UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CIVIL ACTION NO. 1:26-cv-20074-WPD

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

Plaintiffs

v.

DOES 1-7,

Defendants

PLAINTIFFS' FED. R. CIV. P. 55(b) MOTION FOR DEFAULT JUDGMENT

INTRODUCTION

Plaintiffs filed this action to remediate harm caused by a group of unknown cybercriminals abusing Microsoft technology and third-party Internet infrastructure located *inter alia* in the Southern District of Florida. In brief, DOES 1-7 each participated in a scheme to use pirated versions of Microsoft Windows Server 2022 to gain unauthorized access to the computers of unsuspecting victims, and to automate unlawful activities like phishing schemes and business email compromise attacks. In this Court, Plaintiffs obtained injunctive relief that effectively shut down Defendants' U.S.-based infrastructure, including the Internet domains redvds[.]com and redvds[.]pro ("RedVDS Domains") that served as the front end for an illegal marketplace for Defendants' malicious services. And through a related proceeding in the United Kingdom, Microsoft shut down foreign-based hosting infrastructure leveraged by Defendants.[1]

After Plaintiffs executed the Court's temporary restraining order ("TRO"), Defendants lost access to the RedVDS domains that they were using to carry out their scheme. Pursuant to the Court's order authorizing service by electronic means (Dkt. 20), any time Defendants visited the RedVDS domains on or after January 14, 2026, instead of finding the malicious RedVDS websites they were expecting, they encountered a notice page advising them of this lawsuit and providing links to the pleadings in this case. In addition, this case and related proceedings in the U.K. received significant international press coverage. Despite having more than adequate notice of this case, Defendants chose not to appear. Accordingly, Plaintiffs respectfully request entry of default judgment against Defendants pursuant to Rule 55(b) to ensure that the RedVDS domains remain permanently beyond Defendants' control.

LEGAL STANDARD

"Rule 55 of the Federal Rules of Civil Procedure establishes a two-step process for obtaining a default judgment. First, when a defendant fails to plead or otherwise defend the lawsuit, the Clerk of Court must enter a clerk's default against the defendant." *On Clouds GmbH v.*

[1] In addition to civil proceedings, Defendants' misconduct instigated multiple law enforcement referrals and criminal investigations in the U.S. and abroad.

Individuals, Bus. Entities, & Unincorporated Ass'ns Identified on Schedule "A", No. 1:25-cv-23974-GAYLES, 2026 U.S. Dist. LEXIS 22179, at *1 (S.D. Fla. Feb. 3, 2026). "Once a Clerk's default has been entered, a plaintiff may apply for a default judgment to either the Clerk or the Court." *Roberts v. SC Prot. & Sec. Agency LLC*, No. 6:25-cv-0508-CEM-DCI, 2025 U.S. Dist. LEXIS 255745, at *2 (M.D. Fla. Dec. 8, 2025).

"Before entering default judgment, the Court must ensure it has jurisdiction over the claims and the parties, and that the well-pled factual allegations of the complaint adequately state a viable claim for relief." *Optima Tax Relief, LLC v. Keith L. Jones, CPA LLC*, No. 3:25-cv-406-WWB-SJH, 2026 U.S. Dist. LEXIS 23114, at *1 (M.D. Fla. Feb. 4, 2026) (citations omitted); *Surtain v. Hamlin Terrace Foundation*, 789 F.3d 1239, 1245 (11th Cir. 2015) (holding that default standard is akin to a motion to dismiss for failure to state a claim). "Akin to a 'reverse motion to dismiss for failure to state a claim[,]' a court evaluating a motion for default judgment must consider whether a pleading could survive a motion to dismiss." *Optima Tax Relief*, 2026 U.S. Dist. LEXIS 23114, at *2. A "defaulted defendant is deemed to admit the plaintiff's well-pleaded allegations of fact." *Surtain*, 789 F.3d at 1245.

