IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION, et al.,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	Case No. 1:24-cv-02013 (RDA/WBP)
	)	
ABANOUB NADY, et al.,	)	
	)	
Defendants.	)	

REPORT AND RECOMMENDATION

Plaintiffs Microsoft Corporation ("Microsoft") and LF Projects, LLC ("LF Projects") (collectively, "Plaintiffs") moved for default judgment and a permanent injunction under Rule 55(b) of the Federal Rules of Civil Procedure against Defendants Abanoub Nady and John Does 1–4 (collectively, "Defendants"). ("Motion," ECF No. 46.) Under 28 U.S.C. § 636(b)(1)(C), I recommend that the district judge grant the Motion.

I. Procedural Background

On November 12, 2024, Plaintiffs filed a Complaint (ECF No. 1), a Motion for a Protective Order Temporarily Sealing Documents (ECF No. 2), an Application for an Emergency Temporary Restraining Order ("TRO") (ECF No. 4), and an Application for an Order to Show Cause Re Preliminary Injunction (*id.*). Plaintiffs allege that Defendants manufacture and sell illegal phishing kits, deceptively branded as "ONNX," designed to steal sensitive information and to perpetrate business email compromise, ransomware, and financial fraud against Microsoft customers (the "Fake ONNX" scheme). (ECF No. 1 at 1.) Plaintiffs assert claims under the Computer Fraud and Abuse Act ("CFAA") (Count I), the Racketeer Influenced and Corrupt Organizations Act ("RICO") (Counts II–III), the Electronic Communications Privacy Act

("ECPA") (Count IV), and the Lanham Act (Counts V–VII), along with Virginia common-law claims for trespass to chattels, conversion, and unjust enrichment (Counts VIII–X). (*Id.* at 1–2.)

On November 13, 2024, the Court entered a protective order and a TRO in favor of Plaintiffs (ECF Nos. 16, 19), which the district judge converted into a preliminary injunction on December 12, 2024 (ECF No. 31). On January 29, 2025, Plaintiffs filed a Motion for Limited Authority to Conduct Discovery Necessary to Identify and Serve Doe Defendants (ECF No. 34), which the Court granted the following day (ECF No. 37).

On November 21, 2024, Plaintiffs served Defendants by publishing notice of this action on a "Notice of Pleadings" website hosted by Plaintiffs' counsel, Crowell & Moring, and, in December 2024, by emailing the Complaint, the Summons, the Notice of Hearing, the TRO, and Appendix A to the email address listed for each domain's registrant. (ECF No. 43 at 3; ECF No. 43-1 ¶¶ 17–20; ECF No. 27 at 3.) Rule 12 required Defendants to answer within 21 days of service. *See* Fed. R. Civ. P. 12(a)(1)(A)(i). Defendants never filed a responsive pleading, so Plaintiffs asked the Clerk to enter a default, which the Clerk entered on June 9, 2026. (ECF Nos. 43, 45.)

The Court held a hearing on Plaintiffs' Motion on August 21, 2026. (ECF No. 50, 57.) Plaintiffs' counsel appeared, but no one appeared for Defendants. (ECF No. 57.)

II. Factual Background

The following facts come from the Complaint (ECF No. 1), the Motion (ECF No. 46), the Brief in Support of Default Judgment (ECF No. 47), and the Supplemental Submission (ECF No. 54).

Microsoft, a Washington corporation, maintains its principal place of business in Redmond, Washington, and LF Projects, a Delaware limited liability company, maintains its

principal place of business in Wilmington, Delaware. (ECF No. 1 ¶¶ 9–10.) Microsoft offers integrated computer software and hardware systems globally. It owns the MICROSOFT, WINDOWS, MICROSOFT 365, OFFICE365, OFFICE, MICROSOFT OFFICE, SHAREPOINT, ONEDRIVE, OUTLOOK, MICROSOFT EXCHANGE SERVER, TEAMS, MICROSOFT DEFENDER, WINDOWS VISTA, SWAY, and AZURE Marks (collectively, "Microsoft Marks"). (*Id.* ¶ 23.) LF Projects has established multiple open-source and industry projects, including the Open Neural Network Exchange ("ONNX"), an open-source artificial intelligence ecosystem of technology companies and research organizations that establishes open standards for representing machine learning algorithms and software tools. (*Id.* ¶¶ 7, 24.) LF Projects owns the ONNX Mark and licenses it to the ONNX Exchange. (*Id*. ¶ 24.)

