution channels, and related services for running the Yam Store marketplace, CoGUI, Ironman operations. Active Iron Man infrastructure includes control-panel-hosting domains and servers, installation and distribution domains, and a licensing server that controls who has access to Iron Man software and infrastructure. The Iron Man Phishing-as-a-Service (PaaS) domains (“Phishing Domains”) are identified in **Appendix B** to the complaint.

8. A second group of “Phishing Defendants” consists of the persons who use the

software, infrastructure, and services sold by the Infrastructure Provider Defendants to carry out phishing attacks and financial crimes. Together, the Infrastructure Provider Defendants and Phishing Defendants operate as a continuing transnational Chinese cybercrime enterprise (“TCC Enterprise”).

9. Defendant DOE 1 is an Infrastructure Provider Defendant. DOE 1 is a natural person and Chinese-speaking threat actor with access to and control over instrumentalities used in connection with the violations of law described in this Complaint, including at least source code for a phishing kit and related infrastructure sold by DOE 1 as part of a phishing-as-a-service (PaaS) business known as “CoGUI.” A foreign law enforcement agency made a controlled test purchase a CoGUI phishing system from DOE 1 in March 2026.

10. Defendant DOE 2 is an Infrastructure Provider Defendant. DOE 2 is a natural person with access to and control over instrumentalities used in connection with the violations of law described in this Complaint, including at least source code for a phishing kit and related infrastructure sold by DOE 2 as part of a phishing-as-a-service (PaaS) business known as “Iron Man.” DOE 2 also controls the Phishing Domains identified in Appendix B to the Complaint.

11. Defendant DOE 3 is a Phishing Defendant who has used at least 34 Microsoft tenants used to operate multiple instances of CoGUI phishing systems in 2026 targeting victims primarily located in the United States and Japan. DOE 3 also had control over or access to the malicious domains identified used to carry out phishing operations against American and Japanese businesses.

12. Defendant DOE 4 is a Phishing Defendant. DOE 4 is a natural person with access to and control over instrumentalities used in connection with the violations of law described in this Complaint, including at least one instance of a CoGUI phishing system used to victimize multiple

well-known international businesses headquartered in Japan.

13. Defendant DOE 5 is a Phishing Defendant and a natural person with access to and control over instrumentalities used in connection with the violations of law described in this Complaint, including at least one instance of a CoGUI phishing system used to victimize multiple American health care businesses who are members of Health-ISAC.

14. Defendant DOE 6 is a Phishing Defendant and/or Infrastructure Provider Defendant who created an instance of an Iron Man phishing system with pre-built templates intended to be used to impersonate the Hokkaido Metropolitan Police Department.

15. Defendant DOE 7 is a Phishing Defendant and a natural person with access to and control over instrumentalities used in connection with the violations of law described in this Complaint, including at least one instance of a CoGUI phishing system and one instance of an Ironman phishing system.

16. Defendant DOE 8 is a Phishing Defendant and natural person with access to and control over instrumentalities used in connection with the violations of law described in this Complaint, including at least one instance of an Ironman phishing system used to victimize multiple Japanese businesses.

17. Defendant DOE 9 is a Phishing Defendant and/or Infrastructure Provider Defendant and a natural person with access to and control over instrumentalities used in connection with the violations of law described in this Complaint, including at least one of the malicious domains used to conduct phishing operations from within Japan.

18. Defendant DOE 10 is a Phishing Defendant and/or Infrastructure Provider Defendant and a natural person with access to and control over instrumentalities used in connection with the violations of law described in this Complaint, including at least one of the malicious

domains used to conduct phishing operations from within the United States.

19. Defendants collectively operate and/or control infrastructure, software, and technical artifacts used to carry out the violations of law described in this Complaint. In addition, Defendants also each receive financial benefits from operation of the Yam Store Enterprise.

20. Each Defendant is responsible in some part for the occurrences alleged herein and the injuries resulting from such occurrences.

21. The actions taken by each Defendant individually were actions that the other Defendants authorized, controlled, benefited from, intended, and/or that each Defendant had the ability to authorize, control or direct. In the alternative, actions taken by each Defendant individually were actions that the other Defendants assisted with, participated in, benefited from, and/or encouraged.

22. Each Defendant aided and abetted in whole or in part the other Defendants in carrying out the conduct alleged in this Complaint.

23. Each Defendant was the agent of the others in carrying out the acts alleged in this Complaint and was acting in the course and scope of such agency with knowledge, permission, consent, and/or ratification of the other Defendants.

JURISDICTION AND VENUE

24. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises out of Defendants' violation of the Computer Fraud and Abuse Act (CFAA 18 U.S.C. §§ 1030 *et seq.*); the Stored Communications Act (18 U.S.C. §§ 2701 *et seq.*); the Lanham Act (15 U.S.C. §§ 1114, 1125(a),(c)); and the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. §§ 1961 *et seq.*). The Court has supplemental jurisdiction over Microsoft's Florida tort claim pursuant to 28 U.S.C. § 1367.

25. In carrying out the conduct described in this Complaint, Defendants have directed their acts toward the state of Florida and its residents, including residents of this judicial district.

26. Defendants have victimized multiple businesses located in the State of Florida, including at least one educational institution located in Miami.

27. In carrying out the conduct described in this Complaint, Defendants availed themselves of the privilege of conducting business in Florida and intended to use computers and wire services physically located in Florida and this judicial district. For example, Defendants contracted with and/or abused the services of Cloudflare, Inc., which operates data centers in 55 U.S. cities, including Miami, Jacksonville, Tampa, and Tallahassee. Defendants also intentionally targeted businesses, organizations, and persons located in Florida.