Permanent injunctions may be granted as part of a default judgment. *See, e.g., Albion Brand Foundry Ltd. v. P'ships, Unincorporated Ass'ns Identified on Schedule A*, No. 25-cv-25718-JB, 2026 U.S. Dist. LEXIS 51257, at *15 (S.D. Fla. Mar. 11, 2026) (granting default judgment and issuing permanent injunction to prevent future trademark infringement); *Bridlington Bud Ltd. v. P'ships*, No. 25-cv-23968-DPG, 2025 U.S. Dist. LEXIS 264058, at *8 (S.D. Fla. Dec. 22, 2025) (same); *Gelsinger v. Armanity*, No. 25-23659-CIV-MARTINEZ, 2025 U.S. Dist. LEXIS 250454, at *11 (S.D. Fla. Dec. 4, 2025) (same, copyright infringement); *Cricket Wireless, LLC v. Noelthetechexperts, LLC*, No. 20-62165-CIV-SMITH, 2022 U.S. Dist. LEXIS 88624, at *6 (S.D. Fla. May 17, 2022) (same, DMCA and CFAA claims).

FACTUAL AND PROCEDURAL BACKGROUND

Plaintiffs filed this action on January 7, 2026. Dkt. 1. Also on January 7, Plaintiffs filed *ex parte* motions to temporarily seal the case (Dkt. 6), for a temporary restraining order (Dkt. 7), and

for leave to serve Defendants with process through electronic means (Dkt. 9). On Thursday, January 8, the Court granted Plaintiffs' *ex parte* motions and ordered Defendants to show cause why a preliminary injunction should not issue. Dkt. 18. Among other things, the Court's TRO directed seizure of the RedVDS domains that were central to Defendants' scheme. *Id*. By the evening of Monday, January 12, 2026, the undersigned received confirmation from third-party domain Registries that the RedVDS domains had been redirected to Microsoft infrastructure. Pursuant to the Court's January 8, 2026 Order Granting Plaintiff's Motion for Issuance of Summons and Authorization to Serve process on Defendants' By Electronic Means Pursuant to Fed. R. Civ. P. 4(f)(3) (Dkt. 20), Defendants were served with process at the RedVDS Domains on January 14, 2026, (Dkt. 35), and this case was unsealed on January 16, 2026 (Dkt. 28). On January 22, the Court held an in-person hearing on Plaintiffs motion to convert the TRO to a preliminary injunction. Dkt. 33. Defendants did not oppose Plaintiffs' preliminary injunction request or otherwise appear at the January 22 hearing, and the Court issued a preliminary injunction on January 23, 2026. Dkt. 30. On April 8, the Clerk of Court entered default as to Defendants DOES 1 through 7. Dkt. 38.

Because Defendants have defaulted, they are deemed to admit the well-pleaded factual allegations of Plaintiffs January 7, 2026 Complaint. *Surtain*, 789 F.3d at 1245. Accordingly, the following facts are taken as true for purposes of the instant motion.[2]

Plaintiff Microsoft is a corporation duly organized and existing under the laws of the State of Washington. Dkt. 1 ¶2. Plaintiffs H2-Pharma, LLC ("H2") and Gatehouse Dock Condominium Association, Inc. ("GDCA") are corporations duly organized and existing under the laws of the State of Florida. Id. ¶¶ 2-3. 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

[2] The facts alleged in the Complaint are corroborated by testimonial and documentary evidence submitted in support of Plaintiffs motions. *See* Dkt. 7-1 (Declaration of Josh Blackwell); Dkt. 7-2 (Declaration of Donal Keating); Dkt. 7-3 (Declaration of Geoffrey Noyes); Dkt. 7-4 (Declaration of Maurice Mason); Dkt. 7-5 (Declaration of Sean Ensz).

phishing attacks, unauthorized account takeover, unauthorized computer intrusions, and financial fraud. Dkt. 1 ¶ 26. 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. Dkt. 1 ¶ 38.

