Sealed

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CIVIL ACTION NO.

MICROSOFT CORPORATION, H2-PHARMA, LLC, and GATEHOUSE DOCK CONDOMINIUM ASSOCIATION, INC.,

Plaintiffs

v.

DOES 1-7,

Defendants

FILED UNDER SEAL

COMPLAINT

Plaintiffs Microsoft Corporation ("Microsoft"), H2-Pharma LLC, and Gatehouse Dock Condominium Association, Inc. ("GDCA") bring this action to stop Defendants' ("DOES 1-7" or "Defendants") malicious scheme to distribute and exploit software and services targeting unsuspecting victims for financial fraud.

NATURE OF ACTION

1. This action arises under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA"); the Electronic Communications Privacy Act (18 U.S.C. §§ 2701 *et seq.*); the Copyright Act (17 U.S.C. §§ 101 *et seq.*), the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); and the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962(c)). This action also involves Florida common law claims. Plaintiffs seek injunctive and other equitable relief and damages from Defendants for their creation, control, maintenance, and ongoing use of illegal computer networks and piratical software to cause harm to Plaintiffs and the public at large.

THE PARTIES

2. 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 and a Florida office located at 830 Brickell Plaza, Miami FL 33131. Microsoft is a leading provider of technology products and services, including computer software, internet services, websites, and email services.

3. Plaintiff H2-Pharma, LLC, is a corporation duly organized and existing under the laws of the State of Florida, having its headquarters and principal place of business in Montgomery, Alabama. H2 is a privately owned and funded specialty pharmaceutical company focused on the sales, marketing and distribution of both branded and generic prescription, and non-prescription products.

4. Plaintiff GDCA is a corporation duly organized and existing under the laws of the State of Florida, having its principal place of business in Key Largo, Florida.

5. Defendant DOE 1 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 the source copy of the Windows Server 2022 Standard Evaluation version discussed below and the webpages located at the URLs redvds[.]com, redvds[.]pro, and vdspanel[.]space, and the subdomains of those URL ("RedVDS Domains"). The RedVDS Domains are used by Defendants to market, sell, distribute, and/or operate the unauthorized copies of Windows Server and associated services described in this Complaint. RedVDS Domains host webpages that include a user portal that can be used to control virtual instances of Windows Server, webpages that facilitate end user purchases of additional unauthorized instances of Windows Server, and webpages offering customer support through chat sessions and

a chat bot. The RedVDS Domains also facilitate API functionality that permits users to control numerous computers at scale. The RedVDS Domains also facilitate a referral bonus program and loyalty program through which end users can share in the ill-gotten profits generated by the RedVDS Enterprise. Plaintiffs believe that a reasonable opportunity for discovery will yield evidence that DOE 1 resides outside the United States.

6. Defendant DOE 2 is a natural person who makes ongoing use of the RedVDS Enterprise's services to send fraudulent emails to and from recipients located in the United States. DOE 2 has used unauthorized depictions of Microsoft's trademark and logos in executing a business email compromise (BEC) scheme. One of DOE 2's BEC schemes involved victim companies with locations in Washington and Florida. DOE 2 compromised one victim company's email system and used unauthorized access to that system to intercept private email communications and to send fraudulent emails to GDCA employees in March and April 2025, resulting in financial losses due to GDCA's reliance on DOE 2's fraudulent email communications. DOE 2 operates these types of fraudulent email campaigns at scale, resulting in transmission of thousands of emails containing false and misleading depictions of Microsoft's trademarks and/or logos.

7. Defendant DOE 3 is a natural person who makes ongoing use of the RedVDS Enterprise's services to send fraudulent emails to and from recipients located in the United States. One of DOE 3's BEC schemes involved a European corporation and a Florida corporation headquartered in Alabama, H2. DOE 3 gained unauthorized access to H2's email system and used that unauthorized access to intercept private email communications and to send fraudulent emails to H2 commencing in mid-April 2025. H2 was deceived by DOE 3's emails and transferred money to an account controlled by DOE 3 in April and May 2025 in reliance on

DOE 3's fraudulent emails, which impersonated an actual employee of the European corporation.

8. Defendant DOE 4 is a natural person who makes ongoing use of the RedVDS Enterprise's services to send fraudulent emails to and from recipients located in the United States. One of DOE 4's phishing campaigns used attached pdf files impersonating HR compensation summaries that contained QR codes to deceive the recipients into providing their account credentials. DOE 4 operates these types of fraudulent email campaigns at scale, resulting in transmission of thousands of emails containing false and misleading attachments.

9. Defendant DOE 5 is a natural person who makes ongoing use of the RedVDS Enterprise's services to send fraudulent emails to and from recipients located in the United States. DOE 5 is primarily engaged in unauthorized email account takeover, likely after a successful phishing attack where account credentials were stolen. DOE 5 attempted, and may have been successful, in accessing many user accounts in 2025. Some of the accounts accessed belong to Real Estate, Construction, and Insurance companies in the United States, and located in Florida, California, Wisconsin, and Alabama.

10. Defendant DOE 6 is a natural person who makes ongoing use of the RedVDS Enterprise's services to send fraudulent emails to and from recipients located in the United States. DOE 6 is primarily engaged in unauthorized email account takeover, likely after a successful phishing attack where account credentials were stolen. DOE 6 attempted, and may have been successful, in accessing many user accounts in 2025. Some of the accounts accessed belonging to Accounting and Manufacturing companies in the United States, and located in Florida, California, and New York.

11. Defendant DOE 7 is a natural person who makes ongoing use of the RedVDS Enterprise's services to send fraudulent emails to and from recipients located in the United States. DOE 7 is primarily engaged in unauthorized email account takeover, likely after a successful phishing attack where account credentials were stolen. DOE 7 attempted, and may have been successful, in accessing many user accounts in 2025. Some of the accounts accessed belonging to Education Institutions in the United States and located in Florida and Texas.