Defendants offer "Phishing-as-a-Service" to other cybercriminals. (*Id.* ¶ 3.) They manufacture, sell, and help deploy pre-packaged toolsets ("phishing kits") that include email templates, fake website templates, domain registration services, and customer support. (*Id*. ¶¶ 2–3.) Defendants use the ONNX and Microsoft Marks to design websites that mimic legitimate Microsoft and ONNX sites. (*Id*. ¶ 4–7.) After an unsuspecting Microsoft customer clicks a phishing email or website link, Defendants' customers can bypass Microsoft security measures, establish a permanent presence in the victim's computer system, intercept communications, and steal personal and business information. (*Id*. ¶¶ 2–7.)

Defendants jointly own, rent, lease, or otherwise control the organization's infrastructure and sell, distribute, implement, and use the phishing kits. (*Id.* ¶ 19.) Abanoub Nady, an Egyptian resident, controls the phishing organization. (*Id.* ¶ 11.) John Doe 1 manages the organization and controls its technical infrastructure, and John Doe 2 provides technical support. (*Id.* ¶¶ 13–14.) John Doe 3, a cybercriminal who purchased an ONNX-branded phishing kit, registered a new

phishing domain and incorporated it into the organization and its technical infrastructure. (*Id.* ¶ 15.) John Doe 4, also a cybercriminal, took an existing domain already connected to an ONNX-branded phishing kit and incorporated it into the organization. (*Id.* ¶ 16.)

III. Proposed Findings of Fact and Recommendations

A. Jurisdiction and Venue

The Court must confirm that it has subject matter jurisdiction and personal jurisdiction before entering default judgment.

The Court has subject matter jurisdiction over all counts. Federal law grants district courts original jurisdiction over "all civil actions arising under the Constitution, laws, or treaties of the United States," 28 U.S.C. § 1331, including civil actions arising under federal trademark law. 28 U.S.C. § 1338(a); 15 U.S.C. § 1121(a). A court may also exercise supplemental jurisdiction over state-law claims "so related" to the federal claims "that they form part of the same case or controversy." 28 U.S.C. § 1367(a). Claims meet that test when they "derive from a common nucleus of operative fact." *United Mine Workers of Am. v. Gibbs*, 383 U.S. 715, 725 (1966). In deciding whether to exercise that jurisdiction, courts weigh "convenience and fairness to the parties, the existence of any underlying issues of federal policy, comity, and considerations of judicial economy." *Shanaghan v. Cahill*, 58 F.3d 106, 110 (4th Cir. 1995).

Here, Counts I through IV arise under the CFAA, RICO, and the ECPA, and Counts V through VII arise under the Lanham Act. (ECF No. 1 ¶ 21, 43–45.) This Court therefore has subject matter jurisdiction over Counts I through VII under 28 U.S.C. §§ 1331 and 1338(a) and 15 U.S.C. § 1121(a). The Court should exercise supplemental jurisdiction over the trespass, conversion, and unjust enrichment claims because they arise from the same phishing scheme. Those claims raise no novel or complex issues of state law and do not predominate over the

seven federal claims. *See* 28 U.S.C. § 1367(c)(1)-(2); *Royal Canin U.S.A., Inc. v. Wullschleger*, 604 U.S. 22, 31 (2025). Finally, this case has been pending for nearly two years, and judicial economy warrants exercising § 1367 jurisdiction over Counts VIII through X.

The Court may also exercise personal jurisdiction over Defendants. The Due Process Clause requires that a nonresident defendant have "certain minimum contacts with [the forum state] such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice.'" *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945); *see ePlus Tech., Inc. v. Aboud*, 313 F.3d 166, 176 (4th Cir. 2002) (explaining that Virginia long arm statute extends to the limits of due process). To determine whether it has specific personal jurisdiction, a court considers (1) the extent to which the defendant purposefully availed itself of the privilege of conducting activities in the state; (2) whether the plaintiff's claims arise out of those activities; and (3) whether the exercise of personal jurisdiction would be constitutionally reasonable. *See Perdue Foods LLC v. BRF S.A.*, 814 F.3d 185, 189 (4th Cir. 2016). A nonresident defendant's electronic activities satisfy due process when the defendant "(1) directs electronic activity into the State, (2) with the manifested intent of engaging in business or other interactions within the State, and (3) that activity creates, in a person within the State, a potential cause of action cognizable in the State's courts." *ALS Scan, Inc. v. Dig. Serv. Consultants, Inc.*, 293 F.3d 707, 714 (4th Cir. 2002).

First, Defendants purposefully availed themselves of the privilege of conducting activities in Virginia. Although Defendants appear to live abroad, they intentionally reached into this district by directing malicious computer code and launching phishing attacks against individuals and companies in this district to steal their information. (ECF No. 1 ¶ 22; ECF No. 54 at 7.) *See Zaletel v. Prisma Labs, Inc.*, 226 F. Supp. 3d 599, 605–08 (E.D. Va. 2016)

(analyzing personal jurisdiction based on electronic activity directed into Virginia); *see also Ontel Prods. Corp. v. Unincorporated Ass'ns Identified in Schedule A*, No. 1:21-cv-1452-JFA, 2022 WL 9874815, at *6 (E.D. Va. Aug. 22, 2022) (finding online conduct directed to a state sufficient to establish personal jurisdiction).