Defendant DOE 1 is a natural person with access to and control over the source copy of the Windows Server 2022 Standard Evaluation version discussed in the Complaint and the webpages located at the URLs redvds[.]com, redvds[.]pro, and vdspanel[.]space, and the subdomains of those URLs. Dkt. 1 ¶ 5. Defendant DOE 2 is a natural person who used the RedVDS Enterprise's services and unauthorized depictions of Microsoft's trademark and logos in executing a business email compromise (BEC) schemes, including against GDCA. Dkt. 1 ¶ 6. Defendant DOE 3 is a natural person who used the RedVDS Enterprise's services in executing a business email compromise (BEC) schemes, including against H2. Dkt. 1 ¶ 7. Defendant DOE 4 is a natural person who used the RedVDS Enterprise's services to conduct phishing campaigns attaching pdf files impersonating HR compensation summaries, using QR codes to deceive the recipients into providing their account credentials. Dkt. 1 ¶ 8. Defendant DOE 5 is a natural person who used the RedVDS Enterprise's services to conduct email account takeovers related to Real Estate, Construction, and Insurance companies in the United States, and located in Florida, California, Wisconsin, and Alabama. Dkt. 1 ¶ 9. Defendant DOE 6 is a natural person who used the RedVDS Enterprise's services to conduct email account takeovers related to accounting and manufacturing companies in the United States, and located in Florida, California, and New York. Dkt. 1 ¶ 10. Defendant DOE 7 is a natural person who used the RedVDS Enterprise's services to conduct email account takeovers related to educational institutions in the United States and located in Florida and Texas. Dkt. 1 ¶ 11

Defendants collectively operate and/or control infrastructure, software, and technical artifacts used to carry out the RedVDS Enterprises' affairs. Dkt. 1 ¶ 12. 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. The RedVDS Enterprise traffics and uses the unauthorized images and copies of Windows Server and an associated Windows Server Key through the website located at the URL redvds[.]com. *Id.* ¶ 43. 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. *Id.* ¶ 49. 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. *Id.* ¶ 43.

In 2025, using RedVDS infrastructure, one or more Defendants compromised H2's corporate email system. Dkt. 1 ¶¶ 54-58. After observing H2's email discussions with a supplier, at least DOE 3 used their unauthorized access to H2's email system to fraudulently misdirect millions of dollars of H2 payments to a bank account under the control of DOE 3. *Id.* Similarly, one or more DOE Defendants compromised the email systems of one of GDCA's contractors and used their unauthorized access to the contractors' emails to fraudulently misdirect hundreds of thousands of dollars in payments to a bank account under the control of DOE 2. Dkt. 1 ¶¶ 60-64.

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, the RedVDS Enterprise 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. Dkt. 1 ¶ 17. Defendants have acted at all times relevant with knowledge that their acts would cause harm through computers located in Florida thereby injuring Plaintiffs and others in the United States. Defendants used pirated versions of

Windows Server hosted on computers that geolocate to Miami, Florida. Dkt. 1 ¶ 18. Defendants also have contacts with the United States as a whole. Dkt. 1 ¶ 19 (listing U.S. contacts).

ARGUMENT

I. THE COURT HAS JURISDICTION OVER THE DEFENDANTS AND CLAIMS

The Court has federal question subject matter jurisdiction over Plaintiffs federal claims and also has supplemental jurisdiction over Florida state-law claims pursuant to 28 U.S.C. § 1367. The Court has personal jurisdiction over Defendants because in carrying out the conduct described in this Complaint, Defendants have availed themselves of the privilege of conducting business in Florida. *See, e.g., Diamond Crystal Brands, Inc. v. Food Movers Int'l*, 593 F.3d 1249, 1267 (11th Cir. 2010).

First, Defendants have intentionally extracted data from Florida corporations and used that data to send fraudulent communications to the corporations' employees. *Skyhop Techs., Inc. v. Narra*, 58 F.4th 1211, 1228 (11th Cir. 2023) ("SkyHop's CFAA claim arises from Indyzen's communications into Florida"); Dkt. 1 ¶¶ 16-19 (discussing forum contacts); 1-7 (discussing particular actions of each defendant). Second, Defendants have intentionally used servers located in Florida and services provided by ReliableSite.Net LLC, a U.S. company headquartered in Miami, Florida, in order to run the unauthorized copies of Windows Server at issue, and to use those instances of Windows Server to carry out BECs and financial fraud. *Id*. Defendants have thus acted within the state and directed the acts complained of toward the State, its residents, and this judicial district. *United States v. Auernheimer*, 748 F.3d 525, 533 (3d Cir. 2014) (Venue would be proper in any district where the CFAA violation occurred, or wherever any of the acts in furtherance of the conspiracy took place.").

