UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

Microsoft Corporation, a Washington State Corporation and Health-ISAC, Inc., a Florida non-profit organization,

Plaintiffs,

- v. -

Joshua Ogundipe,

and

John Does 1-4, Controlling A Computer Network and Thereby Injuring Plaintiffs and Their Customers,

Defendants.

Civil Action No. 25-cv-07111-JSR

MEMORANDUM OF LAW IN SUPPORT OF MOTION FOR DEFAULT JUDGMENT AND PERMANENT INJUNCTION

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

I. INTRODUCTION

Plaintiffs Microsoft Corporation ("Microsoft") and Health-ISAC, Inc., (collectively, "Plaintiffs") respectfully move the Court to grant default judgment and issue a permanent injunction against Defendants Joshua Ogundipe and John Does 1-4 (collectively "RaccoonO365 Defendants"). Plaintiffs seek default judgment against the Defendants under Fed. R. Civ. P. 55(b)(2) and an injunction (1) prohibiting the RaccoonO365 Defendants from operating their cybercriminal phishing operation and (2) preventing registration of malicious domains identified in the Court's temporary restraining order and preliminary injunction order.

Granting default judgment and permanent injunction against Defendants is proper in this matter because (i) Defendants have been properly served, (ii) Defendants are aware of these proceedings, have received full due process and have chosen not to respond to this action for fear of being arrested and/or prosecuted, which makes them non-responsive parties, (iii) the Clerk has entered a default against Defendants, (iv) there is long-standing precedent for granting default judgment and permanent injunctions against defendants in similar cybercrime circumstances, and (v) unless enjoined and held accountable, Defendants will continue to engage in their cybercriminal phishing scheme, causing great harm to Plaintiffs, their customers, and member organizations.

II. FACTUAL BACKGROUND

The RaccoonO365 Defendants are foreign cybercriminals that facilitate relentless and persistent phishing attacks against Microsoft and its customers, Health-ISAC and its member organizations, and the public. One of the most pernicious forms of cybercrime is known as "phishing." Phishing is the fraudulent practice of sending emails or other messages purporting to be from legitimate senders to induce recipients to reveal personal information, such as passwords or other credentials. It is a form of social engineering and a scam where the recipient-victim is

convinced to interact with the correspondence (referred to as the "lure").

RaccoonO365 Defendants manufacture and sell phishing kits that are designed to allow users of the kit to steal sensitive information, compromise business email and perpetrate ransomware and financial fraud. This business model of selling phishing kits and services for use by other cybercriminals is referred to as "Phishing-as-a-Service" or "PhaaS." The RaccoonO365 Defendants sell these kits to downstream cybercriminals who set up their own internet domains to perpetrate phishing attacks and add their domains to the RaccoonO365 Defendants' infrastructure. This results in a vast infrastructure overseen and administered by the RaccoonO365 Defendants comprised of hundreds of domains that launch phishing attacks against Microsoft and its customers.

RaccoonO365 Defendants develop phishing kits for cybercriminals to purchase and use for their cybercrime operations. Dkt. 17 ("Lyons Decl.") ¶ 13. These cybercriminals become part of the RaccoonO365 Defendants' operations when they in turn purchase domains and connect them to the RaccoonO365 infrastructure, deploy the RaccoonO365-branded phishing kits, conduct phishing attacks, use the stolen credentials to infiltrate the victims' systems, and leverage this infiltration to conduct additional cybercrimes, such as ransomware attacks. *Id.* ¶ 24. RaccoonO365 Defendants advertise that their kits can circumvent the security features of Microsoft products. In reality, the kits do not exploit any alleged Microsoft vulnerability. *Id.* ¶ 7. Rather the kits misuse Microsoft logos and mimic the appearance of authentic communications to deceive victims into thinking that the email communications they receive, the files they are directed to open, or links to websites used to enter their personal credentials are authentic and Microsoft-approved. *Id.* ¶ 7. In doing so, RaccoonO365 Defendants capitalize on and misuse the brand recognition that Microsoft has cultivated and the trust Microsoft has built with its customers. *Id*. ¶ 62. When a

victim clicks on a weaponized link or attachment, the RaccoonO365 Defendants are essentially ushered in through the front door of the victim's system.

The RaccoonO365 Defendants' phishing operation is made possible by leveraging a vast infrastructure of website domains. Lyons Decl. ¶18. Also known as a web address, domains are used to identify a website and allow users on the internet to access the website. *Id.* RaccoonO365 Defendants include the domains in their phishing emails and when the victims click on the malicious domains they are redirected to a RaccoonO365-controlled webpage and then unknowingly provide their credentials to Defendants. These domains re listed in **Appendix A** to the Proposed Order.