Defendants also used domains whose registries, VeriSign and Public Interest Registry, are located in Reston, Virginia. (ECF No 1 ¶ 17.) *See Microsoft Corp. v. Does*, No. 1:22cv607 (LMB/WEF), 2024 WL 1708328, at *5 (E.D. Va. Jan. 10, 2024) (recommending a finding that the Court had personal jurisdiction over defendants in part because the registries for their domains were in Virginia), *report and recommendation adopted*, 2024 WL 1708323 (E.D. Va. Jan. 30, 2024). Defendants thus acted with knowledge that their acts would harm Microsoft and its customers through domains maintained in this district. *See, e.g.*, *Verizon Online Servs., Inc. v. Ralsky*, 203 F. Supp. 2d 601, 610 (E.D. Va. 2002) (holding that transmitting millions of spam emails through servers located in Virginia was an act within Virginia for purposes of personal jurisdiction).

Second, Plaintiffs' claims arise out of these contacts. The phishing attacks and the domain infrastructure directed into this district are the conduct on which every count rests.

Third, exercising jurisdiction is constitutionally reasonable. Defendants chose to route their scheme through Virginia-based registries, and Virginia has a strong interest in protecting its residents from cybercrime. Plaintiffs also have no other forum for effective relief against concealed foreign defendants.

Venue is proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in this district, and a substantial part of the property at issue is located here. (ECF No. 1 ¶ 22.)

B. Service

Before entering default judgment, a court must determine that the defaulting party was properly served. Rule 4(f)(3) permits service on an individual in a foreign country "by other means not prohibited by international agreement, as the court orders." Fed. R. Civ. P. 4(f)(3). On December 12, 2024, the district judge permitted Plaintiffs to serve Defendants:

> by any means authorized by law, including (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by the Fake ONNX Defendants to their domain registrars and/or hosting companies and as agreed to by the Fake ONNX Defendants in the domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent the Fake ONNX Defendants provided accurate contact information in the U.S.; or (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon the Fake ONNX Defendants, to the extent they provided accurate contact information in foreign countries that are signatories to such treaties.

(ECF No. 31 at 9.)

Plaintiffs used the methods that order approved. In November 2024, they published notice on the Notice of Pleadings website, and in December 2024, they emailed the Complaint, Summons, Notice of Hearing, TRO, and Appendix A to the email addresses Defendant had given their registrars. (ECF No. 43 at 3–4; ECF No. 43-1 ¶¶ 13–20.)

Because Defendants concealed their identities, Plaintiff continued to give notice by email. (ECF No. 43 at 3.) On July 6, 2026, Plaintiffs sent the Complaint, Summons, Request for Entry of Default, the Court's Order Granting the Request, and the Clerk's Entry of Default to the email addresses associated with Defendants' domain names. (ECF No. 51 ¶¶ 1–2.) Defendants actively use these email addresses to operate the domain infrastructure and service their customers' accounts. (*Id.*; ECF No. 31 ¶ 13.)

Consistent with the Court's Order, Plaintiffs also published notice of the Motion on the publicly available website, https://noticeofpleadings.com/FAKEONNX/. (ECF No. 51 ¶¶ 8–9.)

On July 29, 2026, Plaintiffs emailed the Complaint, Summons, and Motion using Readnotify.com,[1] which confirmed delivery and showed that recipients opened some of the emails. (*Id.* ¶¶ 5–7.)

Defendants likely know about this case. Recipients opened the emailed papers (*id.*), and the TRO and preliminary injunction disrupted Defendants' control of their infrastructure. Plaintiffs' service was therefore "reasonably calculated . . . to apprise interested parties of the pendency of the action and afford them an opportunity to present their objections." *Mullane v. Cent. Hanover Bank & Tr. Co.*, 339 U.S. 306, 314 (1950).

Plaintiffs properly served Defendants.

C. Grounds for Entry of Default

Rule 55(a) of the Federal Rules of Civil Procedure directs the clerk to enter default when, upon a party's request, "a party against whom a judgment for affirmative relief is sought has failed to plead or otherwise defend." As noted above, Defendants' answers were due within 21 days of service, but no Defendant filed a responsive pleading, and the Clerk entered default on June 9, 2026. (ECF No. 45.)

The Clerk therefore properly entered default against Defendants.