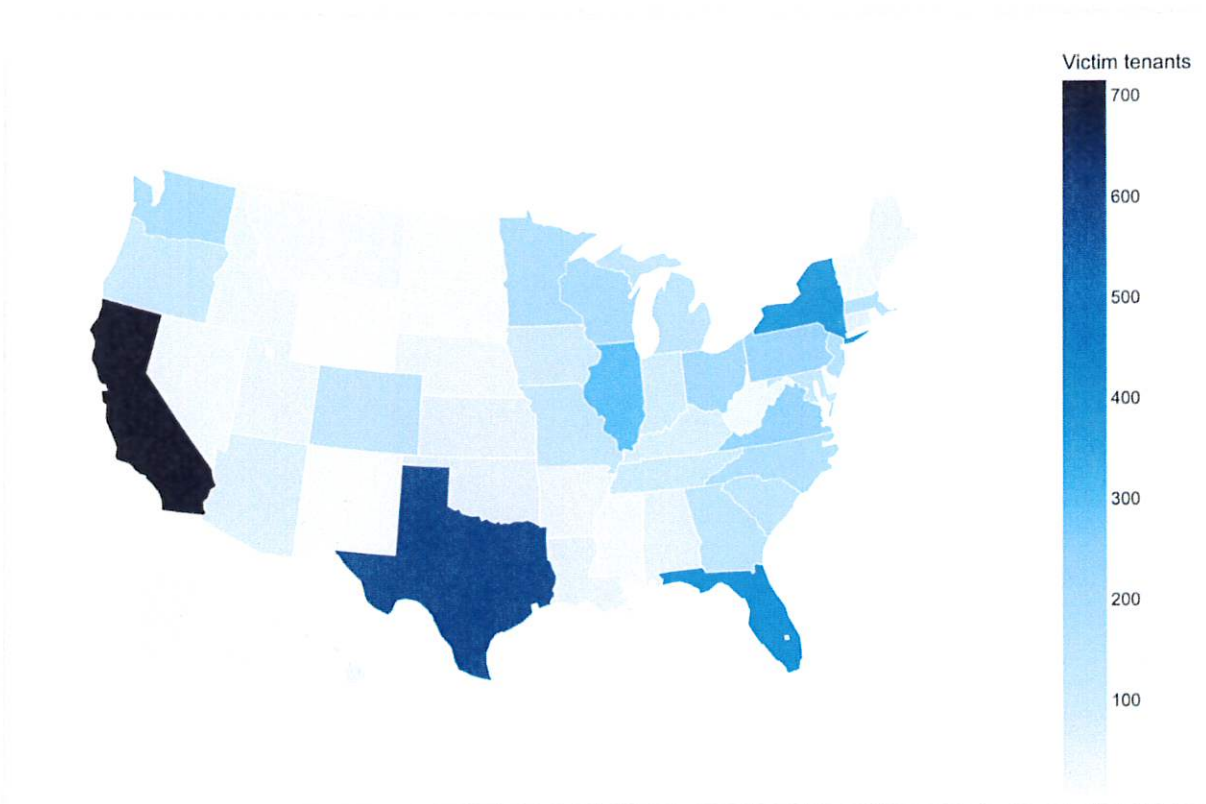
28. Defendants also have sufficient national contacts with the United States as a whole to subject each Defendant to the Court's jurisdiction consistent with requirements of due process. Defendants intentionally availed themselves of the privilege of doing business in the United States by contracting with and/or using the services of U.S.-based Domain Registries, hosting companies, and other infrastructure providers. For example, Defendants contracted with and/or abused the services of the following U.S.-based entities in order to set up the infrastructure used to carry out the conduct described in this complaint:

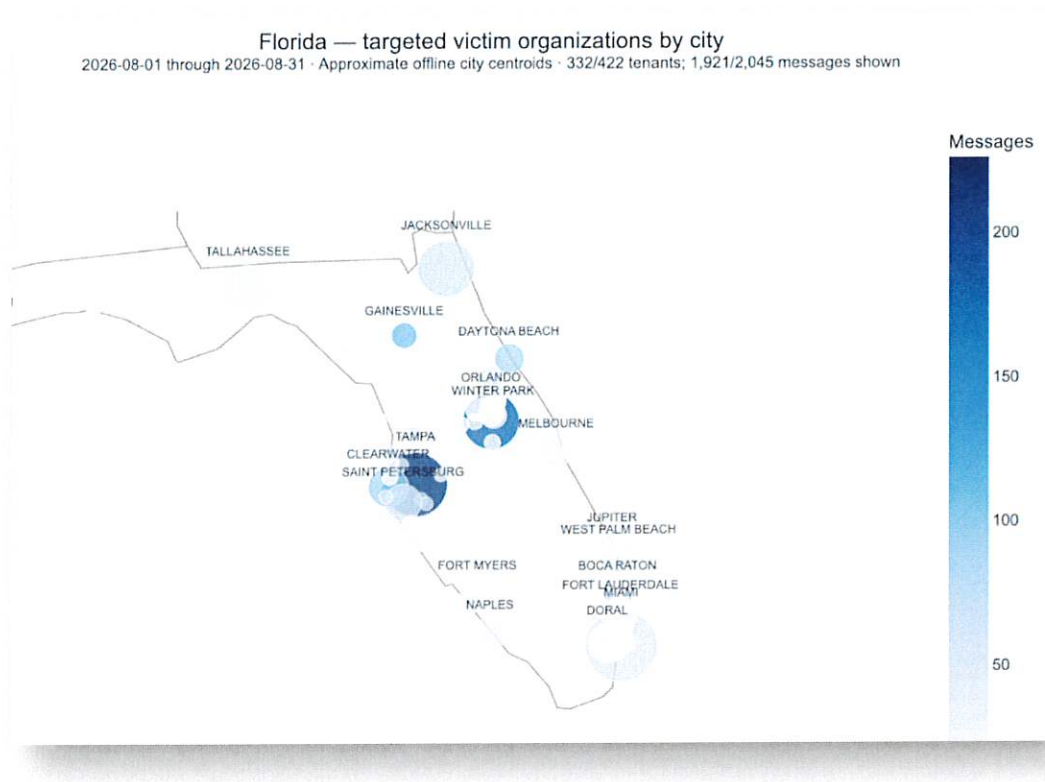
- Microsoft Corporation
- Cloudflare, Inc.
- GoDaddy Registry Operating Company, LLC
- Squarespace Domains II LLC
- Dropcatch.com

29. By using the services and infrastructure of Microsoft, GoDaddy, Squarespace,

Dropcatch, and Cloudflare, Defendants acted with the knowledge and intention that their acts would use computers and wire services located in the United States intended to use those instrumentalities to injure Plaintiff, its customers, and others residing in Florida and throughout the United States

30. Defendants also victimized at least thousands of victims in the United States. Defendants' intentional targeting of victims in the United States is reflected by the fact that a majority of Defendants' victims are U.S. persons and businesses. **Figure 1** below depicts the location of victims in the U.S. and in Florida.





FACTUAL BACKGROUND

31. Microsoft is the well-known creator and provider of some of the world's most popular software, including the Windows operating system and the Microsoft 365 suite of productivity tools.

32. Microsoft has invested in substantial resources in developing high-quality, secure products, and services. 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 developing the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized and trusted. Microsoft has registered trademarks representing the quality of its products and services and its brand, including the Microsoft®, Microsoft 365®, Azure®, and Outlook® marks. Microsoft uses these registered

marks alongside well-known and widely recognized logos for these products.

33. Microsoft hosts many of its products, including Microsoft 365, on Microsoft's Azure cloud environment. Launched in 2010, Azure is Microsoft's public cloud computing platform. It provides a global collection of cloud services that organizations use to build, deploy, manage, and scale applications, data platforms, AI solutions, and IT infrastructure without having to own and maintain all the underlying hardware. By offering businesses a global network of datacenters maintained and managed by Microsoft, Azure reduces the time and expense associated with maintaining on-premises infrastructure.

34. Azure offers more than 200 products and services across a global network of datacenters. With more than 400 highly secure datacenters in over 70 regions, Azure delivers the most extensive cloud footprint, giving businesses more regions to choose from than any other cloud provider. Businesses of all sizes from around the world rely on Azure, including 95% of Fortune 500 companies.

35. Most Azure cloud services fall into four broad categories: infrastructure as a service, platform as a service, serverless, and software as a service. These are sometimes called the cloud computing "stack" because they build on top of one another. The most basic category of cloud services is infrastructure as a service ("IaaS"), which allows customers to rent IT infrastructure like servers, virtual machines, storage, networks, and operating systems on a pay-as-you-go basis. Platform as a service ("PaaS") refers to cloud computing services that supply an on-demand environment for developing, testing, delivering, and managing software applications. PaaS is designed to make it easier for developers to quickly create web or mobile apps without worrying about setting up or managing the underlying infrastructure of servers, storage, network, and databases needed for development. Software as a service ("SaaS") is a method for delivering

software applications over the Internet on demand and typically on a subscription basis. With SaaS, cloud providers host and manage the software application and underlying infrastructure and handle any maintenance, like software upgrades and security patching. Users connect to the application over the Internet, usually with a web browser on their phone, tablet, or PC. Microsoft Azure provides all these types of services, both via its public cloud infrastructure and via hybrid cloud offerings (a type of cloud computing that combines on-premises infrastructure—or a private cloud—with a public cloud).