As a direct result of RaccoonO365 Defendants' conduct, Microsoft and Health-ISAC have been harmed. There has been damage to their brands and reputations, customers and member organizations have been deceived and defrauded, and both Microsoft and Health-ISAC have incurred significant damages and costs to investigate and remediate the harm caused by RaccoonO365 Defendants.

III. PROCEDURAL HISTORY

Plaintiffs filed this action on August 27, 2025, alleging violations of the Digital Millennium Copyright Act, Electronic Communications Privacy Act, the Racketeer Influenced and Corruptions Act, copyright infringement, trademark infringement and common law trespass to chattels, conversion, and unjust enrichment. Plaintiffs also sought a temporary restraining order aimed at shutting down the technical infrastructure that RaccoonO365 Defendants use to carry out their criminal attacks in this jurisdiction as well as other parts of the United States. Plaintiffs' TRO was supported by declarations from Microsoft and Health-ISAC, including detailed technical declarations explaining how Plaintiffs were able to identify and attribute the technical infrastructure to John Doe Defendants. See Dkts. 17 (Lyons Decl.), 18 (Monaco Decl.), and 19

(Weiss Decl.).

On August 27, 2025, the Court granted Plaintiffs' request for a TRO, ordering the transfer of the domains and the blocking of IP addresses that John Doe Defendants use to carry out their attacks. Dkt. 21. The Court specifically found that Plaintiffs were likely to prevail on each of their claims. *Id.* at 2-6. Additionally, the Court authorized alternative service given that John Doe Defendants' *modus operandi* is to obfuscate their identity and avoid detection. *Id.* at 11. The Court ordered Defendants to appear on September 24, 2025 to show cause, if any, why the Court should not enter a Preliminary Injunction. Dkt. 22.

Plaintiffs served John Doe Defendants via email service (utilizing the email addresses that Defendants used to register the domains that they deploy as part of their attacks) and publication on September 16, 2025. Plaintiffs' counsel used a service known as ReadNotify to track whether the service emails were delivered. By appending ".readnotify.com" to the end of each of the registrant emails, counsel is able to track the correspondence, including when the email is received and when it is viewed (to the extent that it is viewed). Plaintiffs' counsel confirmed using ReadNotify that the service emails were delivered and, in some instances, opened.

On September 24, 2025, the Court held a hearing concerning Plaintiffs' request for a preliminary injunction. Defendants failed to appear or file an opposition. The Court granted the preliminary injunction on September 24, 2025, and ordered third party registrars to transfer the website domains that RaccoonO365 Defendants use, own, or operate as part of their infrastructure to Microsoft in order to shut down Defendants' ability to carry out future attacks. Dkt. 32.

On April 1, 2026, Plaintiff requested a certificate of default. Dkt. 36. On April 3, 2026, the Clerk signed the Certificate of Default. Dkt. 38.

In connection with the foregoing injunction order, and consistent with the unrebutted

allegations in the Complaint, the Court has made several factual findings and conclusions of law. Among other findings, the Court concluded that:

- The Court has jurisdiction;
- Defendants have used and continue to use domains identified by Plaintiffs throughout this case to control the RaccoonO365 cybercriminal phishing operation;
- Defendants have used and continue to use domains containing Microsoft's trademarks and brands to deceive victims and control the RaccoonO365 cybercriminal phishing operation;
- Defendants' activities concerning the domains have violated or are likely to violate the (i) Computer Fraud and Abuse Act, 18 U.S.C. § 1030, (ii) Electronic Communications Privacy Act, 18 U.S.C. § 2701, (iii) Lanham Act 15 U.S.C. § 1114 *et seq*.) (iv) Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962, (v) and the common law doctrines of (vi) Trespass to Chattels, (vii) Conversion, and (viii) Unjust Enrichment; and
- Unless enjoined, Defendants are likely to continue to engage in conduct that violates the (i) Circumvention of Copyright Protection Systems under the (i) Computer Fraud and Abuse Act, 18 U.S.C. § 1030, (ii) Electronic Communications Privacy Act, 18 U.S.C. § 2701, (iii) Lanham Act 15 U.S.C. § 1114 *et seq*.) (iv) Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962, (v) and the common law doctrines of (vi) Trespass to Chattels, (vii) Conversion, and (viii) Unjust Enrichment.