D. Liability

Because the Clerk entered default against Defendants, the Complaint's factual allegations are deemed admitted, and the Court must determine whether they state a claim. *See* Fed. R. Civ. P. 8(b)(6) ("An allegation—other than one relating to the amount of damages—is admitted if a responsive pleading is required and the allegation is not denied."); *see also Ryan*

[1] ReadNotify is an online email and document tracking service that, among other things, notifies a sender when a tracked email message has been opened or read. *See* https://www.readnotify.com/readnotify/about.asp (last visited Oct. 17, 2026).

v. Homecomings Fin. Network, 253 F.3d 778, 780 (4th Cir. 2001); *GlobalSantaFe Corp. v. Globalsantafe.com*, 250 F. Supp. 2d 610, 612 n.3 (E.D. Va. 2003). Because Plaintiffs seek only equitable relief, the Court need not determine damages.

A default judgment also "must not differ in kind from, or exceed in amount, what is demanded in the pleadings." Fed. R. Civ. P. 54(c). Plaintiffs ask the Court to permanently enjoin Defendants from operating the Fake ONNX infrastructure[2] and to transfer ownership of the domains at issue to Microsoft. (ECF No. 47 at 2; ECF No. 54 at 7–8.) The Complaint requests the same relief. (ECF No. 1 at 49.)

1. Computer Fraud and Abuse Act, 18 U.S.C. § 1030

The CFAA, though principally a criminal statute, gives a civil cause of action to "[a]ny person who suffers damage or loss by reason of a violation." 18 U.S.C. § 1030(g). As relevant here, the CFAA penalizes a party that (1) intentionally accesses a protected computer without authorization and as a result causes damage and loss, § 1030(a)(5)(C); (2) intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains information from any protected computer, § 1030(a)(2)(C); or (3) knowingly causes the transmission of a program, information, code, or command and thereby intentionally causes damage, without authorization, to a protected computer, § 1030(a)(5)(A). A "protected computer" includes a computer "used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B); *see Estes Forwarding Worldwide LLC v. Cueller*, 239 F. Supp. 3d 918, 926 (E.D.

[2] The Fake ONNX infrastructure is "a malicious computer network infrastructure and Internet-based cybercriminal operation" that relies on a pre-packaged set of tools—including "email templates, fake website templates, domain registration services, and customer support features"—to lead Plaintiffs' customers to believe that they are interacting with Plaintiffs' legitimate products when they are actually interacting with fake products that Defendants have made to look like Plaintiffs' products. (ECF No. 54 at 4–5.)

Va. 2017). The CFAA does not define "without authorization," but the Fourth Circuit has adopted the Oxford English Dictionary's definition of "authorization" as a "formal warrant, or sanction." *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012); *see Cueller*, 239 F. Supp. 3d at 923 n.3. To "exceed[] authorized access" is to "access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). To establish a civil claim, the plaintiff must show damages aggregating at least $5,000 during a one-year period. *Id.* § 1030(c)(4)(A)(i)(I), (g). "Loss" means "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* § 1030(e)(11); *see Sprint Nextel Corp. v. Simple Cell, Inc.*, No. CIV. CCB-13-617, 2013 WL 3776933, at *6 (D. Md. July 17, 2013).

Here, Plaintiffs sufficiently allege that Defendants, as part of the phishing scheme, intentionally accessed protected computers without authorization by tricking victims into providing Defendants with login information and then using that information and the Fake ONNX infrastructure to access victims' computers and computer applications and to misappropriate confidential, sensitive, and high-value information. (ECF No. 1 ¶¶ 4–6, 31, 63, 68; ECF No. 47 at 14.) Defendants also knowingly transmitted malicious code through phishing kits that damaged those computers. (ECF No. 1 ¶¶ 6, 59-65.) Those computers are used in interstate and foreign commerce. (ECF No. 1 ¶ 65, 83.*) See e.g.*, *Global Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631, 635–37 (E.D. Va. 2009) (holding that accessing a computer using credentials that do not belong to the defendant was actionable under the CFAA)*; Facebook, Inc.*

v. Fisher, No. 09–05842 JF (PVT), 2009 WL 5095269, at *1–3 (N.D. Cal. Dec. 21, 2009) (finding a CFAA violation where defendants allegedly engaged in a phishing and spamming scheme that compromised Facebook users' accounts); *Physicians Interactive v. Lathian Sys., Inc.,* No. 03-1193-A, 2003 WL 23018270, at *5–7 (E.D. Va. Dec. 5, 2003) (finding a CFAA violation more likely than not occurred where defendant hacked into computer and stole confidential information); *Microsoft Corp. v. Doe*, No. 1:14–cv–811, 2015 WL 4937441, at *8–9 (E.D. Va. Aug. 17, 2015) (finding a CFAA violation for operating a botnet); *Microsoft Corp. v. Does 1-18*, No. 1:13cv139 (LMB/TCB), 2014 WL 1338677, at *5–6 (E.D. Va. Apr. 2, 2014) (same). Microsoft and LF Projects also allege that they have spent $650,000 and $27,000, respectively, to investigate and remediate Defendants' scheme, well above the $5,000 threshold. (ECF No. 1 at 70; ECF No. 4-3 ¶ 15.) *See Sprint Nextel Corp*., No. CCB–13–617, 2013 WL 3776933, at *7 (permitting plaintiffs to aggregate multiple intrusions or violations to satisfy the $5,000 threshold).