12. 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 each contribute funds used to facilitate the operation of the RedVDS Domains. Defendants also each receive financial benefits from operation of the RedVDS Domains

13. Plaintiffs are uncertain of the true names and capacities of Defendants sued herein as Does 1-7 inclusive and therefore sues these Defendants by such fictitious names. Plaintiff will amend this complaint to allege Defendants' true names and capacities when ascertained with reasonable certainty. Plaintiff will exercise due diligence to determine Defendants' true names, capacities, and contact information, and to effect service upon those Defendants.

14. Each of the Defendants is responsible in some manner for the occurrences herein alleged, and the injuries and the injuries to Plaintiffs' customers alleged are proximately caused by such Defendants.

15. The actions and omissions alleged herein to have been undertaken by Defendants individually were actions and omissions that each Defendant authorized, controlled, directed, benefited from, and/or that each Defendant had the ability to authorize, control or direct, and/or were actions and omissions each Defendant assisted, participated in, or otherwise encouraged,

and are actions for which each Defendant is liable. Each Defendant aided and abetted the actions of Defendants set forth below, in that each Defendant had knowledge of those actions and omissions, provided assistance, and benefited from those actions and omissions, in whole or in part. Each Defendant was the agent of each of the remaining Defendants, and in doing the things hereinafter alleged, was acting within the course and scope of such agency and with the permission and consent of other Defendants.

JURISDICTION AND VENUE

16. 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 CFAA (18 U.S.C. § 1030), the ECPA (18 U.S.C. §§ 2701 *et seq.*), the Lanham Act (15 U.S.C. §§ 1114, 1125(a), (c)), the Copyright Act (17 U.S.C. §§ 101 *et seq.*), and the Racketeer Influence and Corrupt Organizations Act (18 U.S.C. § 1961 *et seq.*). The Court has supplemental jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367.

17. In carrying out the conduct described in this Complaint, Defendants have availed themselves of the privilege of conducting business in Florida and have directed acts complained of herein toward the state of Florida and this judicial district. For example, in carrying out the scheme described in this complaint, RedVDS contracted with and used the hosting services of ReliableSite.Net LLC, a U.S. company headquartered in Miami, Florida, sent fraudulent communications to victims in Florida, received monies from victims located in Florida, and otherwise directed their activities towards Florida corporations and Florida residents.

18. Defendants have acted at all times relevant with knowledge that their acts would cause harm through computers located in Florida thereby injuring Plaintiff, its customers, and

others in the United States. Defendants used pirated versions of Windows Server hosted on computers that geolocate to Miami, Florida.

19. 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. For example, Defendants intentionally availed themselves of the privilege of doing business in the United States by:

- Contracting with and utilizing the services of Cloudflare, Inc., a U.S. company headquartered in San Francisco, California that provides network infrastructure and proxy services
- Contracting with and utilizing the services of Interserver, Inc., a U.S. hosting company headquartered in Secaucus, New Jersey
- Contracting with and utilizing the services of ReliableSite.Net LLC, a U.S. company headquartered in Miami, Florida
- Contracting with and utilizing the services of Verisign, Inc., a U.S. Company, to register and use the RedVDS ".com" domains
- Using the U.S. wires to transmit computer commands and electronic communications to victim computers
- Using computers located in the U.S. to host pirated copies of Windows Server
- Targeting and victimizing U.S. companies, organizations, and persons, as discussed herein.

20. Accordingly, to the extent Defendants do not have sufficient contacts with Florida alone to support jurisdiction and venue in this Court, each Defendant is subject to jurisdiction based on their national contacts with the United States and is thus subject to national service of process and jurisdiction is proper in this Court.

21. Pursuant to 28 U.S.C. § 1391(b), venue is proper in this judicial district. A substantial part of the events or rise to Plaintiffs' claims, and a substantial amount of the infrastructure used to carry out Defendants' scheme, is situated in this judicial district. Venue is

proper in this judicial district under 28 U.S.C. § 1391(c) because Defendants are subject to personal jurisdiction in this judicial district.

FACTUAL BACKGROUND

Overview

22. Microsoft is the well-known creator and provider of the Windows operating system and a variety of related software and services. Microsoft has invested substantial resources in developing high-quality 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 within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including the Microsoft®, Windows®, Outlook®, and Microsoft 365® marks. Microsoft also uses well-known and widely recognized logos for its products, including the Windows and Microsoft 365 logos.

23. Operating systems like Windows face an onslaught of security threats, from malware and exploits to unauthorized access and privilege escalation. To address the ever-evolving threat landscape, Windows is designed with zero-trust principles at its core, offering powerful security from chip to cloud. Windows integrates advanced hardware and software protection, ensuring data integrity and access control across devices.

24. Microsoft's Security Development Lifecycle (SDL) embeds comprehensive security requirements, technology specific tooling, and mandatory processes into the development and operation of all software products. All development teams at Microsoft must

adhere to the SDL processes and requirements, resulting in more secure software with fewer and less severe vulnerabilities at a reduced development cost.

25. Although Microsoft is constantly evolving, enhancing, and innovating its security technology, increasingly sophisticated cybercriminals are also constantly evolving and working on new ways of defeating cybersecurity measures. Research shows that employees, including their devices, services, and identities, are at the center of attacks on businesses of all sizes. Some leading threats include identity attacks, ransomware, targeted phishing attempts, and BEC.

26. The scheme carried out by Defendants in this case exemplifies the type of evolving threat that Microsoft and its customers face. Defendants are a group of criminal actors working together to operate a malicious computer network comprised of computers and virtual machines running unauthorized copies of Microsoft's Windows Server Software in order to remotely carry out activities like phishing attacks, unauthorized account takeover, unauthorized computer intrusions, and financial fraud. Defendants also participate with each other in a marketplace that offers services and software related to their malicious activities.