IV. LEGAL STANDARD

Rule 55 of the Federal Rules of Civil Procedure authorizes the entry of a default judgment when a defendant fails to plead or otherwise defend in accordance with the Federal Rules. Fed. R. Civ. P. 55 establishes a two-step process for entering judgment against a party who fails to defend. *See City of N.Y. v. Mickalis Pawn Shop, LLC*, 645 F.3d 114, 128 (2d Cir. 2011). First,

"[w]hen a party against whom a judgment for affirmative relief is sought has failed to plead or otherwise defend, and that failure is shown by affidavit or otherwise, the clerk must enter the party's default." Fed. R. Civ. P. 55(a). Second, "the party must apply for a default judgment." Fed. R. Civ. P. 55(b). The Clerk's "certificate of default" pursuant to Fed. R. Civ. P. 55(a) provides notice to the defaulting party prior to the entry of default judgment by the court. In turn, Fed. R. Civ. P. 55(b)(2) authorizes courts to enter a default judgment against a properly served defendant who fails to file a timely responsive pleading. Entry of a default judgment is appropriate when "the adversary process has been halted because of an essentially unresponsive party." *Dae Woo Kim v. City of New York*, 1990 U.S. Dist. LEXIS 7137, 1990 WL 83465, at *2 (S.D.N.Y. June 13, 1990).

In determining whether to enter a default judgment, the Court is guided by several factors including: (i) whether the defendant's default was willful, (ii) whether the defendant has a meritorious defense to plaintiff's claims, and (iii) the level of prejudice the non-defaulting party would suffer as a result of the denial of the motion for default judgment. *Western Union Holdings, Inc. v. Haideri Paan & Cigarettes Corp*., 2020 U.S. Dist. LEXIS 38788 (E.D.N.Y. Mar. 5, 2020). When a plaintiff moves for a permanent injunction on a motion for default judgment, injunctive relief may be granted where "the moving party shows that (i) it is entitled to injunctive relief under the applicable statute and (ii) it meets the prerequisites for the issuance of an injunction." *Finkel v. Universal Sec. Sys.*, 2011 U.S. Dist. LEXIS 128239, *33-34 (E.D.N.Y. 2011).

Permanent injunctions depriving cybercrime defendants of their malicious infrastructure, on an ongoing basis in the future, have been entered by this Court in connection with entry of default judgments. *See Microsoft v. John Does 1-2*, Case No. 1:20-cv-01217-LDH-RER (E.D.N.Y), *Microsoft Corporation et al. v. John Does 1-39 et al.,* Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) and *Microsoft v. John Does 1-5*, 1:15-cv-06565-JBW-LB (E.D.N.Y. 2015).

Beyond this district, courts have granted default judgment and permanent injunctions to Microsoft against John Doe Defendants engaged in cybercriminal acts similar to those at issue in this case: See e.g. *Microsoft Corporation v. John Does 1-2*, Case No. 1:19-cv-00716-ABJ (D.C. 2019) (Berman-Jackson, J.); *Microsoft Corporation v. John Does 1-2,* Case No. 1:19-cv-01582 (E.D. Va. 2019) (O'Grady, J.); *Microsoft Corporation and FS-ISAC, Inc. v. John Does 1-2,* Case No. 1:20-cv-1171 (E.D. Va. 2020) (Trenga, J.).

V. DISCUSSION

Default judgment and permanent injunction are warranted because (i) Defendants have failed to appear and are purposefully non-responsive, (ii) Plaintiffs have adequately pled the case, and (iii) Plaintiffs would be harmed if the relief is not granted.

A. Defendants Have Been Served and Failed to Appear.

Defendants have failed to plead or otherwise respond this matter. Plaintiffs served Defendants with the Complaint, pleadings, and all key orders in this action pursuant to the means authorized by the Court in the TRO and Order for Preliminary Injunction. The Court authorized service by email, as follows: "the Complaint may be served by any means authorized by law, including (1) transmission by email . . . to the contact information provided by Defendants to Defendants' domain registrars and/or hosting companies and as agreed to by Defendants in the domain registration and/or hosting agreements." Dkt. 21 at 11.

On September 16, 2025, consistent with the TRO, Plaintiff served copies of the Summons, Complaint and Plaintiffs' TRO Application upon the registrant emails identified in Appendix A to the Complaint. Dkt. 28 ¶¶ 5-7. In connection with sending the service email to the registrant emails as identified in Appendix A, Plaintiff used Readnotify.com to track the email correspondence. By appending ".readnotify.com" to the end of each of the registrant's emails, Plaintiff's counsel was able to track the correspondence, including when the email was received and when it was opened

(to the extent the recipient opens the email). Plaintiff's counsel has reviewed the ReadNotify.com records, and have confirmed that successful delivery (*i.e.*, no bounce back) of the emails and have confirmed that in many instances the service email was opened by the recipient.