I therefore recommend that the district judge find that Defendants violated 18 U.S.C. § 1030(a)(2)(C), (a)(5)(A), and (a)(5)(C).

2. RICO, 18 U.S.C. § 1962(c), (d)

The RICO statute makes it unlawful for "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," or to conspire to do the same. 18 U.S.C. § 1962(c), (d). A private person may sue if "injured in his business or property by reason of a violation of section 1962 of this chapter." *Id*. § 1964(c). The plaintiff must establish (1) conduct (2) of an enterprise (3) through a pattern (4) of racketeering activity, and (5) injury to its business or property by

reason of the violation. *See Sedima, S.P.R.L. v. Imrex Co.*, 473 U.S. 479, 496 (1985) "Racketeering activity" includes any act indictable under certain listed provisions of Title 18, including § 1030(a)(5)(A), when the violation damages ten or more protected computers in a one-year period. 18 U.S.C. §§ 1961(1)(G), 2332b(g)(5)(B)(i), 1030(c)(4)(A)(i)(VI). A "pattern" requires at least two predicate acts, the last occurring within ten years after a prior act. *Id.* § 1961(5). The plaintiff must also show that the predicate acts "are related, and that they amount to or pose a threat of continued criminal activity." *H.J. Inc. v. N.W. Bell Tel. Co*., 492 U.S. 229, 239 (1989). Courts presume a threat of continuity "when the enterprise's business is primarily or inherently unlawful." *Spool v. World Child Int'l Adoption Agency*, 520 F.3d 178, 185 (2d Cir. 2008).

Plaintiffs adequately allege a RICO claim. As noted above, I recommend that the district judge find that Defendants violated the CFAA. *See supra* Part III.D.1. Those violations are predicate acts because Defendants knowingly transmitted malicious code that damaged ten or more protected computers within a one-year period. (ECF No. 1 ¶ 6, 8, 35, 60–65, 84; ECF No. 4-1 ¶ 63; ECF No. 56 at 22–23.) See 18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(A)(i)(VI), 1961(1)(G), 2332b(g)(5)(B)(i). Beginning in 2020, Defendants formed an association to develop, sell, implement, and service phishing kits and to operate a phishing infrastructure that furthered their criminal activities, including compromising email communications, financial fraud, and ransomware. (ECF No. 1 ¶¶ 83–87.) Defendants regularly accessed protected computers without authorization after a successful phishing attempt to infect targets' computers and steal personal and financial information. (*Id.*.) *See H.J. Inc.,* 492 U.S. at 242 (stating that "the threat of continuity may be established by showing that the predicate acts or offenses are part of an ongoing entity's regular way of doing business"). Each such act is related to the others, furthers

Defendants' common unlawful purpose, and will continue unless restrained. Plaintiffs have also shown significant financial injury, including about $677,000 spent investigating and remediating damage to customers' computers and Microsoft's security protocols. (ECF No. 1 ¶ 70; ECF No. 4-3 ¶ 15.)

I therefore recommend that the district judge find that Defendants violating 18 U.S.C. § 1962(c) and conspired to violate it under § 1962(d).

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

Plaintiffs next allege a violation of the ECPA, which punishes anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a); *see id.* § 2707(a) (creating a civil action). A person who logs into another's account without permission or with stolen credentials can violate the ECPA. *See, e.g.*, *McPherson v. Harker*, No. 18-cv-3082, 2021 WL 1820290, at *11 (D.D.C. May 6, 2021) (finding that a husband may have violated the ECPA when he logged into his wife's Facebook account without permission to obtain stored messages); *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 667–69 (D. N.J. 2013) (holding that Facebook "wall posts" are protected from disclosure by 18 U.S.C. § 2701).

Plaintiffs allege that their computer system is a facility through which an electronic communication service is provided to users and customers. (ECF No. 1 ¶ 97.) They further allege that Defendants knowingly and intentionally accessed Plaintiffs' operating system, software, services, and computers and Plaintiffs' customers' computers without authorization (or at least in excess of any authorization) to acquire sensitive documents and personal information stored there. (*Id*. at ¶¶ 2, 98–99.) Courts in this district have found that obtaining stored electronic

information this way violates the ECPA. *See State Analysis, Inc. v. Am. Fin. Svs. Assoc'n*, 621 F. Supp. 2d 309, 317–18 (E.D. Va. 2009) (finding a violation of the ECPA when the defendant intentionally accessed a password-protected area of the plaintiff's website without authorization to use the database).