In addition to their contacts with Florida, 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. *See, e.g., Charter Oil Co. v. Cotton (In re Charter Oil Co.)*, 189 B.R. 527, 530 (Bankr. M.D. Fla. 1995) ("The national contacts analysis requires that defendants have national contacts with the United States, not the State"). Defendants have acted at all times

relevant with knowledge that their acts would cause harm through computers located in Florida, thereby injuring Plaintiffs and others in in the United States. Dkt. 1 ¶¶ 16-19 (discussing forum contacts); 1-7 (discussing particular actions of each defendant). Further, Defendants intentionally availed themselves of the privilege of doing business in the United States by engaging in the following activities:

- fraudulently gaining access to Microsoft's Windows Server software, which required one or more Defendants to affirmatively enter into license agreements with Microsoft by misrepresenting that they would not use Microsoft's materials for illegal purposes;
- 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 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. domain registry.
- Contracting with and utilizing the services of Identity Digital, Inc., a U.S. domain registry.
- Using the U.S. wires to transmit computer commands and electronic communications to victim computers;
- Targeting and victimizing U.S. companies, organizations, and persons, as discussed below.

Dkt. 1 ¶¶ 17-19 (discussing contacts); Dkt. 39 (discussing assent to Windows Server license terms). 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 are thus subject to national service of process and jurisdiction is proper in this Court. Fed. R. Civ. P. 4(k)(2); *Gen. Cigar Holdings, Inc. v. Altadis, S.A.*, 205 F. Supp. 2d 1335, 1340 (S.D. Fla. 2002) ("personal jurisdiction is proper in any district, so long as sufficient national contacts have

been established."); *Republic of Pan. v. BCCI Holdings (Luxembourg) S.A.*, 119 F.3d 935, 942 (11th Cir. 1997) ("Section 1965(d) of the RICO statute provides for service in any judicial district in which the defendant is found."); *see also* Dkt. 18 (finding jurisdiction).

II. PLAINTIFFS HAVE ADEQUATELY STATED THEIR CLAIMS

"Akin to a 'reverse motion to dismiss for failure to state a claim[,]' a court evaluating a motion for default judgment must consider whether a pleading could survive a motion to dismiss." *Optima Tax Relief*, 2026 U.S. Dist. LEXIS 23114, at *2. When evaluating a motion to dismiss, a court looks to see whether the complaint "contain[s] sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Surtain*, 789 F.3d at 1245 (citing *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "This plausibility standard is met when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (citation omitted). The Complaints' allegations (and Plaintiffs' evidence) contain sufficient factual matter to state plausible claims for each cause of action asserted.

A. The Complaint Alleges Plausible CFAA Claims

Congress enacted the CFAA specifically to address computer crime. *See, e.g., Univ. Sports Pub. Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 384 (S.D.N.Y. 2010); *Big Rock Sports, LLC v. AcuSport Corp.*, 2011 U.S. Dist. LEXIS 110995, *3 (E.D.N.C. Sept. 26, 2011). "Any computer with Internet access [is] subject [to] the statute's protection." *Id.*; *United States v. Gasperini*, 2017 WL 2399693, at *3 (E.D.N.Y. June 1, 2017); *SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593, 608 (E.D. Va. 2005). *Inter alia*, the CFAA penalizes a party that intentionally accesses a protected computer without authorization in furtherance of a scheme to defraud. 18 U.S.C. § 1030(a)(4).

That is exactly what Defendants did when they accessed the computers that run the email systems of H2, GDCA, and their respective counterparties. Dkt 1. ¶¶5-11; 60-67; 68-75. Defendants' systematic use of social engineering to trick users and gain unauthorized access to victims' computers and data in furtherance of financial fraud schemes represent quintessential

CFAA violations. *See, e.g.*, *Microsoft Corp. v. Does 1-51*, No. 1:17-CV-4566, 2017 WL 10087886 at *4 (N.D. Ga. Nov. 17, 2017);*Volk v. Zeanah*, No. 608CV094, 2010 U.S. Dist. LEXIS 5621, at *4 (S.D. Ga. Jan. 25, 2010) ("The CFAA is meant to reduce hacking of computer systems/networks"); *Schwartz v. ADP, Inc.*, No. 2:21-cv-283-SPC-MRM, 2021 U.S. Dist. LEXIS 231613, at *3 (M.D. Fla. Dec. 3, 2021) ("The CFAA punishes computer hacking"). Defendants' conduct has caused harm to H2 and GDCA far exceeding the $5,000 jurisdictional threshold. Dkt. 1 ¶¶ 60-67.