Microsoft's Windows Server Software

27. Windows Server is Microsoft's enterprise server platform that enables organizations to run and secure applications, services, and workloads across on-premises, hybrid, and cloud environments. Built on decades of Windows innovation, it serves as the backbone for millions of organizations worldwide, powering everything from file servers and web applications to complex enterprise workloads and AI-driven solutions.

28. From a user interface perspective, Windows Server is similar to the common version of Windows that most users are familiar with, but Windows Server has additional features designed to help manage data and applications across multiple computers.

29. Like many Microsoft products, Windows Server is licensed, not sold to end users. In order to obtain a license and lawfully use Windows Server, users must agree to a license agreement that requires, among other things, an agreement not to use Microsoft's software for harmful purposes. One element of Microsoft's licensing program is a cryptographically generated key, sometimes referred to as a product key, license key, or license certificate ("Windows Server Key"). Windows Server Keys are unique alphanumeric codes cryptographically generated by Microsoft to validate the license status of a copy of Windows Server.

30. Microsoft's Windows Server software is generally licensed through Microsoft Commercial Licensing programs. Specific license terms for Windows Server are defined in the Microsoft Commercial Licensing Product Terms, the Microsoft Commercial Licensing agreement under which it was acquired, and/or its original equipment manufacturer (OEM) or Retail Software License Terms.

31. Windows Server software licenses are sold through channels designed to meet the unique needs of customers. These sales channels include online retailers offering full packaged product (FPP) licenses of Windows Server software, original equipment manufacturers (OEMs) offering pre-installed licenses with their hardware systems, as well as Licensing Solutions Partners (LSPs) and Enterprise Software Advisors (ESAs) offering Windows Server software through Microsoft Commercial Licensing programs for end-customer organizations.

32. The current version of Windows Server is Windows Server 2025. There are three versions of Windows Server 2025 commercially licensed by Microsoft. Windows Server Data Center Edition is ideal for highly virtualized and software-defined datacenter environments. Standard edition is ideal for customers with low density or non-virtualized environments.

Essentials edition is a cloud-connected first server, ideal for small businesses with up to 25 users and 50 devices. Windows Server 2025 Essentials edition is available to purchase from OEMs only.

33. Windows Server includes technologies designed to simplify the task of configuring the distribution and management of an organization's volume software licenses. For example, Microsoft's Volume Activation is a set of technologies and tools designed to automate the product activation process for systems that are deployed under a Microsoft Commercial Licensing agreement. Volume Activation Services is a server role in Windows Server (2012 or later editions) that enables a customer to automate and simplify the issuance and management of Microsoft software volume licenses for a variety of scenarios and environments. With Volume Activation Services, customers can install and configure the Key Management Service (KMS) and enable Active Directory-based Activation.

34. KMS is a role service that allows organizations to activate systems within their network from a server where a KMS host has been installed. With KMS, IT professionals can complete activations on their local network, eliminating the need for individual computers to connect to Microsoft for product activation. KMS does not require a dedicated system, and it can be cohosted on a system that provides other services. By default, volume editions of Windows client and server operating systems connect to a system that hosts the KMS service to request activation. No action is required from the user.

35. Active Directory-based activation is another role service customers can use to manage volume licensing. Active Directory-based activation allows the customer to use Active Directory Domain Services (Active Directory DS) to store activation objects, which can further simplify the task of maintaining volume activation services for a network. With Active

Directory-based activation, no additional host server is needed, and activation requests are processed during computer startup.

36. Any computers running Windows Server 2016 (or later editions) with a Generic Volume License Key (GVLK) that are connected to the domain will activate automatically and transparently. They will stay activated as long as they remain members of the domain and maintain periodic contact with a domain controller. Activation takes place after the licensing service starts. When this service starts, the computer running Windows Server 2016 (or later editions) contacts Active Directory DS automatically, receives the activation object, and activates without user intervention.

37. In addition to commercially licensed versions of Windows Server, Microsoft also licenses evaluation versions of Windows Server for customers who wish to evaluate the software before entering into a commercial license. Evaluation licenses only authorize usage for 180 days and these licenses may not be sold or used in live operating environments. Microsoft currently only offers evaluation licenses for Windows Server 2025 on Azure, Windows Server 2025 64-bit ISO, and Windows Server 64-bit VHD. Evaluation versions of Windows Server must be activated over the internet in the first 10 days to avoid automatic shutdown.

The RedVDS Enterprise and its Unlawful Virtualization Services

38. Each DOE Defendant is a member of an organization that is conducted through a pattern of illegal activity ("RedVDS Enterprise"). The RedVDS Enterprise markets, sells, hosts and uses unauthorized evaluation copies of Windows Server 2022 Standard in a virtual environment that can be remotely accessed from any computer connected to the internet. The "VDS" in RedVDS stands for "virtual desktop server", as DOE 1 markets the RedVDS service as a service that allows users to remotely access a virtual Windows desktop that can then be used

as a server to facilitate network operations for multiple computers. For example, a user can use one computer to remote into a RedVDS virtual Windows Server running on a different computer and use that Windows Server computer as a hub for controlling networks of other computers. In other words, the RedVDS Enterprise is selling and operating a grey-market Windows Server service using evaluation copies of Windows Server 2022 over which Microsoft has no control.

39. At some point prior to 2023, DOE 1 obtained a copy of Windows Server 2022 from Microsoft or a third party. In order to download and install Windows Server, DOE 1 was required by Microsoft's systems to agree to Microsoft's terms of use and license agreement for the Windows Server software.

40. The copy of Windows Server obtained by DOE 1 contains an embedded evaluation Windows Server Key that enables 156 days of usage; after 156 days of usage, a user receives a message informing them that their evaluation license has expired and prompting them to obtain a proper usage license. DOE 1 unlawfully cloned this copy of Windows Server and its embedded Windows Sever Evaluation key in order to enable an unlimited number of users to run copies of the cloned RedVDS Windows Server instance.