I therefore recommend that the district judge find that Defendants violated the ECPA.

4. Lanham Act, 15 U.S.C. §§ 1114, 1125(a), and 1125(c)

Plaintiffs also allege that Defendants are liable under the Lanham Act, 15 U.S.C. § 1051 *et seq*., for (1) trademark infringement, 15 U.S.C. § 1114; (2) false designation of origin, *id.* § 1125(a); and (3) trademark dilution, *id.* § 1125(c).

For trademark infringement, the Lanham Act imposes liability on anyone who, without the registrant's consent, uses a colorable imitation of a registered mark in connection with the distribution of goods or services when such use is likely to cause confusion or to deceive. 15 U.S.C. § 1114(1). A plaintiff must show: (1) that it owns a valid mark; (2) that the defendant used the mark in commerce without authorization; (3) that the defendant used the mark, or an imitation of the mark, in connection with the sale, offering for sale, distribution, or advertising of goods and services; and (4) that the defendant's use is likely to confuse consumers. *Rosetta Stone Ltd. v. Google, Inc.*, 676 F.3d 144, 152 (4th Cir. 2012).

Here, the well-pleaded facts establish that Defendants used and distributed electronic copies of Plaintiffs' federally registered trademarks in interstate commerce, including LF Projects' ONNX Mark and the Microsoft Marks (ECF No. 1-1, 1-6), in connection with fraudulent schemes designed to lure victims into clicking links to malicious websites or otherwise interacting with them. (ECF No. 1 ¶¶ 2–3, 30, 72, 110.) Defendants use Plaintiffs' Marks in domain names and websites and cause consumers to use adulterated products that bear

Plaintiffs' registered trademarks. (*Id*. ¶¶ 7, 44.) Defendants also use Microsoft and Azure-based services to host the malicious content and rely on the Microsoft and ONNX brands to perpetrate their phishing and malware attacks. (*Id*. ¶ 33, 60, 68.) This conduct deceives victims and causes confusion, mistake, or deception as to the origin, sponsorship, or approval of the fraudulent domains and accompanying links, products, and malware. (*Id*. ¶ 35.) Plaintiffs have therefore stated a claim for trademark infringement under § 1114.

The Lanham Act also prohibits using a trademark, a false designation of origin, or a false or misleading representation of fact that is likely to cause confusion as to the origin, sponsorship, or approval of goods or services. 15 U.S.C. § 1125(a)(1)(A). The claim has three elements: "(1) the alleged violator must employ a false designation; (2) the false designation must deceive as to origin, ownership or sponsorship; and (3) the plaintiff must believe that 'he or she is or is likely to be damaged by such [an] act.'" *Am. Online, Inc. v. IMS*, 24 F. Supp. 2d 548, 551 (E.D. Va. 1998) (quoting 15 U.S.C. § 1125(a)(1)) (holding that a spam email with a fake sender address showing plaintiff's trademarks constituted false designation of origin).

Plaintiffs' Marks are widely recognized within their trades. (ECF No. 1 at 7, 9–10, 23–24.) Defendants falsely associated Plaintiffs' trademarks with malicious conduct carried out on victims' computers. (*Id.* at 7, 23 69.) *See, e.g.*, *Hotmail Corp. v. Van$ Money Pie Inc*., No. C 98-20064 JW, 1998 WL 388389, at *5 (N.D. Cal. Apr. 16, 1998) (finding that the defendant's "falsification of e-mail return addresses" and "fraudulent creation of Hotmail mailboxes" made plaintiff likely to succeed on the merits of its false designation of origin claim). That conduct caused confusion about Plaintiffs' roles in the phishing scheme. Victims could reasonably have associated Microsoft or LF Projects with Defendants' scheme or believed that Microsoft was the source of the computer intrusions and theft. Plaintiffs suffered damage to their reputations,

brands, and goodwill as a result. Plaintiffs have therefore stated a claim for false designation or origin under § 1125(a).

Finally, the Lanham Act entitles the owner of a famous mark "to an injunction against another person" who uses the mark in a way "that is likely to cause dilution by blurring or dilution by tarnishment of the famous mark." 15 U.S.C. § 1125(c)(1). "A dilution claim is made out by showing: (1) the ownership of a distinctive mark; and (2) a likelihood of dilution." *IMS*, 24 F. Supp. 2d at 552. A mark is famous when it is "widely recognized by the general consuming public of the United States as a designation of source of the goods or services of the mark's owner," 15 U.S.C. § 1125(c)(2)(A), and a mark is tarnished when it is portrayed in an unwholesome or unsavory context, *see id.* § 1125(c)(2)C); *Hormel Foods Corp. v. Jim Henson Prods., Inc*., 73 F.3d 497, 507 (2d Cir. 1996).