36. Some Azure services are provided free of charge, but most require payment. Microsoft provides predictable and transparent pricing models that let customers pay only for the cloud resources they use and scale as they grow. After agreeing to the Microsoft Customer Agreement, users wishing to access and use Azure resources and services must authenticate themselves with valid Microsoft-provided user credentials.

37. A person or company that wishes to use Azure services must first create an Azure account and user profile. Azure users must provide accurate location, name, and contact information and must agree to the Microsoft customer agreement. Among other things, the Microsoft Customer Agreement states:

Licenses for Products. Products are licensed and not sold. Upon Microsoft's acceptance of each order and subject to Customer's compliance with this Agreement, Microsoft grants Customer a nonexclusive and limited license to use the Products ordered as provided in this Agreement. These licenses are solely for Customer's own use and business purposes and are nontransferable except as expressly permitted under this Agreement or applicable law.

Duration of licenses. Online Services and some Software are licensed on a subscription basis for a specified period of time. Subscriptions expire at the end of the applicable subscription period unless renewed. Some Subscriptions renew automatically until canceled. The Subscription term for Online Services that are billed in arrears based on usage is the same as the billing period unless otherwise specified in the Product Terms. Perpetual Software licenses become perpetual upon payment in full.

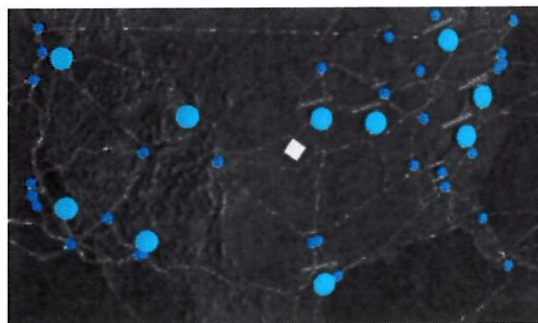
End Users. Customer will control access to, and use of, the Products by End Users and is responsible for any use of the Products that does not comply with this Agreement.

38. The Microsoft Customer Agreement also includes a “restrictions” section that expressly prohibits several categories of conduct:

Restrictions. Except as expressly permitted in this Agreement or Product documentation, Customer must not (and is not licensed to):

- (i) reverse engineer, decompile, or disassemble any Product or Services Deliverable, or attempt to do so (except where applicable law permits despite this limitation);
- (ii) install or use non-Microsoft software or technology in any way that would subject Microsoft’s intellectual property or technology to any other license terms;
- (iii) work around any technical limitations in a Product or Services Deliverable or restrictions in Product documentation;
- (iv) separate and run parts of a Product or Services Deliverable on more than one device;
- (v) upgrade or downgrade parts of a Product at different times;
- (vi) transfer parts of a Product separately; or
- (vii) distribute, sublicense, rent, lease, or lend any Products or Services Deliverables, in whole or in part, or use them to offer hosting services to a third party.

39. Azure global infrastructure includes access-controlled computers and networks that may only be accessed and used by authenticated customers. Azure datacenters and regional hubs are depicted below in **Figure 2**. In addition to the Microsoft-owned resources depicted in Figure 2, customers use their own computing resources and public Internet infrastructure to connect to and use Azure services.



40. Azure provides built-in security solutions designed to protect company’s workloads

from code to cloud. A dedicated team of more than 10,000 security experts continuously monitors systems, detects vulnerabilities, and tracks breach patterns and bad actors. The team synthesizes 78 trillion security signals daily with AI and advanced analytics to understand and protect against cyberthreats. Microsoft reinforces this commitment with a planned \$20 billion investment in security over the next five years.

41. One pillar of Azure's built-in security system is "Microsoft Entra," a family of identity and network access products that helps organizations implement a Zero Trust security strategy. Microsoft Entra is used to verify identities, validate access conditions, check permissions, encrypt connection channels, and monitor for compromise across customer environments.

42. "Microsoft Entra ID," Azure's central identity service, is a cloud-based identity and access management service that provides authentication, policy enforcement, and protection for users, devices, apps, and resources. Microsoft Entra ID Protection detects and reports identity-based risks. Administrators can investigate and automatically remediate risks using tools like risk-based Conditional Access policies. A "Microsoft Entra ID Free" license is included with Microsoft cloud subscriptions like Microsoft Azure and Microsoft 365.

43. Customers who obtain licenses to use Azure services are assigned a dedicated instance of Microsoft Entra ID that an organization or app developer receives at the beginning of a relationship with Microsoft. That relationship could start with signing up for Azure or Microsoft 365, for example.

44. A customer who purchases a subscription to Microsoft 365 is assigned a unique Microsoft 365 tenant. A Microsoft 365 tenant is a dedicated instance of the services and data for a particular organization, stored within a specific default location such as Europe or North America. Customers pick a region for their tenant when they set up their account. Each Microsoft 365 tenant

is distinct, unique, and separate from all other Microsoft 365 tenants.

45. Defendants collectively set up and use fraudulent Microsoft 365 tenants to engage in a wide range of criminal activities. Microsoft discovered Defendants' activities in the course of investigating a widespread phishing operations believed to be run by foreign nationals.

The Transnational Chinese Cybercrime ("TCC") Enterprise

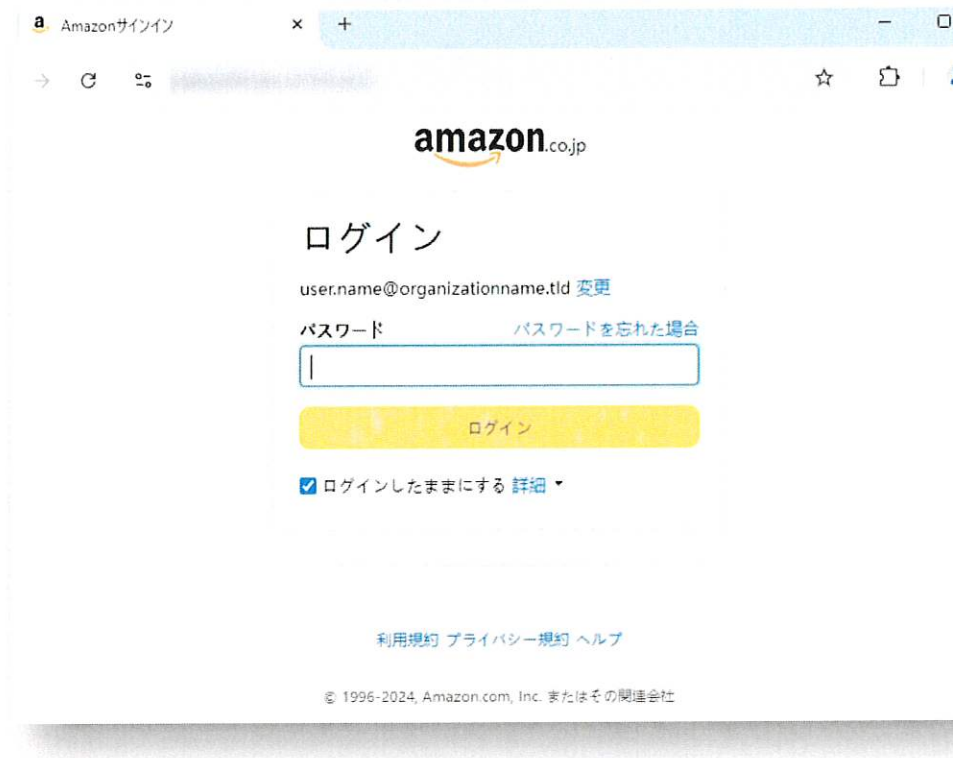
46. In mid-2025, Microsoft began investigating a group of Chinese-speaking threat actors offering a Phishing-as-a-Service (PaaS) product targeting U.S. and Japanese entities in particular. Primary industry verticals targeted by CoGUI operators include finance, retail, government, and educational institutions in Japan. This service, referred to as CoGUI by its creators, uses popular consumer and payment brands to create phishing lures designed to steal financial information and gain access to targeted organizations.