41. In violation of Microsoft's licensing terms, DOE 1 installed one copy of Windows Server onto a virtual computer with the identifying Computer Net Bios Name "WIN-BUNS25TD77J". DOE 1 then created numerous images of this virtual computer for distribution to multiple end users. In this context, the term "image" refers to a snapshot of the entire state of a system, disk, or environment at a specific point in time. An image usually includes operating system files, installed applications, configurations settings, and sometimes boot sector data.

42. These images were then mounted across a variety of hosting sites in locations all over the world. An open-source virtualization software Quick Emulator, or "QEMU", is used to

manage the deployments of these images. Because each image represents a copy of the original system as it existed at the time of imaging, the evaluation license timer in the Windows Server software reflects the number of days left in the evaluation period at the time of the imaging. Because DOE 1 created the image at a time when there were 156 days remaining on the Windows Server evaluation license, each instantiation of that image will also show 156 days remaining evaluation usage, even after the original 156-day period has expired. DOES 1-7 each used these images to conduct unlawful activity.

43. The RedVDS Enterprise traffics and uses the unauthorized images and copies of the original Windows Server and Windows Server Key through the website located at the URL redvds[.]com. Microsoft believes that the RedVDS Enterprise has distributed thousands of unauthorized copies of Windows Server.

44. The RedVDS Enterprise engages the services of other third-party hosting providers and installs unauthorized copies of Windows Server on those hosting providers' servers, including within the United States. The RedVDS Enterprise then sells access to these copies of Windows Server to end users at a rate of $24 to $80 per month, depending on storage, CPU, and memory preferences. The RedVDS Enterprise maintains and uses a significant number of active virtual servers monthly. These servers are used by cybercriminals, facilitating a wide range of illicit activities targeting Microsoft and its customers. Microsoft's Digital Crimes Unit has linked RedVDS infrastructure to numerous security incidents and has determined that RedVDS is a significant and persistent enabler of attacks against users of Microsoft's operating systems, communications services, and cloud computing services.

Malicious Use of RedVDS's Piratical Windows Server Instances

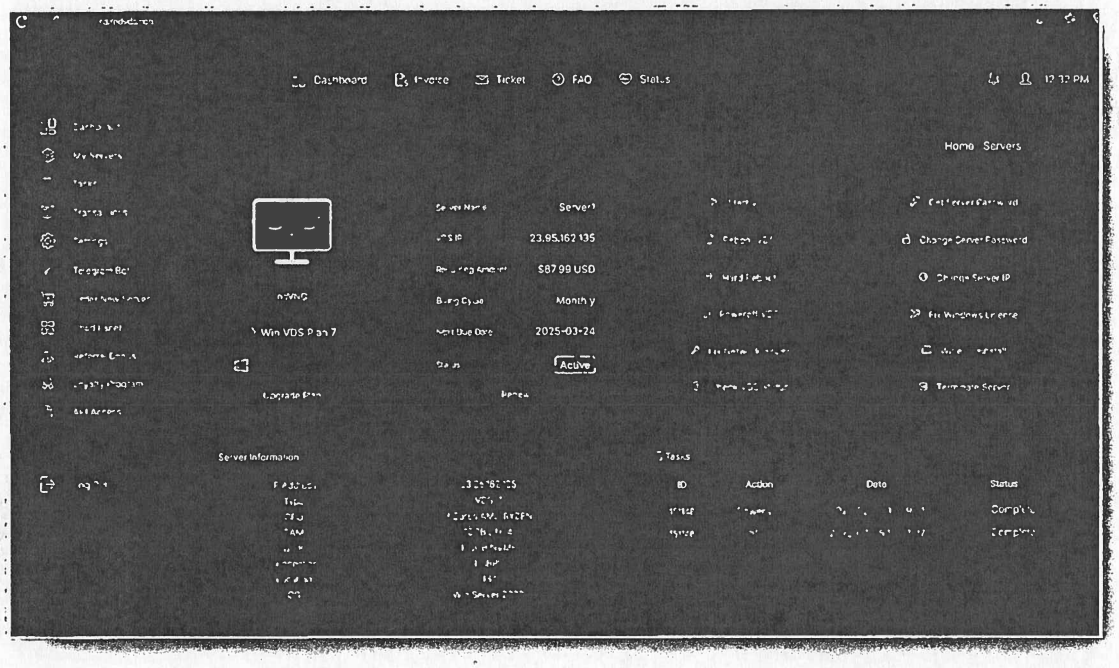
45. Commencing in 2024, Microsoft observed the existence of numerous malicious Windows hosts with the Computer Net Bios Name WIN-BUNS25TD77J. Further investigation revealed that the WIN-BUNS25TD77J identifier is associated with thousands of stolen credentials, invoices, mass mailers, and phish kits. Microsoft determined that the host machines associated with WIN-BUNS25TD77J were all created from the same virtual computer image. These images contain the cloned evaluation copy of Windows Server 2022 discussed above.

46. RedVDS's user interface makes prominent use of Microsoft's Windows Server trademark and trademarked Microsoft Windows logo. **Figure 1** below depicts the RedVDS user interface:

Fig. 1

47. **Figure 2** below depicts the RedVDS user interface displaying Microsoft's trademarks and Windows logo:

Fig. 2



48. **Figure 3** and **Figure 4** below depict the user interface encountered by RedVDS end users upon executing the 2022 copy of Windows Server provided by RedVDS.