The Court also authorized service by Internet publication, as follows: "the Complaint may be served by any means authorized by law, including . . . publishing notice on a publicly available Internet website." Dkt. 21 at p. 10.

On September 16, 2025, the "Notice of Pleadings" website, which is hosted by Crowell & Moring, went live. This website contains copies of the pleadings filed in this case to date, including all Orders issued by this Court, and information regarding the preliminary injunction hearing. Dkt. 28 ¶¶ 8-10.

Defendants have purposefully taken the position of a non-responsive party. The Clerk has subsequently entered a default against the Defendant. Dkt. 38.

B. Plaintiffs Have Adequately Pled Each of Their Claims

The Complaint alleges that Defendants have violated (i) Computer Fraud and Abuse Act, 18 U.S.C. § 1030, (ii) Electronic Communications Privacy Act, 18 U.S.C. § 2701, (iii) Lanham Act 15 U.S.C. § 1114 *et seq.*) (iv) Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962, (v) and the common law doctrines of (vi) Trespass to Chattels, (vii) Conversion, and (viii) Unjust Enrichment. Each of these claims has been adequately pled. The law requires a court to accept as true a plaintiff's well-pled fact when uncontested by a defaulting defendant. *See Priestley v. Headminder, Inc.,* 647 F.3d 497, 504 (2d Cir. 2011). There is no question that a "default judgment entered on well-pleaded allegations in a complaint establishes a defendant's liability." *Trans World Airlines, Inc. v. Hughes,* 449 F.2d 51, 69 (2d Cir. 1971), *rev'd on other grounds,* 409 U.S. 363 (1973).

CFAA Claim. The CFAA penalizes a party that: (1) intentionally accesses a protected

computer without authorization, and as a result of such conduct, causes damage, 18 U.S.C. § 1030(a)(5)(C); or (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer, 18 U.S.C. § 1030(a)(2)(C); or (3) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage to a protected computer, 18 U.S.C. § 1030(a)(5)(A). A "protected computer" is a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communications in the United States." 18 U.S.C. § 1030(e)(2)(B). The phrase "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled to obtain or alter." *Id.* (citing 18 U.S.C. § 1030(e)(6)). To prosecute a civil claim under the CFAA, a plaintiff must demonstrate loss or damage in excess of $5,000.

"The phrase 'exceeds authorized access' means 'to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter.'" *JBCHoldings NY, LLC v. Pakter*, 931 F. Supp. 2d 514, 523 (S.D.N.Y. 2013) (citing 18 U.S.C. § 1030(e)(6)). The entire purpose of RaccoonO365 Defendants' phishing operation is to steal credentials to infiltrate the systems of the victim. Lyons Decl. ¶ 15. RaccoonO365 Defendants' end goal is to deceive the victim into providing credentials and 2FA information so that it can surreptitiously and without authorization take control. Indeed, by its very nature, the AiTM model employed by RaccoonO365 Defendants exceeds authorized access. Lyons Decl. ¶ 50.

"[D]amage, in turn, is defined as 'any impairment to the integrity or availability of data, a

program, a system, or information.'" *Sewell v. Bernardin*, 795 F.3d 337, 340 (2d Cir. 2015) (citing 18 U.S.C. § 1030(e)(8)); *Nexans Wires S.A. v. Sark-USA, Inc.*, 166 F. App'x 559, 563 (2d Cir. 2006) (damage includes "investigating and remedying damage to a computer, or a cost incurred because the computer's service was interrupted"); *Univ. Sports Publ'ns Co.*, 725 F. Supp. 2d at 387 (loss includes "the costs of investigating security breaches constitute recoverable 'losses,' even if it turns out that no actual data damage or interruption of service resulted from the breach). As a direct result of RaccoonO365 Defendants' conduct, Microsoft has been forced to spend at least $250,000 investigating and remediating RaccoonO365 Defendants' activities. Lyons Decl. ¶ 66. Similarly, as a direct result of RaccoonO365 Defendants' conduct, Health-ISAC and its member organizations have been forced to spend at least $12,000 to investigate RaccoonO365 Defendants' activities and mitigate the impact on the member organizations. Weiss Decl. ¶ 13.