47. A CoGUI phishing kit distributed through various underground channels enables widespread attacks by multiple cybercriminals with minimal expertise. The kit allows easy swapping of branding and content to adapt to different victim groups and regions, underscoring its design as a scalable, high-risk phishing technology easily deployed across many industries. The CoGUI phishing kit can be easily installed on control servers to provide a dashboard for managing operations.

48. The CoGUI kit is designed to help users set up and manage fake websites and phishing messages designed to dupe victims into sharing password and other sensitive information. CoGUI users capture victim data through fake login pages and credentials like usernames, passwords, and payment details are automatically stored in the CoGUI dashboard. CoGUI users monetize stolen credentials through account takeover or credential resale.

49. Microsoft observed that the CoGUI kit is sold and used by multiple actors,

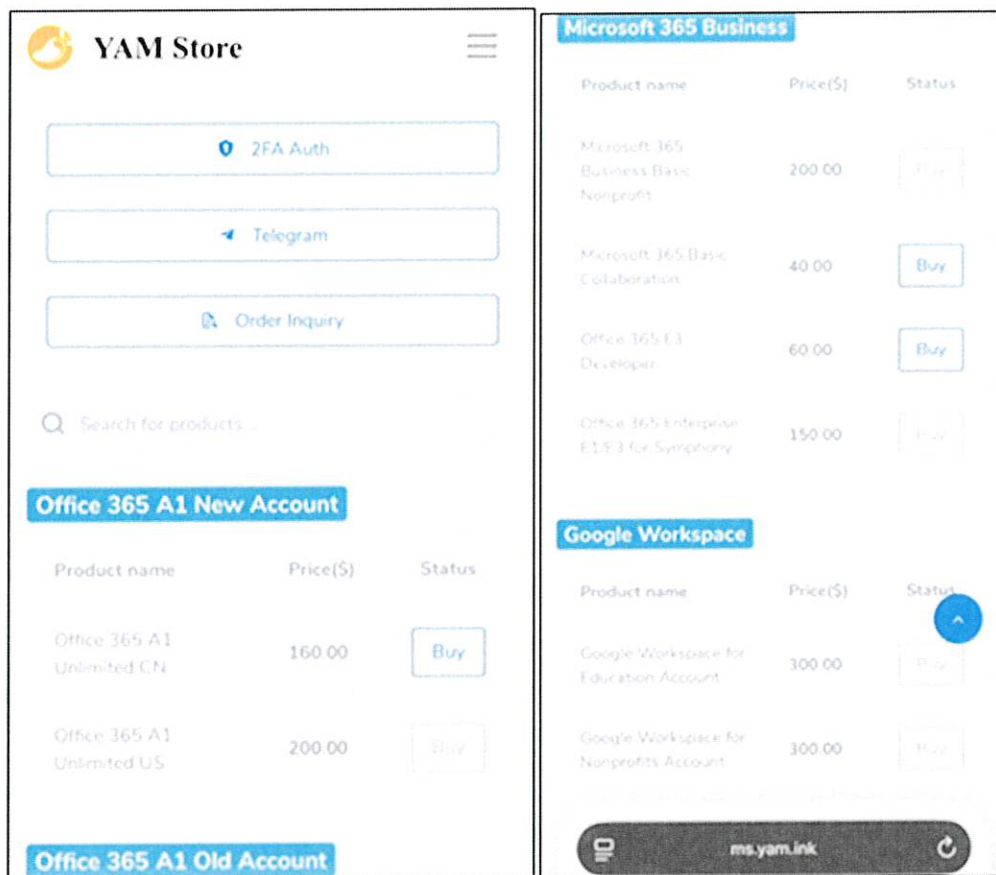
highlighting its widespread use as a commercial fraud service. Microsoft further observed that CoGUI drives millions of phishing messages, causing extensive harm especially in Japan. **Figure 3** below depicts a fake Amazon login page deployed by a CoGUI user to steal credentials from Japanese-speaking victims:



50. CoGUI users typically employ common tradecraft and infrastructure management techniques. Attackers register short-lived front-end domains resembling legitimate brands but switch domains frequently in order to reduce detection and takedown risks. However, Microsoft observed that some CoGUI users employ stable backend infrastructure, including backend infrastructure illegally hosted in fraudulent Azure tenants.

51. Microsoft's investigation into CoGUI Azure tenants lead Microsoft to discover a Chinese-speaking individual advertising access to Microsoft and Google infrastructure to other threat actors on criminal underground platforms on website labeled as "Yam Store." **Figure 4**

below is a compilation of screenshots taken from the main page of the Yam Store website:



52. Microsoft observed Yam Store offering a variety of Azure infrastructure products to buyers, including:

- Office 365 A1 Unlimited Licenses (China)
- Office 365 A1 Unlimited Licenses (USA)
- Microsoft 365 Business Basic Nonprofit
- Microsoft 365 Basic Collaboration
- Office 365 E3 Developer
- Office 365 Enterprise E1/E3 for Symphony

53. Yam Store is, of course, not authorized to sell or distribute any Microsoft products or services. On the contrary, Yam Store is violating the Azure services agreement by selling fraudulent or compromised tenant subscriptions.

54. Microsoft's investigation into Yam Store revealed that it is operated by Defendant YANG JIAN. JIAN has used several techniques to bypass security detections used to prevent the creation of fraudulent Azure tenants.

55. One technique employed by JIAN involves impersonating non-profit organizations. This technique involves identifying a legitimate non-profit organization and setting up an account in that organization's name. Microsoft has observed JIAN and/or their affiliates leveraging Dropcatch.com, which is a service that helps users find expiring web domains. Using Dropcatch.com, JIAN waits for a legitimate organization's domain to expire and then uses Dropcatch.com's services to register the domain for JIAN in an automated manner. After taking control of the domain, JIAN and/or their affiliates create a fake website at the previously-legitimate-webpage URL and then use the website and other seemingly legitimate identifying information to set up fraudulent Microsoft 365 tenants. **Figure 5** below depicts a fake website created by JIAN or at JIAN's direction in connection with setting up a fraudulent Microsoft 365 tenant.