Fig. 3

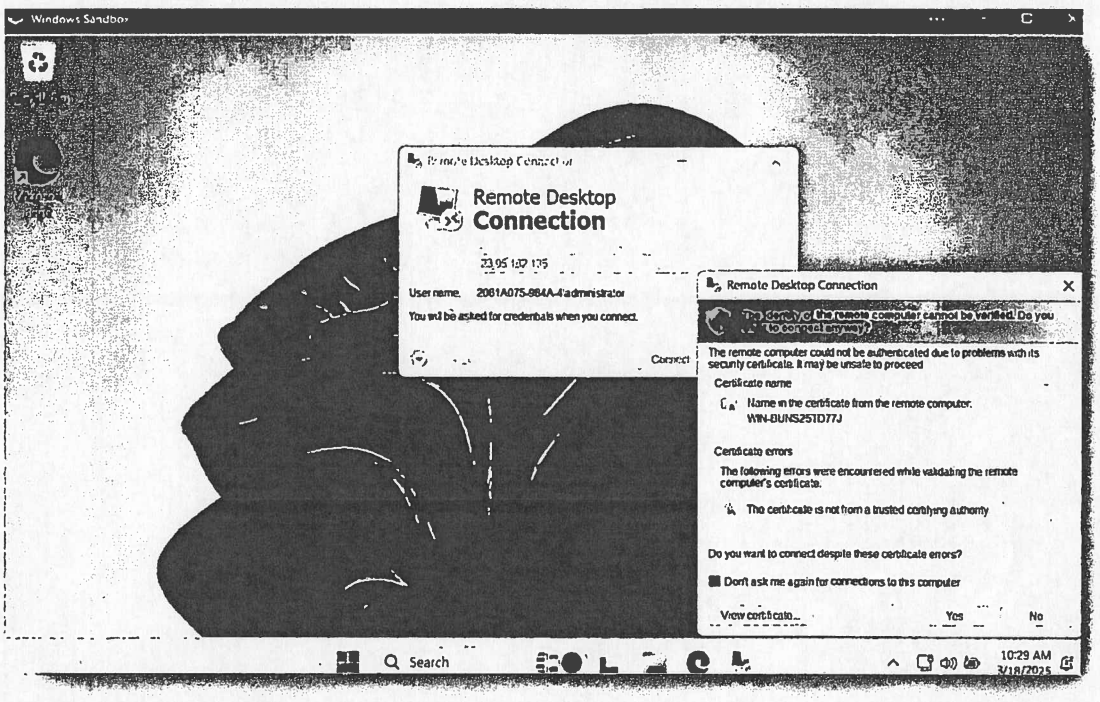

Windows Sandbox
Remote Desktop Connection
User name: 2061A075-884A-4\administrator
You will be asked for credentials when you connect.
Connect
Remote Desktop Connection
The identity of the remote computer cannot be verified. Do you want to connect anyway?
The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed
Certificate name
Name in the certificate from the remote computer:
WIN-BUNS251D77J
Certificate errors
The following errors were encountered while validating the remote computer's certificate:
The certificate is not from a trusted certifying authority
Do you want to connect despite these certificate errors?
Don't ask me again for connections to this computer
View certificate...
Yes
No
Search
10:29 AM
2/18/2025

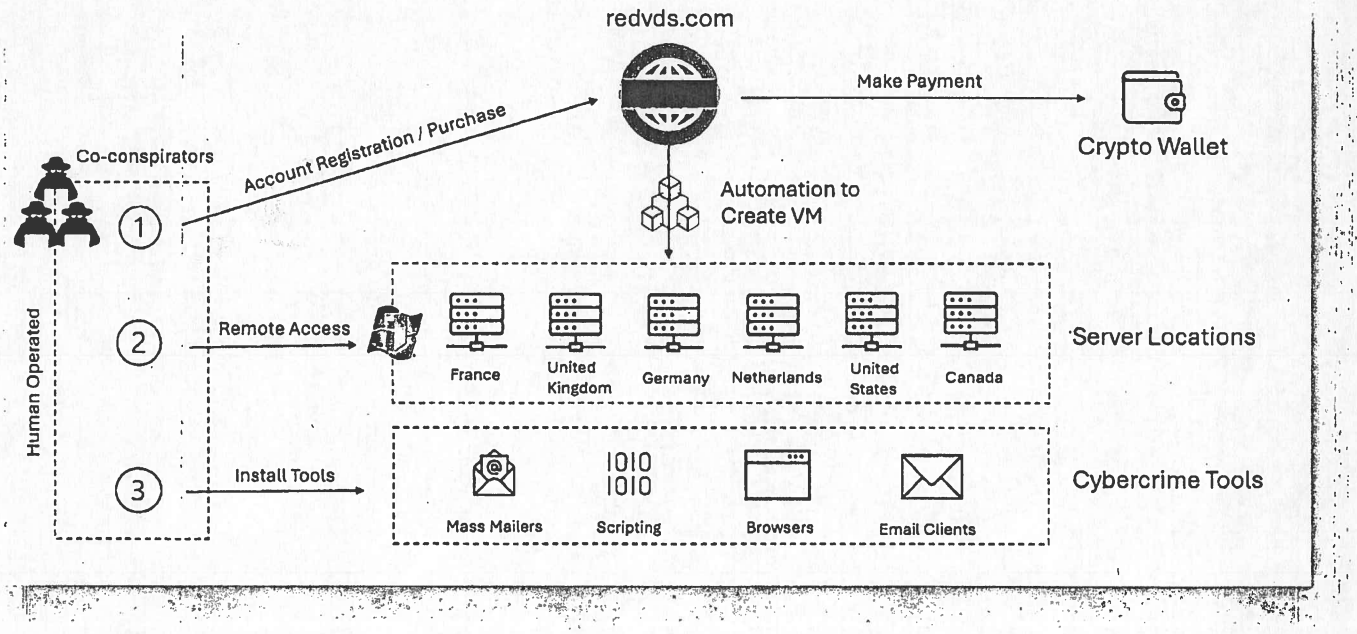
Fig. 4


23.95.162.135

49. End users purchasing services from the RedVDS Enterprise typically tender payment to DOE 1 via one or more crypto wallets. Since June 2023, approximately $5.3 million in cryptocurrency transactions have been linked to purchases of the RedVDS Enterprise. This amount likely represents only a portion of the total revenue, as Microsoft's analysis is limited to the cryptocurrencies used during the controlled purchases it conducted from RedVDS. RedVDS accepted payments in additional cryptocurrencies that were not included in our purchases.