B. The Complaint Alleges Plausible ECPA Claims

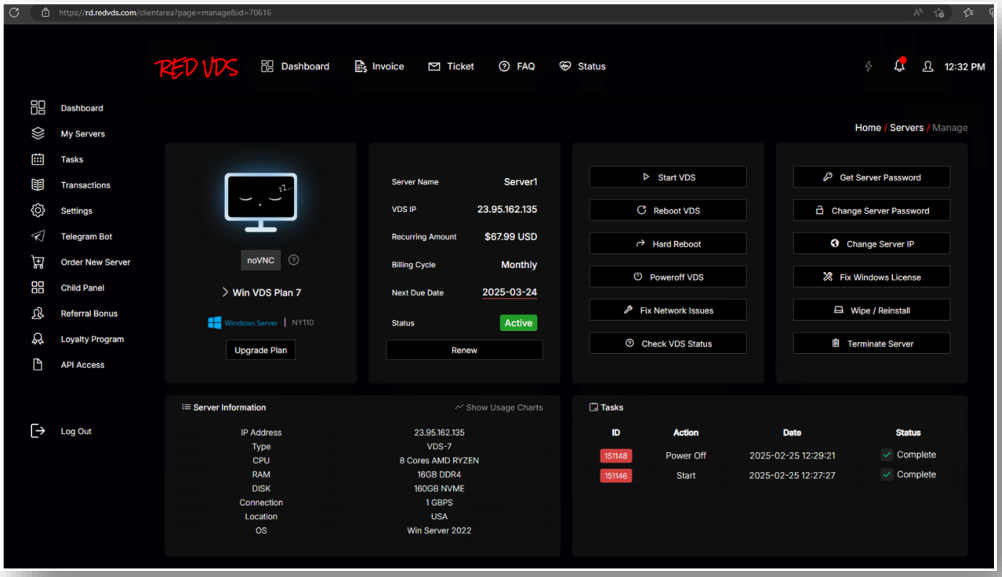
Like the CFAA, the ECPA is "primarily a criminal statute with a civil component aimed at creating a private right of action against computer hackers and electronic trespassers. *St. Johns Vein Ctr. v. StreamlineMD Ltd. Liab. Co.*, 347 F. Supp. 3d 1047, 1063 n.16 (M.D. Fla. 2018) (quoting *IPC Sys. v. Garrigan*, No. 1:11-CV-3910-AT, 2012 U.S. Dist. LEXIS 195619, at *24-25 (N.D. Ga. May 21, 2012)). The ECPA "makes it unlawful for anyone to '(1)intentionally access[] without authorization a facility through which an electronic communication services is provided; or (2) intentionally exceed[] an authorization to access that facility; and thereby obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage in such system.'" 18 U.S.C. § 2701(a). Section 2701 may be enforced in a civil action brought by "any…person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind." 18 U.S.C. § 2707(a).

Defendants' conduct "violates the ECPA because Defendants break into computing devices and computer networks with the direct intention of acquiring the contents of sensitive communications such as e-mails, voice mails, or other communications types." *Microsoft Corp. v. Does*, Civil Action No. 1:16cv993, 2017 U.S. Dist. LEXIS 145448, at *13 (E.D. Va. Aug. 1, 2017). H2 and GDCA both suffered losses because of Defendants' ECPA violations and unlawful access to their private communications with business partners. Dkt. 1 ¶¶ 60-67.