RICO Claim. The Racketeer Influenced and Corrupt Organizations Act ("RICO") prohibits "any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity." 18 U.S.C. § 1962(c). RICO also makes it unlawful "for any person to conspire to violate" that provision, regardless of whether that conspiracy ultimately comes to fruition. 18 U.S.C. §1962(d). "Any person injured in his business or property by reason of a violation of" either of these provisions is entitled to recovery, 18 U.S.C. § 1964(c), and this court has "jurisdiction to prevent and restrain" such violations "by issuing appropriate orders." 18 U.S.C. 1964(a). *See also United States v. Carson*, 52 F.3d 1173, 1181-82 (2d Cir. 1995) ("the jurisdictional powers in § 1964(a) serve the goal of foreclosing future violations," and "the equitable relief under RICO is intended to be broad enough to do all that is necessary."); *United States v. Sasso*, 215 F.3d 283, 290 (2d Cir. 2000)

(same); *Trane Co. v. O'Connor Sec.*, 718 F.2d 26, 29 (2d Cir. 1983) (injunction proper under RICO where plaintiff establishes "a likelihood of irreparable harm").

Defendants in this case have formed and associated with such an enterprise affecting foreign and interstate commerce and have engaged in an unlawful pattern of racketeering activity involving thousands of predicate acts of fraud and related activity in connection with violations of (i) the Computer Fraud and Abuse Act (18 U.S.C. § 1030(a)(5)(A)), incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(G) and 18 U.S.C. § 2332b(g)(5)(B), and (ii) wire fraud (18 U.S.C. § 1343), incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(B).

The Racketeering Enterprise has existed at least since July 2024 when Defendants Joshua Ogundipe, John Doe 1-2 conspired to, and did, form an associated-in-fact Racketeering Enterprise with a common purpose of developing, selling, and implementing phishing kits, as well as operating a phishing infrastructure resulting in criminal activities including business email compromise, financial fraud, and ransomware. Lyons Decl. ¶ 16. Specifically, John Does 1-2 work in tandem with Ogundipe to provide technical and administrative support, including for example, managing the administrative panel and customer dashboard that is made available to customers. *Id.* ¶ 35. Based on the communications in the Telegram channel, Microsoft identified participants in the channel who appeared to be involved in the administration of the RaccoonO365 store and operation. *Id.* ¶ 19. John Does 3-4 joined the conspiracy and began participating in the Racketeering Enterprise at various times thereafter, specifically when they purchased the kits, purchased the phishing and cover domains, connected the domains to the infrastructure, and began using the kits to conduct phishing attacks. *Id.* ¶ 20. The Racketeering Enterprise has continuously and effectively carried out its purpose of operating their PhaaS business model, with use of the RaccoonO365-branded phishing kits at the core of the operation ever since, and will continue to

do so absent the relief Plaintiffs request. RaccoonO365 Defendants' racketeering acts include persistent violations of the Computer Fraud and Abuse Act. Violation of the CFAA is incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(G) and 18 U.S.C. § 2332b(g)(5)(B).

ECPA Claim. The Electronic Communications Privacy Act prohibits "intentionally access[ing] without authorization a facility through which electronic communications are provided" or doing so in excess of authorization, and, in so doing, obtaining, altering, or preventing authorized access to an electronic communication while it is in electronic storage. 18 U.S.C. § 2701(a); *Organization JD LTDA v. United States DOJ*, 124 F.3d 354, 359 (2d Cir. 1997) ("The ECPA was enacted to 'protect against the unauthorized interception of electronic communications.'"); *In re Doubleclick Privacy Litig.*, 154 F. Supp. 2d at 507 ("18 U.S.C. § 2701 *et. seq.* … aims to prevent hackers from obtaining, altering, or destroying certain stored electronic communications."). ECPA is violated when Defendants log into Plaintiffs' customers' account without permission (including with stolen credentials) and intentionally access the contents of an inbox. *See Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp*, LLC, 759 F. Supp. 2d 417 (S.D.N.Y. 2010) (holding that an employer's unauthorized access of an employee's personal emails stored on a third-party communication service provider's system violated the ECPA).

Here, the object of RaccoonO365 Defendants' scheme is to obtain the credentials and then surreptitiously infiltrate the victims' systems. Lyon Decl. ¶ 28. From there, the cybercriminals move within the system, including accessing email inboxes for the purpose of identifying additional targets for subsequent phishing and engaging in business email compromise to exfiltrate sensitive emails and information. *Id.* The RaccoonO365 Defendants do not have permission or authority to access the contents of the victims' inboxes; they use stolen credentials and violate ECPA. Through this unauthorized access, RaccoonO365 Defendants intercepted, had access to,

obtained, altered, or prevented legitimate, authorized access to, wire and electronic communications transmitted through the computers and infrastructure of Microsoft and its users. *Id.* ¶ 30. Obtaining stored electronic information in this way, without authorization, is a per se violation of ECPA.