56. Another technique used by JIAN and/or their affiliates is to create fraudulent educational tenants. Using fake or compromised email addresses (commonly involving university-associated email domains), JIAN registers fraudulent educational accounts by masquerading as a student or teacher. Cybercriminals have long viewed educational institutions as attractive targets, and higher education institutions in particular face an especially challenging environment because of their decentralized technology structures that support academic freedom and innovation but also create inconsistencies in security controls that make it easier for bad actors to compromise or

impersonate legitimate educational email accounts.¹

57. Another technique used by JIAN involves compromising legitimate customer accounts. Using stolen credentials, JIAN gains access to Microsoft's Azure infrastructure and the customer accounts residing on that infrastructure. JIAN impersonates legitimate customers and sets up new tenants or sells existing tenants to customers that can then use the legitimate customer's account to engage in criminal activity.

58. Using the techniques described above, JIAN and/or their affiliates set up hundreds of fraudulent tenants for resale to criminal end users. Buyers can purchase Yam Store offerings using several cryptocurrency types: USDT via TRON (TRC-20) networks; USDT via Ethereum (ERC-20) networks; USDT via Binance Smart Chain (BEP-20) networks; and USDC via Ethereum (ERC-20) networks. Once purchased, buyers are provided with credentials to access the resource. Buyers are typically provided with an account with Global Administrator role permissions.

59. JIAN sold unauthorized Azure tenants to DOE 1 or DOE 1's customer in order to enable operation of a CoGUI PaaS system. Thereafter, DOE 1 or its customer used the unauthorized Azure tenant to operate a CoGUI PaaS system and send malicious phishing emails to recipients in the United States. At its peak, DOE 1's CoGUI PaaS infrastructure was responsible for sending over sixty-five thousand malicious phishing email messages per day to Microsoft customers.

60. Many users of JIAN and DOE 1's services focused their phishing activities on victims located in the U.S. or Japan. For example:

- Defendant DOE 3 used at least 34 Microsoft tenants used to operate multiple

¹ <https://www.securityinfowatch.com/school-security/article/55391823/when-ai-learns-to-lie-the-new-era-of-campus-phishing>

instances of CoGUI phishing systems in 2026 targeting victims primarily located in the United States and Japan.

- Defendant DOE 4 used at least one instance of a CoGUI phishing system used to victimize multiple well-known international businesses headquartered in Japan
- DOE 5 used a CoGUI phishing system used to victimize multiple American health care businesses who are members of Health-ISAC
- DOE 6 created an instance of an Iron Man phishing system with pre-built templates intended to be used to impersonate the Hokkaido Metropolitan Police Department
- DOE 7 used at least one instance of a CoGUI phishing system and one instance of an Ironman phishing system to victimize companies in the U.S.
- DOE 8 used at least one instance of an Ironman phishing system used to victimize multiple Japanese businesses
- DOE 9 used at least one of the malicious domains used to conduct phishing operations from within Japan
- DOE 10 used at least one of the malicious domains used to conduct phishing operations

61. The activities of JIAN and DOES 1-10 appear to be carried out primarily by Chinese-speaking threat actors. JIAN and DOES have been observed marketing and selling their respective services to threat actors in the Chinese-speaking criminal underground.

62. In mid-2026, a related kit of CoGUI named “Iron Man” began circulating in Chinese underground phishing forums.

63. Defendant operators of the CoGUI and Ironman PaaS systems have historically focused on attacking organizations in the U.S. and Japan, targeting a wide range of organizations in the consumer and government sectors with phishing lures designed to steal information and gain access to private network environments.

64. Analysis of the Ironman PaaS revealed over 2,335 phishing templates targeting primarily U.S. and Japanese businesses. These phishing kits contain lures designed to impersonate government entities, healthcare organizations, finance and banking sector business, transportation companies, and numerous ecommerce providers.

65. JIAN, via Yam Store, has generated over \$1 million in illicit proceeds as of August 2026. These monies have been paid to JIAN through a number of cryptocurrency wallets and cashed out through accounts with Binance, OKX, Kraken, and others.

66. Defendants have used Yam Store infrastructure to attack multiple Health-ISAC members. One Health-ISAC member suffered an intrusion into their protected computer systems after a member's user unknowingly clicked on a malicious link in a CoGUI phishing email.

67. Defendants have also used Yam Store infrastructure to attack multiple Japanese and U.S. businesses.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

Violations of the Lanham Act 15 U.S.C. §§ 1114 & 1125

68. Plaintiffs reallege and incorporate by this reference the allegations set forth in the paragraphs above.

69. Microsoft® is a registered trademark owned by Microsoft, U.S. Trademark Registration No. 1689468. The Microsoft® mark is famous, distinctive, and widely recognized by

the general consuming public of the United States as a designation of the source of goods or services.

70. Microsoft 365® is a registered trademark owned by Microsoft, U.S. Trademark Registration No. 6,701,693. The mark is famous, distinctive, and widely recognized by the general consuming public of the United States as a designation of the source of goods or services.

71. Office 365® is a registered trademark owned by Microsoft, U.S. Trademark Registration No. 4,380,754. The mark is famous, distinctive, and widely recognized by the general consuming public of the United States as a designation of the source of goods or services.

72. Defendants are importing, distributing, trafficking, and using non-genuine services bearing Microsoft's trademarks.

73. Defendants advertise their services using Microsoft's trademarks without authorization.

74. Defendants send fraudulent emails containing unauthorized and counterfeit copies of one or more Microsoft trademarks or affiliated logos in a manner that is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of Defendants and Microsoft, or of Microsoft's sponsorship, or approval of Defendants' goods, services, or commercial activities.

75. Defendants' conduct harms Microsoft's reputation and is likely to dilute by tarnishment Microsoft's famous marks.

76. Microsoft is entitled to actual damages in an amount to be proven at trial.

77. As a direct result of 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 Defendants' actions are enjoined.

78. Microsoft is entitled to an award of attorneys' fees on its trademark claim.

SECOND CLAIM FOR RELIEF

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

79. Plaintiffs reallege and incorporate by this reference the allegations set forth in the paragraphs above.

80. Defendants knowingly and intentionally accessed protected computers without authorization.

81. Defendants knowingly caused the transmission of a program, information, code and commands, resulting in damage to the protected computers.

82. Defendants knowingly and intentionally accessed protected computers without authorization with the intent to defraud victims into installation of a program, information, code and commands, resulting in damage to the protected computers.

83. Defendants knowingly and with intent to defraud accessed protected computers without authorization and by means of such conduct furthered the intended fraud and obtained money or things of value.

84. Defendants' conduct injures Microsoft and its customers.

85. Defendants' conduct injures Health-ISAC and its members.

86. Microsoft has invested substantial time, money, and human resources in remediating Defendants' unlawful computer access and distribution of malicious software.

87. Defendants' conduct involved interstate and foreign communications.

88. Defendants' conduct has caused a loss during a one-year period aggregating more than \$5,000.

89. Plaintiffs seek injunctive relief and compensatory and punitive damages under 18

U.S.C. §1030(g) in an amount to be proven at trial.

90. As a direct result of 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 Defendants' actions are enjoined.

THIRD CLAIM FOR RELIEF

Violations of the Stored Communications Act, 18 U.S.C. § 2701

91. Plaintiffs reallege and incorporate by this reference the allegations set forth in the paragraphs above.

92. Microsoft's Azure-hosted Outlook email services, including email services used by Health-ISAC member organizations compromised by Defendants, comprise an electronic communication service provided to users.