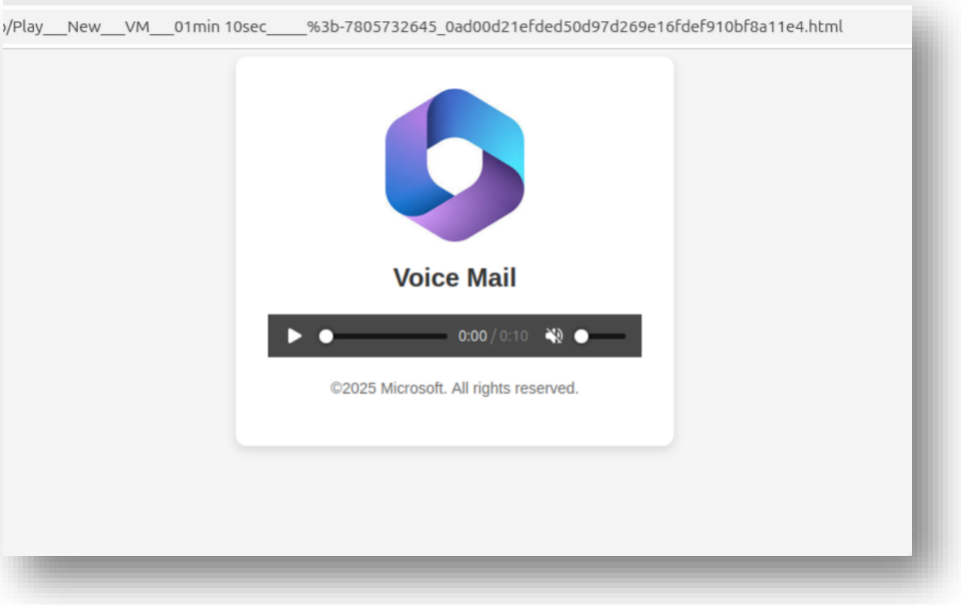
C. The Complaint Alleges Plausible Lanham Act Claims

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. Dkt. 1 ¶85. 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. Id. ¶ 86. 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. Id. ¶ 87.

Defendants have been 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. 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. Id. ¶¶ 88-89. And these unauthorized copies are marketed using Microsoft's trademarks, as depicted in Figure 1 of the Complaint:



Defendants' distribution of pirated, gray market versions of Windows Server and used Microsoft's trademarks to advertise and operate the RedVDS service is trademark infringement. *Microsoft Corp. v. Tierra Comput., Inc.*, 184 F. Supp. 2d 1329, 1333 (N.D. Ga. 2001) ("Defendants used counterfeit marks in the sale of the infringing software packages"); *Sueros & Bebidas Rehidratantes, S.A. de C.V. v. El Boqueron Imps. LLC*, No. 1:24-cv-03874-TWT, 2025 U.S. Dist. LEXIS 201965, at *8 (N.D. Ga. Oct. 10, 2025). In addition, 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. Id. ¶ 91. Figure 6 provides an example of one such infringing use.



Defendants' conduct constitutes numerous violations of the Lanham Act, including false designation of origin under section 1125(a), which prohibits use of a registered mark that is likely to deceive as to the affiliation, connection, or association of such person with another person. 15 U.S.C. § 1125(a)(1)(A). Here, Defendants' social engineering campaigns leverage Microsoft's trademarks and logos to make it look like the messages are legitimate communications from Microsoft. Such misuse of Microsoft's trademarks is a clear violation of Lanham Act § 1125(a) and Microsoft is likely to succeed on the merits. *See Garden & Gun, LLC v. Twodalgals, LLC*, 2008 U.S. Dist. LEXIS 79982 (W.D.N.C. 2008). Where, as here, a defendant uses a plainitff's trademark "likely to cause confusion, or to cause mistake, or to deceive," infringement is established. *E.g., Aeropost Int'l Servs. v. Aerocasillas, S.A.*, No. 09-23437-CIV-MORE, 2011 U.S. Dist. LEXIS 165635, at *26 (S.D. Fla. Mar. 31, 2011).

D. <u>The Complaint Alleges Plausible Copyright Infringement Claims</u>

Under § 106(3) of the Copyright Act, a copyright owner "has the exclusive rights…to distribute copies … of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending." 17 U.S.C. §106(3). *Microsoft Corp. v. Big Boy Distribution Ltd. Liab. Co.*, 589 F. Supp. 2d 1308, 1315 (S.D. Fla. 2008). A certificate of registration from the U.S.

Copyright Office is prima facie evidence of a copyright's validity. *See Glennon v. Rosenblum*, 325 F. Supp. 3d 1255, 1263 (N.D. Ala. 2018). Here, Microsoft holds a registration for Windows Server 2022, which Defendants are reproducing and distributing without authorization. Dkt 1. ¶¶77-78.