50. After receiving payment, DOE 1 deploys an automated process to create a virtual machine for the end user using the image and copy of Windows Server 2022 discussed above. End users then use the RedVDS virtual machine image, Windows Server software, and hosting services to remotely access and control for a variety of malicious purposes. **Figure 5** below depicts the basic architecture of the RedVDS hosting service.

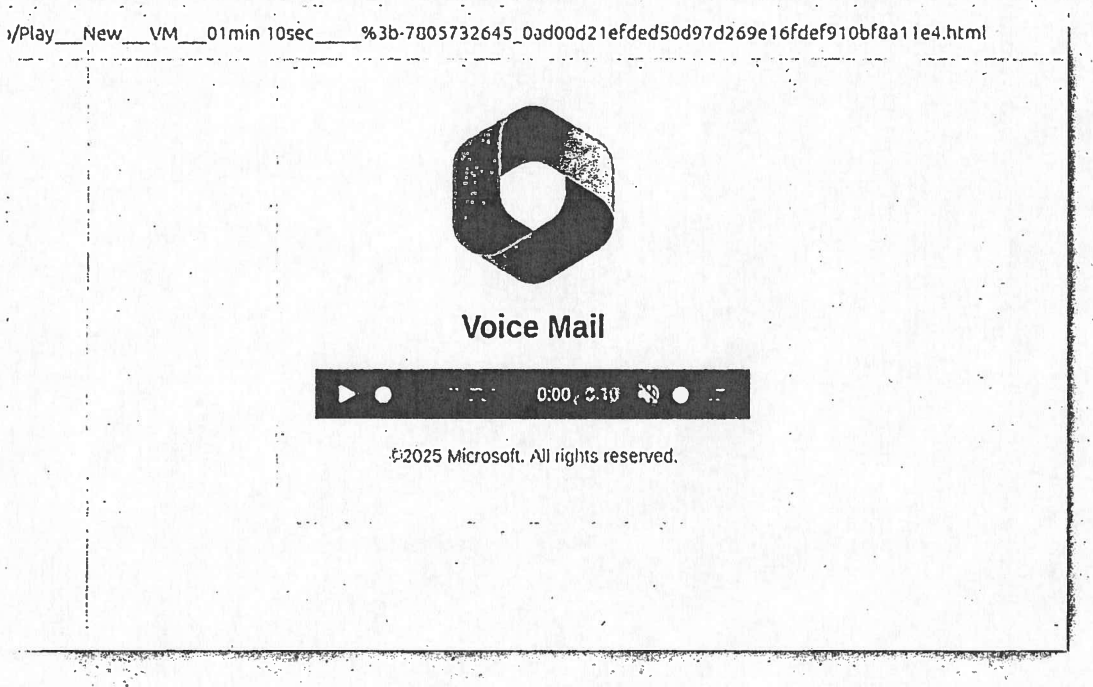
Fig. 5



51. RedVDS users unlawfully use Microsoft's copyright protected software and/or Microsoft's well-known trademarks and logos to carry out various forms of wire fraud.

52. **Figure 6** below depicts an example of a RedVDS-enabled BEC scheme that used Microsoft's trademark and a well-known Microsoft logo.

Fig. 6



53. Investigation into RedVDS revealed that it is not a registered company or legal entity in any state or nation. The Terms of Service indicate it is governed by Bahamian Law, and the domain registration for the RedVDS URL provides what appears to be a fake name ("David Rico") and fake address. For example, the domain registrant address given for RedVDS corresponds to a University of the Bahamas International Building that has been demolished. The use of fake name and address information is consistent with trade craft commonly used by perpetrators of ongoing software piracy and cybercrime schemes.

Defendants' Victimization of H2

54. In early 2025, H2 began discussions with a European supplier about ways for H2 to reduce its transactional costs. These discussions involved email communications about switching H2's payment mechanism from wire transfers to ACH payments.

55. Unbeknownst to H2, its email system had been compromised by one or more DOE Defendants. One or more DOE Defendants monitored H2's communications with its supplier and waited for an opportunity to defraud H2.

56. After observing H2's email discussions with its supplier, at least DOE 3 used their unauthorized access to the compromised email account to mislead H2 about H2's ACH inquiry and to misdirect H2's payments.

57. In April 2025, DOE 3 sent to H2 emails from an account that appeared to belong to H2's supplier providing documentation and instructions to facilitate H2's payment of money to an account that H2 believed belonged to its supplier. In fact, the email account was fraudulent and the bank account referenced in DOE 3's emails was under the control of at least DOE 3.

58. DOE 3 fraudulently caused H2 to send multiple significant payments of money to the subject account in April and May 2025. As a result, H2 sustained a substantial seven-figure loss.

59. H2 learned that it had been defrauded in May 2025 when its supplier inquired about the status of the payments H2 attempted to send to the supplier. H2 promptly reported DOE 3's crime to law enforcement.

Defendants' Victimization of GDCA

60. In March 20205, GDCA and one of its contractors were each in the process of setting up new bank accounts. Around this same time, GDCA engaged in email communications

and video conferences with its contractor's representative inter alia about the timing and routing of payments for services and materials the contractor was providing to GDCA. GDCA's contractor stated that it would provide GDCA with new bank account information in the coming weeks.

61. Unbeknownst to GDCA, the email account of the contractor representative Gatehouse was communicating with had been compromised by one or more DOE Defendants. One or more DOE Defendants monitored GDCA's communications with its contractor and waited for an opportunity to defraud GDCA.