The record establishes that Plaintiffs own registered trademarks. *See Am. Online, Inc. v. AT&T Corp.*, 243 F.3d 812, 816 (4th Cir. 2001) (holding that registering a mark on the United States Patent and Trademark Office's Principal Register is *prima facie* evidence that the mark is distinctive and has secondary meaning). The MICROSOFT, WINDOWS, OUTLOOK, and OFFICE Marks are also famous. Microsoft has used them in commerce for decades, advertised them nationwide, and sold products under them to a large share of American consumers. (ECF No. 1 ¶ 23.) *See* 15 U.S.C. § 1125(c)(2)(A)(i)–(iv). Defendants' misuse of those Marks to further their scheme dilutes them by tarnishment and by blurring of consumer associations with the Marks. *See, e.g.*, *IMS*, 24 F. Supp. 2d at 552 ("The sine qua non of tarnishment is a finding that plaintiff's mark will suffer negative associations through defendant's use.") (quoting *Hormel Foods Corp.*, 73 F.3d at 507).

I therefore recommend that the district judge find that Defendants violated 15 U.S.C. §§ 1114, 1125(a), and that they violated 1125(c) as to the MICROSOFT, WINDOWS, OUTLOOK, and OFFICE Marks.

5. Common Law Claims

Plaintiffs also assert Virginia claims for trespass to chattels, conversion, and unjust enrichment (Counts VIII–X).

a. Trespass to Chattels

"Under Virginia law, '[a] trespass to chattels occurs "when one party intentionally uses or intermeddles with personal property in rightful possession of another without authorization," . . . and "if the chattel is impaired as to its condition, quality, or value."'" *AMF Bowling Ctrs., Inc. v. Tanase*, No. 3:23-cv-448–HEH, 2024 WL 2978775, at *9 (E.D. Va. June 13, 2024) (quoting *State Analysis*, 621 F. Supp. 2d at 320). "The unauthorized intrusion into an individual's computer system through hacking, malware, or even unwanted communications supports actions under [a trespass to chattels claim]." *Id.* (quoting *Microsoft Corp.*, 2014 WL 1338677, at *9). Here, Defendants intentionally accessed Plaintiffs' operating system without permission and interfered with Plaintiffs' possession of their software. (ECF No. 1 ¶¶ 62–63, 68, 98–99.) The intrusions impaired the value of that software by compromising its security and requiring Plaintiffs to spend substantial sums to remediate it. (*Id.* ¶ 7, 70; ECF No. 4-3 ¶ 8, 15.) Microsoft alleges that Defendants have irreparably harmed the value of Microsoft's software by confusing Microsoft customers into compromising their own personal and business information—and thus diluted and tarnished the value of Microsoft's trademarks and brands. (ECF No. 1 ¶ 69.) And LF Projects alleges that Defendants have irreparably harmed LF Projects' goodwill by leading customers to believe that the Defendants' actions are attributable to LF Projects' legitimate

ONNX Exchange. (*Id.* ¶ 72–75; ECF No. 4-3 ¶ 8–13.) These allegations show that Defendants committed trespass to chattels. *See Microsoft Corp.*, 2014 WL 1338677, at *10 (finding that Microsoft adequately alleged trespass to chattels when it claimed that the defendants "accessed computers and servers associated with Microsoft's Internet Explorer . . . without authorization" and engaged in "click-fraud" by directing search results "to websites of defendant's choice").

b. Conversion

Plaintiffs also assert conversion. Conversion is "any wrongful exercise or assumption of authority . . . over another's goods, depriving [them] of their possession; [and any] act of dominion wrongfully exerted over property in denial of the owner's right, or inconsistent with it." *United Leasing Corp. v. Thrift Ins. Corp.*, 247 Va. 299, 305 (1994) (quoting *Universal C.I.T. Credit Corp. v. Kaplan*, 198 Va. 67, 75 (1956)). Defendants intentionally and without authorization deprived Plaintiffs of control over their software and services. (ECF No. 1 ¶¶ 62–63, 98–99.) Defendants' phishing kits "are specifically developed to target Microsoft 365 and Azure users" and "Defendants advertise[] the kits' abilities to break into Microsoft systems." (*Id.* ¶ 31.) Plaintiffs have therefore stated a claim for conversion. See, e.g., *Microsoft Corp.*, 2014 WL 1338677, at *10 (finding that Microsoft's allegations were sufficient to "show[] that defendant committed conversion" where it alleged that the defendant "converted Microsoft's property in a way that allowed defendant to control Microsoft software, servers, and search engines").