At some point prior to 2023, DOE 1 obtained a copy of Windows Server 2022 from Microsoft or a third party. Dkt. 1 ¶39. 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. Dkt. 1 ¶ 41. 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. Dkt. 1 ¶ 43. 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. Dkt. 1 ¶ 44. The elements of copyright infringement have thus been established. *See, e.g., Big Boy Distribution Ltd. Liab. Co.*, 589 F. Supp. 2d 1308 at 1321; *Microsoft Corp. v. Silver Star Micro, Inc.*, No. 1:06-cv-1350-WSD, 2008 U.S. Dist. LEXIS 1526, at *18 (N.D. Ga. Jan. 9, 2008) ("evidence here establishes that the Defendants duplicated Microsoft [software] without authorization and therefore infringed on Plaintiff's copyrights on that software.").

E. The Complaint Alleges Plausible RICO Claims

To succeed on a civil RICO claim, a private RICO plaintiff must allege "(1) conduct (2) of an enterprise (3) through a pattern (4) of racketeering activity." *Viridis Corp. v. TCA Glob. Credit Master Fund, LP*, 155 F. Supp. 3d 1344, 1354 (S.D. Fla. 2015) (citation omitted). "Racketeering activity" includes any act violative of several specific federal statutes, including 18 U.S.C. § 1343 wire fraud, 18 U.S.C. § 2319 criminal copyright infringement, and 18 U.S.C. § 2320 criminal

trademark infringement. 18 U.S.C § 1961. A civil RICO plaintiff must also show that multiple acts of racketeering "(5) caused (6) injury to the business or property of the plaintiff." *Cisneros v. Petland, Inc*., 972 F.3d 1204, 1211 (11th Cir. 2020).

The Complaint alleges that Defendants are members of an ongoing association-in-fact enterprise who are participants in the conduct of the RedVDS Enterprise. Dkt. 1 ¶¶ 38-44; 96-114. 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. For example, Defendants exchange referral fees and services in furtherance of the pattern of copyright and trademark infringement for financial gain carried out via the RedVDS Domains. Id. ¶¶ 109-110, *see also* Sections II(d) and II(cd), *supra*. Defendants have also engaged in racketeering by violating the federal wire fraud statute by repeatedly using the Internet to engage in financial fraud against entities like GDCA and H2. Dkt. 1 ¶¶ 107-108; *see, e.g., United States v. Azari,* No. 19-cr-610 (JGK), 2024 U.S. Dist. LEXIS 165416, at *1 (S.D.N.Y. Sep. 10, 2024); *United States v. 113 Virtual Currency Accounts,* Civil Action No. 20-606, 2020 U.S. Dist. LEXIS 142015, at *2 (D.D.C. Aug. 4, 2020) ("the hacking and theft of virtual currencies in violation of 18 U.S.C. § 1343").

F. <u>The Complaint Alleges Tort Claims</u>

Under Florida law, "withdrawing money from an account and exercising wrongful dominion and control over the money is an act of conversion." *Engineered Yacht Sols., Inc. v. Cohoon,* No. 24-61869-CIV/SINGHAL, 2025 U.S. Dist. LEXIS 124951, at *7 (S.D. Fla. June 30, 2025)(citations omitted). The complaint alleges that Defendants converted monies belonging *inter alia* to Plaintiffs H2 and GDCA. Dkt. 1 ¶¶ 128-132. The complaint also alleges that Defendants trespassed on third party computers and misused those computers to carry out their scheme. *Id.* ¶¶ 122-126, 54-64. Defendants wrongful exercise of dominion over such property is a tortious trespass. *See, e.g., AT&T Mobility LLC v. Does,* No. 1:09-cv-00277-JOF, 2012 U.S. Dist. LEXIS 198591, at *8 (N.D. Ga. Mar. 29, 2012). Defendants have also been unjustly enriched by their misconduct. Dkt. 1 ¶¶ 133-139; *Microsoft Corp. v. Malikov,* No. 1:22-CV-1328-MHC, 2022 U.S.

Dist. LEXIS 97298, at *4 (N.D. Ga. Apr. 8, 2022) (finding unjust enrichment in similar circumstances).

CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request entry of default judgment against Defendants.

Dated: April 28, 2026

Respectfully submitted,

/s/ Diana Marie 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

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