62. After observing GDCA's email discussions with its contractor, at least DOE 2 used the compromised contractor email account and a homoglyph of that email account to mislead GDCA and to misdirect GDCA's payments.

63. In April 2025, DOE 2 sent to Gatehouse an email providing documentation and instructions to facilitate GDCA's payment of money to an account that GDCA believed belonged to its contractor. In fact, the account was under the control of at least DOE 2. This email was sent about one week after GDCA's contractor told GDCA to expect to receive contractor's updated bank account information in about a week.

64. DOE 2 fraudulently caused GDCA to send a significant payment of money to the subject account in April 2025. As a result, Gatehouse sustained a substantial six-figure loss.

Defendants' Ongoing Activities

65. Defendants continue to operate and use the RedVDS in the manner explained above. DOE 1 continues to sell pirated versions of Windows Server 2022 and to assist RedVDS end users in circumventing Microsoft's licensing system, and a reasonable opportunity for

discovery is likely to show that DOES 2-7 continue to operate BEC attacks and other malicious activities via the RedVDS service.

66. The RedVDS service continues to facilitate numerous phishing campaigns and related activities at scale.

67. Defendants are carrying out their scheme throughout the United States, including in the state of Florida.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

Violations of the Computer Fraud and Abuse Act (H2 and GDCA against DOES 1-7)

68. Plaintiffs reallege and incorporate by this reference each and every allegation set forth in paragraphs 1-67 above.

69. Defendants knowingly and intentionally accessed H2's protected computers without authorization and knowingly caused the transmission of a program, information, code and commands, resulting in damage to the protected computers.

70. Defendants knowingly and intentionally accessed GDCA's supplier's protected computers without authorization with the intent to defraud GDCA and knowingly caused the transmission of a program, information, code and commands, resulting in damage to the protected computers.

71. Defendants knowingly and with intent to defraud accessed protected computers without authorization and by means of such conduct furthered the intended fraud and obtained substantial sums of money from H2 and GDCA.

72. Defendants' conduct involved interstate and foreign communications.

73. Defendants' conduct has caused a loss during a one-year period aggregating more than $5,000. H2's loss includes a seven-figure payment fraudulently sent to an account under one or more Defendants' control. GDCA's loss includes the sum of multiple six-figure payments fraudulently sent to an account under one or more Defendants' control.

74. Plaintiffs seek injunctive relief and compensatory and punitive damages under 18 U.S.C. §1030(g) in an amount to be proven at trial.

75. 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.

SECOND CLAIM FOR RELIEF

Copyright Infringement (Microsoft against DOES 1-7)

76. Plaintiffs reallege and incorporate by this reference each and every allegation set forth in paragraphs 1-67 above.

77. Microsoft holds a copyright registration for Windows Server 2022, on file with the copyright office as Registration No. TX0009008683.

78. Defendants have reproduced, distributed, displayed, and/or sold unauthorized copies of Windows Server 2022.

79. Defendants have willfully infringed Microsoft's copyrights for commercial gain.

80. Defendants are causing Microsoft monetary damages.

81. Defendants are causing Microsoft irreparable harm.

82. Microsoft is entitled to damages in an amount to be determined at trial or in the alternative to maximum statutory damages.

83. Microsoft is entitled to an award of attorneys fees on its copyright claims.

THIRD CLAIM FOR RELIEF

Trademark Infringement, False Designation of Origin, and Dilution by Tarnishment (Microsoft against DOES 1-7)

84. Plaintiffs reallege and incorporate by this reference each and every allegation set forth in paragraphs 1-67 above.

85. 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.

86. Windows® is a registered trademark owned by Microsoft, U.S. Trademark Registration No. 7706415. The Windows® 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.

87. Microsoft 365® is a registered trademark owned by Microsoft, U.S. Trademark Registration No. 6701693. The Microsoft 365® trademark 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.

88. Defendants are importing, distributing, trafficking, and using non-genuine copies of Windows Server 2022 and/or copies of Windows Server 2022 that are not intended for sale in the United States.

89. The copies of Windows Server 2022 offered by the RedVDS Enterprise and trafficked, imported, and used by each DOE Defendant are materially different from the evaluation and commercial versions of Windows Server currently offered for license by Microsoft in the United States.

90. Defendants are depriving Microsoft of its ability to control the quality of its Windows Server software.

91. Defendants' fraudulent emails contain 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.

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

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

94. 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.

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

FOURTH CLAIM FOR RELIEF

Violations of the Racketeer Influenced and Corrupt Organizations Act (RICO) 18 U.S.C. § 1964(a), (c)&(d) (Plaintiffs against DOES 1-7)

96. Plaintiffs reallege and incorporate by this reference each and every allegation set forth in paragraphs 1-67 and 76-93 above.

97. DOE 1 is conducting the affairs of the business known as RedVDS through a pattern of racketeering. DOE 1's pattern of racketeering conduct includes numerous violations of 18 U.S.C. 2389, 18 U.S.C. 2320, and 18 U.S.C. 1343 over at least the period of time from 2024 to present.

98. In addition, DOES 1-7 are members of an ongoing association-in-fact enterprise (the "RedVDS Enterprise" or "Enterprise") consisting of at least DOE 1 and DOES 2-7, each of whom is using one or more of the instrumentalities described herein to commit wire fraud, criminal copyright infringement, and criminal trademark infringement in violation of federal law.

99. DOES 1-7 have conspired to conduct the affairs of the RedVDS Enterprise.

100. DOES 1-7 have each invested, directly or indirectly, income derived from a pattern of rackettering, or the proceeds of such income, in the operation of the RedVDS Enterprise

101. The 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, access device fraud, and unauthorized distribution of counterfeit marks, counterfeit software, and infringing materials.

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

103. A reasonable opportunity for discovery will yield evidence that Defendants' pattern of wire fraud and access device fraud predates and postdates the conduct described herein.