Lanham Act Claim. Section 1114(1)(a) of the Lanham Act prohibits use of a reproduction, counterfeit, copy or "colorable imitation" of a registered mark in connection with the distribution of goods and services where such use is likely to cause confusion or mistake or to deceive. 15 U.S.C.§ 1114(1)(a). The Lanham Act also prohibits use of a trademark, any false designation of origin, false designation of fact or misleading representation of fact which is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person. 15 U.S.C. § 1125(a).

RaccoonO365 Defendants use Plaintiffs' registered and distinctive trademarks in fraudulent schemes designed to mislead victims into clicking on links to interact with malicious websites and fraudulent versions of Defendants' websites. Lyons Decl. ¶ 65. This conduct deceives victims, engenders confusion, and causes them to mistakenly associate Plaintiffs with this activity. *Id*. For example, when victims click on a link in a malicious phishing email, the victim is routed to a login page that appears to be a Microsoft login page. *Id*. ¶ 30. Anyone seeing this page would naturally believe that they were interacting with a legitimate login page. Beyond the logo, the look and feel of the page is identical to a legitimate Microsoft login page. *Id*. ¶ 50. This is done intentionally: to deceive customers, to create confusion, and to trick customers into believing that it is authentic. *Id*. Customers encountering this page would have no reason to doubt that it is not Microsoft-affiliated. Likewise, nearly all of the domains used by RaccoonO365 Defendants

contain some reference to Microsoft, its products, and its services. *Id*. ¶ 39. Coupled together—a domain that appears to reference Microsoft and a login page that uses Microsoft's logos—is textbook trademark infringement.

In addition to constituting infringement under section 1114 of the Lanham Act, RaccoonO365 Defendants' conduct also constitutes false designation of origin under section 1125(a), which prohibits use of a registered mark that "is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person." 15 U.S.C. § 1125(a)(1)(A). Here, RaccoonO365 Defendants' misuse of Plaintiffs' famous marks in connection with malicious conduct aimed at Plaintiffs' customers and the public dilutes the famous marks by tarnishment and by blurring consumers' associations with the marks.

Specifically, RaccoonO365 Defendants' misleading and false use of Microsoft's trademarks—including Microsoft®, Windows®, Microsoft 365®, Office365®, Office®, Microsoft Office®, SharePoint®, OneDrive®, Outlook®, and Azure®. C trademarks— causes confusion and mistakes as to their affiliation with RaccoonO365 Defendants' malicious conduct. *See supra*. This activity is a clear violation of Lanham Act, section 1125(a), and Plaintiffs are likely to succeed on the merits. *See e.g.*, *Hamzik v. Zale Corp.*, 2007 U.S. Dist. LEXIS 28981 (N.D.N.Y. April 18, 2007); *Hotmail Corp. v. Van$ Money Pie Inc.*, 1998 WL 388389, at *3 (N.D. Cal. Apr. 16, 1998) (spam e-mail with purported "from" addresses including plaintiff's trademarks constituted dilution).

Tort Claims. RaccoonO365 Defendants' conduct is tortious under the common law doctrines of trespass to chattels, conversion, and unjust enrichment. "Conversion is the

unauthorized assumption and exercise of the right of ownership over goods belonging to another to the exclusion of the owner's rights." *Pac. M. Int'l Corp. v. Raman Int'l Gems, Ltd.*, 888 F. Supp. 2d 385, 396 (S.D.N.Y. 2012). Conversion applies to electronic computer records and data. *Thyroff. Nationwide Mut. Ins. Co.*, 8 N.Y.3d 283,288-89 (2007); *see also Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 697 (D. Md. 2011) (holding defendant liable for conversion where defendant replaced current version of plaintiffs' website with former version, because such action effectively "dispossessed [plaintiff] of the chattel;" *i.e.*, its website).

The related tort of trespass to chattels applies where personal property of another is used without authorization, but the conversion is not complete. *Sch. of Visual Arts v Kuprewicz*, 3 Misc. 3d 278, 281 (2003); *Yo! Braces Orthodontics, PLLC v. Theordorou*, 2011 N.Y. Misc. LEXIS 1820, *8 (Apr. 19, 2011). New York law recognizes the tort of trespass to chattels in connection with computer intrusion. *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 404 (2d Cir. 2004) (affirming grant of injunction against defendants accessing plaintiff's computers using automated software); *Democratic Nat'l Comm. v. Russian Fed'n*, 392 F. Supp. 3d 410, 449 (S.D.N.Y. 2019) ("Hacking a computer network may qualify as trespass to chattels.")