93. Defendants successfully compromised the email systems of a Health-ISAC member organization and a Microsoft customer located in Florida.

94. Defendants knowingly and intentionally accessed without authorization Microsoft communications infrastructure and computers hosting customer Outlook email accounts.

95. Through their unauthorized access, Defendants had access to, obtained and altered, and/or prevented legitimate, authorized access to, wire and electronic communications transmitted through the computers and communications infrastructure of Microsoft and its users and stored email messages contained in customer Outlook email accounts.

96. Defendants used their unauthorized access to gain access to the contents of wire and electronic communications, including access to sensitive financial information.

97. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

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

FOURTH CLAIM FOR RELIEF

Violations of the Racketeer Influenced and Corrupt Organizations Act (RICO)

99. Plaintiffs reallege and incorporate by this reference the allegations set forth in the paragraphs above.

100. Defendants form an enterprise in fact and are conducting the affairs of the Yam Store Enterprise through a pattern of racketeering conduct that includes numerous violations of 18 U.S.C. § 2320 and 18 U.S.C. § 1343 over at least the period of time from January 2026 to present.

101. Each Defendant is using one or more of the instrumentalities described herein to continuously commit wire fraud and criminal trademark infringement in violation of federal law.

102. Defendants have conspired to conduct the affairs of the Yam Store Enterprise through a pattern of racketeering and each has taken steps in furtherance of that conspiracy.

103. Defendants have each invested in or contributed to, directly or indirectly, income derived from a pattern of racketeering, or the proceeds of such income, in the operation of the Yam Store Enterprise.

104. The Yam Store Enterprise's members function as a continuing unit for the common purpose of achieving the objectives of the Enterprise, including the common objectives of wire fraud and unauthorized distribution of counterfeit marks.

105. Defendants have conducted the affairs of the Yam Store Enterprise through a coordinated and continuous pattern of illegal activity in order to achieve their common unlawful purposes.

106. The Yam Store Enterprise has engaged in activities that affect interstate commerce through a pattern of racketeering activity.

107. Defendants continuously and effectively carried out the purpose of the Yam Store Enterprise from at least mid-2025 to present, causing harm to the business and property of Microsoft and others. Defendants represent a continuing threat to Microsoft and others.

108. **Wire Fraud** (18 U.S.C. § 1343). At some point prior to January 1, 2026, Defendants devised a scheme to obtain money or property from Microsoft customers and others, and to defraud Microsoft customers and others.

109. For example, JIAN fraudulently misrepresented their identity in order to create hundreds of fraudulent Azure tenants.

110. In addition, multiple Defendants participated in the scheme to use misrepresentation and deceit to lure victims into providing account login credentials in order to facilitate financial crimes and fraud.

111. Defendants transmitted and/or caused to be transmitted by means of wire communication in interstate and foreign commerce writings, signals, and pictures for the purpose of executing their scheme to defraud. For example, on numerous occasions after January 1, 2026, Defendants transmitted by means of wire communication in interstate and foreign commerce deceptive emails fraudulently using trademarks, names, and logos belonging to legitimate organizations. These emails were designed to deceive victims into clicking malicious links. Defendants continue to use communications transmitted by means of wire communication in interstate and foreign commerce in furtherance of their scheme to this day.

112. **Criminal Trademark Infringement** (18 U.S.C. § 2320). Defendants have intentionally and knowingly used one or more counterfeit marks on or in connection with goods

or services trafficked in the United States.

113. Defendants have engaged in similar unlawful conduct in the past and that at least two Defendants are known associates of one another. Defendants' preexisting associations and pattern of unlawful activity make them a continuing risk for conducting the affairs of the Enterprise through a pattern of racketeering.

114. The conduct described above has caused harm to Microsoft's businesses and property in an amount to be computed at trial.

115. The conduct described above was willful and with knowledge of wrongdoing. Plaintiffs are entitled to and hereby demands treble damages, attorneys' fees, and costs of suit in addition to preliminary and permanent injunctive relief.

FIFTH CLAIM FOR RELIEF

Tortious Interference

116. Plaintiffs reallege and incorporate by this reference each and every allegation set forth in the paragraphs above.

117. Microsoft has valid and subsisting contracts with its customers who are users of its Azure, Microsoft 365, and Office 365 products.

118. Defendants have knowledge of Microsoft's contracts with its customers.

119. Defendants wrongfully interfered with Microsoft's contracts with its customers, making it harder for Microsoft and its customers to comply with their respective contractual obligations and obtain their respective benefits under the contracts.

120. Microsoft and its customers have been harmed by Defendants' interference with Microsoft's contracts with its customers.

121. The conduct described above was willful and with knowledge of wrongdoing.

122. Microsoft is entitled to damages caused by Defendants' tortious interference in an

amount to be proven at trial.

123. As a direct result of 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 Defendants' actions are enjoined.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray that the Court:

1. Enter judgment in favor of Plaintiffs and against the Defendants;
2. Declare that Defendants' conduct has been willful and that Defendants have acted with fraud, malice and oppression;
3. Enter a preliminary and permanent injunction enjoining 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 injury complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein;
4. Enter a preliminary and permanent injunction isolating and securing the infrastructure, including the software operating from and through the infrastructure, outside of the control of Defendants or their representatives or agents;
5. Enter judgment awarding Plaintiffs actual damages in an amount to be proven at trial;
6. Enter judgment in favor of Plaintiffs disgorging Defendants' profits; and
7. Order such other relief that the Court deems just and reasonable.

Dated: October 6, 2026

Respectfully submitted,



Markenzy Lapointe

Markenzy Lapointe (Florida Bar No. 172601)
PILLSBURY WINTHROP SHAW PITTMAN LLP
600 Brickell Avenue, Ste. 2600
Miami, FL 33131
Tel: (786) 913-4805
markenzy.lapointe@pillsburylaw.com

Robert L. Uriarte (*pro hac vice* forthcoming)
PILLSBURY WINTHROP SHAW PITTMAN LLP
725 South Figueroa Street, 36th Floor
Los Angeles, CA 90017
Tel: (213) 488-3619
robert.uriarte@pillsburylaw.com

Kayvan M. Ghaffari (*pro hac vice* forthcoming)
PILLSBURY WINTHROP SHAW PITTMAN LLP
Four Embarcadero Center, 22nd Floor
San Francisco, CA 94111
Tel: (415) 983-1144
kayvan.ghaffari@pillsburylaw.com

Alexis N. Wansac (*pro hac vice* forthcoming)
PILLSBURY WINTHROP SHAW PITTMAN LLP
1200 17th Street NW
Washington, DC 20036
Tel: (202) 663-8144
alexis.wansac@pillsburylaw.com

Alexandria C. Marx (*pro hac vice* forthcoming)
PILLSBURY WINTHROP SHAW PITTMAN LLP
2400 Hannover Street
Palo Alto, California 94304
Tel: (650) 233-4009
alexandria.marx@pillsburylaw.com

Attorneys for Plaintiffs

Of Counsel:

Richard Boscovich
MICROSOFT CORPORATION
Microsoft Redwest Building C

5600 148th Ave NE
Redmond, Washington 98052
Tel: (425) 704-0867
rbosco@microsoft.com

Attorney for Microsoft Corp.