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

105. Defendants conspired to operate the Enterprise through a pattern of racketeering activity in furtherance of the common purpose of the Enterprise sometime prior to April 2025. Thereafter, each Defendant took wrongful acts in furtherance of their unlawful agreement by supplying resources to the Enterprise.

106. Defendants continuously and effectively carried out the purpose of the Enterprise from at least 2024 to present, causing harm to the business and property of Microsoft and others. Defendants represent a continuing threat to Microsoft and others.

107. **Wire Fraud** (18 U.S.C. § 1343). At some point prior to April 2025, Defendants devised a scheme to obtain money or property from Microsoft customers and others, and to defraud Microsoft customers and others. For example, multiple Defendants participated in the scheme to defraud H2 of money through a sophisticated BEC attack. Multiple Defendants participated in a similar scheme to defraud Gatehouse through a similarly sophisticated BEC attack.

108. From March to April 2025, 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 between March to April 2025, Defendants transmitted by means of wire communication in interstate and foreign commerce emails designed to deceive victims into clicking malicious links, sending money to accounts controlled by Defendants, and other malicious conduct. Defendants continue to use communications transmitted by means of wire communication in interstate and foreign commerce in furtherance of their scheme to this day.

109. **Criminal Copyright Infringement** (18 U.S.C. § 2319). For over sixth months, Defendants have intentionally and knowingly engaged in willful copyright infringement for purposes of commercial advantage or private financial gain.

110. **Criminal Trademark Infringement** (18 U.S.C. § 2320) For over six months, Defendants have intentionally and knowingly used one or more counterfeit marks on or in connection with goods or services trafficked in the United States.

111. A reasonable opportunity for discovery is likely to yield evidence that 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.

112. The conduct described above has caused harm to Microsoft's, H2's, and GDCA's respective businesses and property in an amount to be computed at trial.

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

114. Plaintiffs are entitled to and hereby demand treble damages, attorneys' fees, and costs of suit in addition to preliminary and permanent injunctive relief.

FIFTH CLAIM FOR RELIEF
Violations of the ECPA 18 U.S.C. § 2701 (H2 and Gatehouse against DOES 1-7)

115. Plaintiffs reallege and incorporate by this reference each and every allegation set forth in paragraphs 1-67 above.

116. H2, Gatehouse, and its contractual counterparty's email systems and computers are facilities through which electronic communication service is provided to users.

117. Defendants knowingly and intentionally accessed these email systems and computers without authorization.

118. Through this unauthorized access, Defendants intercepted, had access to, obtained and altered, and/or prevented legitimate, authorized access to, wire and electronic communications transmitted through the computers and email systems.

119. In connection with this interception, Defendants have intercepted and gained access to the contents of such wire and electronic communications, including access to the

passwords, personal identifying information, sensitive financial information, or other private information contained in such communications.

120. 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

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

SIXTH CLAIM FOR RELIEF
Trespass to Chattels (H2 against DOES 1-7)

122. Plaintiffs reallege and incorporate by this reference each and every allegation set forth in paragraphs 1-67 above.

123. Defendants' activities resulted in the unauthorized access to the computers of H2, resulting in theft of information, account credentials, and funds.

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

125. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to trespass on the computers and computer networks of Plaintiffs and their contractual counterparties.

126. 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.

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

SEVENTH CLAIM FOR RELIEF
Conversion (H2 and Gatehouse against DOES 1-7)

128. Plaintiffs reallege and incorporate by this reference each and every allegation set forth in paragraphs 1-67 above.

129. Defendants have used a computer and/or computer network, without authority, with the intent to convert the property of H2 and Gatehouse.

130. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to trespass on the computers and computer networks of Plaintiffs and their contractual counterparties.

131. 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.

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

EIGHTH CLAIM FOR RELIEF
Unjust Enrichment (Plaintiffs against DOES 1-7)

133. Plaintiffs reallege and incorporate by this reference each and every allegation set forth in paragraphs 1-67 above.

134. The acts of Defendants complained of herein constitute unjust enrichment of the Defendants at the expense of Plaintiffs.

135. Defendants profited unjustly from their unauthorized and unlicensed use of Plaintiffs' property.

136. Defendants had an appreciation and knowledge of the benefit they derived from their unauthorized and/or unlicensed use of Plaintiffs property.

137. Retention by the Defendants of the profits they derived from their malfeasance would be inequitable.

138. 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.

139. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including without limitation disgorgement of Defendants' ill-gotten profits.

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 Plaintiff actual damages in an amount to be proven at trial.

6. Enter judgment in favor of Plaintiffs disgorging Defendants' profits and;

9. Order such other relief that the Court deems just and reasonable

Dated: January 7, 2026

Respectfully submitted,

Diana M. Fassbender

Diana Marie Fassbender

Diana Marie Fassbender (Florida Bar No. 17095)
ORRICK, HERRINGTON & SUTCLIFFE LLP
215 NW 24th St, Suite 200
Miami, FL 33127
Tel: (202) 339-8533
dszego@orrick.com

Robert L. Uriarte (*pro hac vice* forthcoming)
ORRICK, HERRINGTON & SUTCLIFFE LLP
355 S. Grand Ave.
Ste. 2700
Los Angeles, CA 90017
Tel: (213) 629-2020
Fax: (213) 612-2499
ruriarte@orrick.com

Ana M. Mendez-Villamil (*pro hac vice* forthcoming)
ORRICK, HERRINGTON & SUTCLIFFE LLP
The Orrick Building
405 Howard Street
San Francisco, CA 94105
Tel: (415) 773-5700
amendez-villamil@orrick.com

Of Counsel:
Richard Boscovich
MICROSOFT CORPORATION
Microsoft Redwest Building C
5600 148th Ave NE
Redmond, Washington 98052
Tel: (425) 704-0867
rbosco@microsoft.com

Attorneys for Plaintiffs