Here, RaccoonO365 Defendants exercised dominion and authority over Microsoft's proprietary services like Outlook and Azure by intruding into its servers supporting those services to gain access to content stored on those servers like email and access to other applications on the Azure platform. Lyons Decl. ¶ 53. These acts deprived Microsoft and its customers of their right to control the content, functionality, and nature of its software and services, and such computer hacking amounts to tortious conduct under the doctrines of conversion and trespass to chattels. The elements of a claim of unjust enrichment are that a (1) defendant benefitted, (2) at plaintiff's expense, and (3) equity and good conscience require restitution. *Beth Israel Med. Ctr. v. Horizon*

Blue.Cross and Blue Shield, 448 F.3d 573,586 (2d Cir. 2008). RaccoonO365 Defendants' misuse of Microsoft's and Health-ISAC member organizations' brand and reputations constitutes unjust enrichment. Defendants have been unjustly enriched through their unlawful use of Plaintiffs' trademarks, brand names, goodwill, goods, and services to carry out their PhaaS enterprise. Plaintiffs have spent considerable resources to develop their brands, such that the customers and public trust their branding and reputation. Lyons Decl. ¶ 63. In order to ensure greater efficacy of their criminal operation, RaccoonO365 Defendants usurp this goodwill. *Id.* ¶ 2. By leveraging and misusing the branding and reputations, RaccoonO365 Defendants benefit because it is more likely that their phishing attacks are successful. Lyons Decl. ¶ 7. The benefit to RaccoonO365 Defendants (greater success at committing cybercrime) is at the expense of Microsoft and Health-ISAC, who suffer brand tarnishment and harm to customers and member organizations as a result. *Id.*

C. Plaintiffs Are Entitled to a Permanent Injunction.

A permanent injunction is appropriate when a plaintiff (1) shows that an inadequate remedy is available at law, such as by showing that irreparable harm would result if an injunction were not granted, and (2) succeeds on the merits of his claim. *See Weizmann Institute of Science v. Neschis,* 229 F.Supp.2d 234, 258 (S.D.N.Y.2002). Thus, the standard for a permanent injunction is essentially the same as for a preliminary injunction, except that the plaintiff must actually succeed on the merits. *Dodge v. Cnty. of Orange*, 282 F. Supp. 2d 41, 71 (S.D.N.Y. 2003)

i. Plaintiffs Have Suffered Irreparable Harm That Cannot Be Compensated Monetarily.

It is well-settled that consumer confusion and injury to business goodwill constitute irreparable harm. *See Tom Doherty Assocs., Inc. v. Saban Entm't, Inc.*, 60 F.3d 27, 37-38 (2d Cir. 1995) (recognizing that the loss of prospective business or goodwill supports a finding of irreparable harm); *Broker Genius, Inc. v. Volpone*, 313 F. Supp. 3d 484, 496 (S.D.N.Y. 2018)

(same). Here, Defendants tarnish Plaintiffs' valuable trademarks, injuring Microsoft's goodwill, creating confusion about the source of Defendants' malware, and damaging the reputation of and confidence in the services of Microsoft's products, including Office 365.

First, RaccoonO365-branded phishing kits are customized to circumvent the security features of Microsoft products, use Microsoft logos, and mimic the appearance of authentic communications to deceive victims into thinking that the email communication they receive, the files they are directed to open, or links to websites used to enter their personal credentials are authentic and Microsoft-approved. Lyons Decl. ¶ 7.

Second, the RaccoonO365 Defendants leverage Microsoft systems and programs, such as Outlook, Microsoft 365, and Office 365 to further enhance the perceived legitimacy of the attack. Similarly, because the login pages that RaccoonO365 Defendants use include the Microsoft name and logo, the victim will be completely unaware of the threat and believe that the link is to a legitimate Microsoft webpage and trustworthy, when in fact, it is malicious. *Id.* ¶ 63. In doing so, RaccoonO365 Defendants capitalize on and misuse the brand recognition that Microsoft has cultivated, and the trust Microsoft has built with its customers and that customers have come to expect. *Id.* ¶ 63.