APPENDIX A — YAM STORE DOMAINS

yam[.]ink
upay.yam[.]ink
2fa.yam[.]ink
tokenpay.yam[.]ink
ms.yam[.]ink
shop.yam[.]ink
blog.yam[.]ink
mail.yam[.]ink
pay.yam[.]ink
pan.yam[.]ink
vip.yam[.]ink
e5.yam[.]ink
clash.yam[.]ink
od.yam[.]ink

APPENDIX B — PHISHING DOMAINS

loveboy[.]xyz
install.loveboy[.]xyz
docker.loveboy[.]xyz
aidchildren[.]cc
docker.aidchildren[.]cc
peaceman[.]cc
peaceloving[.]xyz
docker[.]peaceloving[.]xyz
log.peaceloving[.]xyz
log1.peaceloving[.]xyz
log2.peaceloving[.]xyz
api2.peaceman[.]cc
apinew.peaceman[.]cc
app.peaceman[.]cc
bin.peaceman[.]cc
bin1.peaceman[.]cc
bin2.peaceman[.]cc
ipapi.peaceman[.]cc
ipapi1.peaceman[.]cc
ipapi2.peaceman[.]cc

APPENDIX C — TRADEMARK REGISTRATION CERTIFICATES

United States of America

United States Patent and Trademark Office

OFFICE 365

Reg. No. 4,380,754

Registered Aug. 6, 2013

Int. Cl.: 39

SERVICE MARK

PRINCIPAL REGISTER

MICROSOFT CORPORATION (WASHINGTON CORPORATION)
ONE MICROSOFT WAY
REDMOND, WA 980526399

FOR: ELECTRONIC STORAGE OF FILES AND DOCUMENTS, IN CLASS 39 (U.S. CLS. 100 AND 105).

FIRST USE 10-19-2010; IN COMMERCE 10-19-2010.

THE MARK CONSISTS OF STANDARD CHARACTERS WITHOUT CLAIM TO ANY PARTICULAR FONT, STYLE, SIZE, OR COLOR.

OWNER OF U.S. REG. NOS. 2,841,438, 3,625,391, AND OTHERS.

NO CLAIM IS MADE TO THE EXCLUSIVE RIGHT TO USE "OFFICE", APART FROM THE MARK AS SHOWN.

SN 85-467,634, FILED 11-8-2011.

SETH A. RAPPAPORT, EXAMINING ATTORNEY



Steven Street
Acting Director of the United States Patent and Trademark Office

**REQUIREMENTS TO MAINTAIN YOUR FEDERAL
TRADEMARK REGISTRATION**

**WARNING: YOUR REGISTRATION WILL BE CANCELLED IF YOU DO NOT FILE THE
DOCUMENTS BELOW DURING THE SPECIFIED TIME PERIODS.**

Requirements in the First Ten Years*

What and When to File:

First Filing Deadline: You must file a Declaration of Use (or Excusable Nonuse) between the 5th and 6th years after the registration date. *See* 15 U.S.C. §§1058, 1141k. If the declaration is accepted, the registration will continue in force for the remainder of the ten-year period, calculated from the registration date, unless cancelled by an order of the Commissioner for Trademarks or a federal court.

Second Filing Deadline: You must file a Declaration of Use (or Excusable Nonuse) **and** an Application for Renewal between the 9th and 10th years after the registration date.*
See 15 U.S.C. §1059.

Requirements in Successive Ten-Year Periods*

What and When to File:

You must file a Declaration of Use (or Excusable Nonuse) **and** an Application for Renewal between every 9th and 10th-year period, calculated from the registration date.*

Grace Period Filings*

The above documents will be accepted as timely if filed within six months after the deadlines listed above with the payment of an additional fee.

**The United States Patent and Trademark Office (USPTO) will NOT send you any future notice or
reminder of these filing requirements.**

***ATTENTION MADRID PROTOCOL REGISTRANTS:** The holder of an international registration with an extension of protection to the United States under the Madrid Protocol must timely file the Declarations of Use (or Excusable Nonuse) referenced above directly with the USPTO. The time periods for filing are based on the U.S. registration date (not the international registration date). The deadlines and grace periods for the Declarations of Use (or Excusable Nonuse) are identical to those for nationally issued registrations. *See* 15 U.S.C. §§1058, 1141k. However, owners of international registrations do not file renewal applications at the USPTO. Instead, the holder must file a renewal of the underlying international registration at the International Bureau of the World Intellectual Property Organization, under Article 7 of the Madrid Protocol, before the expiration of each ten-year term of protection, calculated from the date of the international registration. *See* 15 U.S.C. §1141j. For more information and renewal forms for the international registration, see <http://www.wipo.int/madrid/en/>.

NOTE: Fees and requirements for maintaining registrations are subject to change. Please check the USPTO website for further information. With the exception of renewal applications for registered extensions of protection, you can file the registration maintenance documents referenced above online at <http://www.uspto.gov>.

United States of America

United States Patent and Trademark Office

MICROSOFT 365

Reg. No. 6,701,693

Registered Apr. 12, 2022

Int. Cl.: 9, 35, 37, 38, 41, 42

Service Mark

Trademark

Principal Register

Microsoft Corporation (WASHINGTON CORPORATION)
ONE MICROSOFT WAY
REDMOND, WASHINGTON 98052

CLASS 9: computer software and computer programs for database management, data storage and backup, virtualization, networking, collaboration, remote access, remote support, cloud computing, data sharing, data security, access, administration and management of computer applications and computer hardware, computer application distribution, and for transmission of voice, data, images, audio, video, and information, and for content management, online project management, creating, offering, hosting, and delivering online conferences, meetings, demonstrations, tours, presentations and interactive discussions, word processing programs, and operating system programs; computer software, namely, a full line of computer software for business productivity, business IT service management, business computer devices management, business IT security management, business administration and management, accounting, and marketing in the fields of business, and computer software to facilitate e-commerce business transactions via a global computer network; computer operating system software; network access server operating software; computer programs for managing communications and data exchange between computers and electronic devices; computer network security, anti-virus protection, and intrusion detection and prevention; computer graphics and graphical user interface software; wireless communications devices, namely, mobile phones, cellular telephones, personal digital assistants, and hand-held computers; computer software development tools; website development software; computer software that provides web-based access to applications and services through a web operating system or portal interface; computer software for developing and operating cloud computer networks and applications; computer software for computer system and application development, deployment and management; computer hardware and software for monitoring automobiles performance, for mapping and navigation, for electronic mail and wireless communications, for maintaining personal directories, contact lists, address and telephone number lists

FIRST USE 7-10-2017; IN COMMERCE 7-10-2017

CLASS 35: business services, namely, business consultation services, business advice and information services; business marketing services; and business consulting services; providing business information



Dennis H. H. [Signature]

Performing the Functions and Duties of the
Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office



FIRST USE 7-10-2017; IN COMMERCE 7-10-2017

CLASS 37: consultancy concerning installation, maintenance and repair of computer hardware

FIRST USE 7-10-2017; IN COMMERCE 7-10-2017

CLASS 38: telecommunications services, namely, providing on-line chat rooms for the transmission of messages among users in the field of general interest; voice chat services; electronic transmission and streaming of digital media, messages, documents, images, music, games and data; voice over internet protocol services; video-on-demand transmission services; providing online chat rooms and electronic bulletin boards for transmission of messages among users concerning business services, listings for announcements, events, meetings, activities, politics, family, arts and information on a wide variety of topics of general interest to the public and consultancy services, for all of the aforesaid services