Third, the domains used by RaccoonO365 are intentionally designed to mimic the name Microsoft and its products. *Id.* ¶ 64. This means that when a victim is phished and is redirected to a RaccoonO365-controlled domain, the victim will see a domain that on its face looks like a Microsoft domain and will not be suspicious of these domains because of how similar they appear. *Id.* Customers expect certain quality from Microsoft. When "Microsoft" systems and products are used in connection with cybercrime, customers will mistakenly believe that Microsoft is responsible for the attack. Lyons Decl. ¶ 65. Customers subjected to the negative effects of

Defendants' phishing attacks sometimes incorrectly believe that Microsoft is the source of the problem, and thus there is a significant risk that Microsoft customers will be confused in this way in the future. *Id.*

Additionally, phishing attacks continue to be a major cybersecurity concern for Health-ISAC members and the broader health sector, with significant financial and operational consequences. Dkt. 19 ("Weiss Decl." ¶ 7. Phishing is the top infection vector for cyber attacks in the healthcare industry. For example, phishing simulations conducted in healthcare organizations result in a click rate of 10-30% for employees who are deceived by the phishing email. *Id.* The average downtime for a healthcare company successfully attacked by a cybercriminal is 19 days—during which time patient care can be severely impacted through canceled surgeries, diverted ambulances, and compromised medical records. *Id.* RaccoonO365-branded phishing kits harm the brand reputation of Health-ISAC's member organizations. For example, when member organizations are attacked, their brand and reputation are irreparably harmed when patients are no longer able to rely on the security of patient data and the healthcare network system as a whole is put at risk. *Id.* ¶ 21. Because Health-ISAC organizations are under attack, they are forced to expend tremendous resources to defend themselves. *Id.* ¶ 21.

ii. The Balance of Equities Favors a Permanent Injunction.

Defendants will suffer no harm to any legitimate interest if a permanent injunction is issued, because Defendants have no legitimate interest in committing cybercrime and violating U.S. laws. Moreover, because Defendants are engaged in an illegal scheme to defraud consumers and injure Plaintiffs, the balance of equities is in favor of granting an injunction. *See, e.g.*, *N. Atl. Operating Co., Inc. v. Evergreen Distributors*, LLC, 2013 WL 5603602, at *13 (E.D.N.Y. Sept. 27, 2013) ("Where '[t]he only hardship to Defendant from [an] injunction would be to prevent him from engaging in further illegal activity, [] the balance clearly weighs in Plaintiffs' favor.'"

(*quoting DISH Network L.L.C. v. DelVechhio*, 831 F. Supp. 2d 595, 601-02 (W.D.N.Y. 2011))). On one side of the scales of equity rests the harm to Microsoft, its customers, Health-ISAC, its member organizations, and the public, caused by RaccoonO365 Defendants, while on the other side, RaccoonO365 Defendants can claim no legally cognizable harm because an injunction would only require RaccoonO365 Defendants to cease illegal activities.

iii. A Permanent Injunction is in the Public Interest.

The public interest is clearly served by enforcing statutes designed to protect the public, such as the Lanham Act, CFAA, and ECPA. *See, e.g.*, *ProFitness Phys. Therapy Ctr. v. Pro-Fit Ortho. And Sports Phys. Therapy P.C.*, 314 F.3d 62, 68 (2d Cir. 2002) (finding a "strong public interesting in preventing public confusion"); *Juicy Couture, Inc. v. Bella Intern. Ltd.*, 930 F. Supp. 2d 489, 505 (S.D.N.Y. 2013) (finding that grant of an injunction in case under the Lanham Act would not disserve the public interest, where there was a strong interest in preventing public confusion over parties' competing trademark); *FXDirectDealer, LLC v. Abadi*, 2012 WL 1155139, at *8 (S.D.N.Y. Apr. 5, 2012) (public interest weighed in favor of injunction to enforce CFAA); *DISH Network L.L.C. v. DelVechhio*, 831 F. Supp. 2d 595, 601-02 (W.D.N.Y. 2011) (public interested weighed in favor of injunction to enforce ECPA).

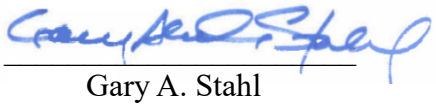
VI. CONCLUSION

For the reasons set forth in this brief, and based on the Complaint, the evidence submitted in this case and the Court's prior orders, Plaintiffs respectfully request that the Court grant Plaintiffs' Motion for Default Judgment and Permanent Injunction.

Dated: May 11, 2026

Respectfully submitted,

CROWELL & MORING LLP

By: 

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

Jeffrey L. Poston (*pro hac vice*)
CROWELL & MORING LLP
1001 Pennsylvania Ave. NW
Washington, DC 20004
T: (202) 624 2500
F: (202) 628-5116
jposton@crowell.com

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

Attorneys for Plaintiffs Microsoft Corporation and Health-ISAC, Inc.

CERTIFICATION PURSUANT TO LOCAL RULE 7.1(c)

The total number of words in the foregoing Memorandum of Law, including point headings and footnotes, and excluding the caption, Table of Contents, Table of Authorities and the signature block is 5,861.

s/Gary A. Stahl

GARY A. STAHL