FIRST USE 7-10-2017; IN COMMERCE 7-10-2017

CLASS 41: providing education and training services, namely, classes, seminars, workshops, and non-downloadable webinars in the field of computers and computer technology; arranging and conducting educational conferences and exhibitions in the field of computer technology; providing information over computer networks and global communication networks in the fields of entertainment, music, interactive games, movies, sports, news relating to current events, and arts and culture; information, advice and consultancy services relating to the aforesaid services

FIRST USE 7-10-2017; IN COMMERCE 7-10-2017

CLASS 42: computer services, namely, providing technical support, information and consultation services, namely, troubleshooting in the nature of diagnosing problems in computer hardware, computer software and computer operating systems; computer hardware and software testing services; computer services, namely, providing software updates via computer networks and global communication networks; computer services, namely, providing on-line non-downloadable software for database management, data storage and backup, virtualization, networking, collaboration, remote access, remote support, cloud computing, data sharing, data security, access, administration and management of computer applications and computer hardware, computer application distribution, and for transmission of voice, data, images, audio, video, and information, and for content management, online project management, creating, offering, hosting, and delivering online conferences, meetings, demonstrations, tours, presentations and interactive discussions, word processing programs, operating system programs; electronic data storage; cloud services, namely, providing on-line non-downloadable operating software for accessing and using a cloud computing network; cloud hosting provider services; computer security services, namely, enforcing, restricting and controlling access privileges of users of computing resources for cloud resources based on assigned credentials, integration of private and public cloud computing environments, remote and on-site infrastructure management services for monitoring, administration and management of public and private cloud computing it and application systems; providing virtual computer systems and virtual computer environments through cloud computing; application service provider (asp), namely, providing, hosting, managing, developing, and maintaining applications, software, web sites, and databases of others; providing technical information in the fields of design, development, programming, customization, selection, and implementation of computers, computer software, and computer networks, and information regarding diagnosing computer hardware and software problems and regarding the maintenance and updating of computer software, and the development and operation of computer systems, software and networks; computer software consulting services; consultancy in the design and development of computer hardware; consulting in the field of information technology; consulting in the field of cloud computing networks and

applications; design and development of networks and network software and applications; leasing computer facilities; electronic storage of files and documents; electronic storage of files, documents and databases; technology consultancy services in the field of development of computer software; platform-as-a-service (paas), infrastructure-as-a-service (iaas) and software-as-a-service (saas) services featuring computer software platforms for creating web applications, data storage and backup, database management, virtualization, networking, collaboration, remote access, remote support, cloud computing, data sharing, data security, access, administration and management of computer applications and computer hardware, computer application distribution, and for transmission of voice, data, images, audio, video, and information, and for content management, online project management, creating, offering, hosting, and delivering online conferences, meetings, demonstrations, tours, presentations and interactive discussions; computer services, namely, creating cloud-based indexes of information; computer hardware and software development

FIRST USE 7-10-2017; IN COMMERCE 7-10-2017

THE MARK CONSISTS OF STANDARD CHARACTERS WITHOUT CLAIM TO ANY PARTICULAR FONT STYLE, SIZE OR COLOR

PRIORITY CLAIMED UNDER SEC. 44(D) ON AZERBAIJAN APPLICATION NO. 201733579, FILED 05-17-2017

SER. NO. 87-640,393, FILED 10-10-2017

REQUIREMENTS TO MAINTAIN YOUR FEDERAL TRADEMARK REGISTRATION

WARNING: YOUR REGISTRATION WILL BE CANCELLED IF YOU DO NOT FILE THE DOCUMENTS BELOW DURING THE SPECIFIED TIME PERIODS.

Requirements in the First Ten Years*

What and When to File:

- **First Filing Deadline:** You must file a Declaration of Use (or Excusable Nonuse) between the 5th and 6th years after the registration date. See 15 U.S.C. §§1058, 1141k. If the declaration is accepted, the registration will continue in force for the remainder of the ten-year period, calculated from the registration date, unless cancelled by an order of the Commissioner for Trademarks or a federal court.
- **Second Filing Deadline:** You must file a Declaration of Use (or Excusable Nonuse) and an Application for Renewal between the 9th and 10th years after the registration date.* See 15 U.S.C. §1059.

Requirements in Successive Ten-Year Periods*

What and When to File:

- You must file a Declaration of Use (or Excusable Nonuse) and an Application for Renewal between every 9th and 10th-year period, calculated from the registration date.*

Grace Period Filings*

The above documents will be accepted as timely if filed within six months after the deadlines listed above with the payment of an additional fee.

***ATTENTION MADRID PROTOCOL REGISTRANTS:** The holder of an international registration with an extension of protection to the United States under the Madrid Protocol must timely file the Declarations of Use (or Excusable Nonuse) referenced above directly with the United States Patent and Trademark Office (USPTO). The time periods for filing are based on the U.S. registration date (not the international registration date). The deadlines and grace periods for the Declarations of Use (or Excusable Nonuse) are identical to those for nationally issued registrations. See 15 U.S.C. §§1058, 1141k. However, owners of international registrations do not file renewal applications at the USPTO. Instead, the holder must file a renewal of the underlying international registration at the International Bureau of the World Intellectual Property Organization, under Article 7 of the Madrid Protocol, before the expiration of each ten-year term of protection, calculated from the date of the international registration. See 15 U.S.C. §1141j. For more information and renewal forms for the international registration, see <http://www.wipo.int/madrid/en/>.

NOTE: Fees and requirements for maintaining registrations are subject to change. Please check the USPTO website for further information. With the exception of renewal applications for registered extensions of protection, you can file the registration maintenance documents referenced above online at <http://www.uspto.gov>.

NOTE: A courtesy e-mail reminder of USPTO maintenance filing deadlines will be sent to trademark owners/holders who authorize e-mail communication and maintain a current e-mail address with the USPTO. To ensure that e-mail is authorized and your address is current, please use the Trademark Electronic Application System (TEAS) Correspondence Address and Change of Owner Address Forms available at <http://www.uspto.gov>.

Int. Cl.: 42

Prior U.S. Cls.: 100 and 101

Reg. No. 1,689,468

United States Patent and Trademark Office Registered May 26, 1992

**SERVICE MARK
PRINCIPAL REGISTER**

MICROSOFT

MICROSOFT CORPORATION (DELAWARE
CORPORATION)
ONE MICROSOFT WAY
REDMOND, WA 980526399

FOR: COMPUTER PROGRAMMING SERVICES; CONSULTING AND TECHNICAL SUPPORT SERVICES IN THE FIELD OF THE DESIGN AND USE OF COMPUTER PROGRAMS, COMPUTERS, COMPUTER HARDWARE AND COMPUTER SYSTEMS; MAIL ORDER SERVICES IN THE FIELD OF COM-

PUTER PROGRAMS, COMPUTER RELATED BOOKS AND PUBLICATIONS, AND OTHER COMPUTER RELATED PRODUCTS, IN CLASS 42 (U.S. CLS. 100 AND 101).

FIRST USE 8-30-1990; IN COMMERCE 8-30-1990.

OWNER OF U.S. REG. NOS. 1,200,236 AND 1,256,083.

SER. NO. 74-184,095, FILED 7-11-1991.

G. T. GLYNN, EXAMINING ATTORNEY