c. Unjust Enrichment

The elements of unjust enrichment are "(1) A benefit conferred on the defendant by the plaintiff; (2) Knowledge on the part of the defendant of the conferring of the benefit; and (3) Acceptance or retention of the benefit by the defendant in circumstances that render it

inequitable for the defendant to retain the benefit without paying for its value." *Nossen v. Hoy*, 750 F. Supp. 740, 744–45 (E.D. Va. 1990) (applying Virginia law). Here, Defendants knowingly and without authorization obtained a benefit from Microsoft's servers, email services, and operating systems by collecting sensitive information through them. (ECF No. 1 ¶¶ 62–68, 98–99.) Defendants profited unjustly from their use of Microsoft's software and other services because that use was unauthorized and depended on infecting the computers of Plaintiffs' customers with malware. (*Id.*) Defendants knew of the benefit because they initiated the unauthorized use. Although Plaintiffs did not confer this benefit voluntarily, Defendants took it from Plaintiffs' property, and the doctrine does not reward a defendant for taking what the plaintiff would not have given. It would be inequitable for Defendants to retain that benefit. *See Nossen*, 750 F. Supp. 740 at 745.

I therefore recommend that the district judge find that Defendants committed trespass to chattels and conversion and were unjustly enriched.

E. Relief

Plaintiffs seek "two forms of relief: default judgment and a permanent injunction whereby (1) the Fake ONNX Defendants are enjoined and prohibited from operating or propagating the Fake ONNX infrastructure; and (2) ownership of the Fake ONNX domains is permanently transferred to Microsoft." (ECF No. 54 at 7–8.)

1. Permanent Injunction

The CFAA authorizes injunctive and other equitable relief. 18 U.S.C. § 1030(g); *see also* 15 U.S.C. § 1116(a) (Lanham Act). A plaintiff seeking a permanent injunction must show (1) that it has suffered an irreparable injury; (2) that remedies at law are inadequate to compensate for that injury; (3) that the balance of hardships favors the plaintiff; and (4) that the public

interest would not be disserved by an injunction. *See eBay Inc. v. MercExchange, LLC*, 547 U.S. 388, 391 (2006); *see also EMI April Music, Inc. v. White*, 618 F. Supp. 2d 497, 509 (E.D. Va. 2009).

First, Plaintiffs have suffered irreparable injury from customer confusion and from Defendants' use of Plaintiffs' trademarks and other branding to run their phishing operation, which harmed Plaintiffs' business goodwill. (ECF No. 1 ¶¶ 7, 69, 74.) The Fourth Circuit has held that irreparable harm exists when a defendant misleads a company's customers and damages its reputation and goodwill. *See PBM Prods., LLC v. Mead Johnson & Co.*, 639 F.3d 111, 127 (4th Cir. 2011).

Because Defendants could continue to confuse Plaintiffs' customers and misuse Plaintiffs' trademarks, Plaintiffs will keep suffering irreparable injury without a permanent injunction. (ECF No. 1 ¶¶ 8, 62, 77.) Courts have repeatedly found that malware operations exploiting Microsoft's trademarks cause irreparable harm. *See Microsoft Corp. v. Does*, 2024 WL 1708328, at *11 (collecting cases).

Second, remedies at law would be inadequate: money damages would leave Defendants free to continue using the infrastructure they developed to harm Plaintiffs. (ECF No. 1 ¶ 8, 81, 101.) Despite due diligence, Plaintiffs have been unable to confirm the identities of the four John Does, and the only known defendant—Abanoub Nady—lives in Egypt. (*Id.* ¶ 11–16.) Any monetary award would be difficult, if not impossible, to enforce.

Third, the balance of hardships favors Plaintiffs. Plaintiffs seek only to halt Defendants' illegal activity, and nothing in the record suggests that Defendants' activities are anything but illegal. *See PBM Prods.*, 639 F.3d at 127 (explaining that a defendant had "no equitable interest

in perpetuating [] false and misleading claims") (quoting *PBM Prods., LLC v. Mead Johnson & Co.*, No. 3:09-CV-269, 2010 WL 957756, at *3 (E.D. Va. Mar. 12, 2010)).

Fourth, a permanent injunction would serve the public interest. Defendants manufacture, sell, and help deploy phishing tools that can bypass Microsoft security measures, establish a permanent presence in a victim's computer system, intercept communications, and steal personal and business information. (ECF No. 1 ¶¶ 2–3, 6–7.) A permanent injunction would help prevent phishing and ransomware attacks and thus benefit the public. (*Id*. ¶ 8.) Enforcing statutes designed to protect the public, such as the Lanham Act and the CFAA, also favors enjoining false or misleading representations and the profits they generate. *See Microsoft Corp.*, 2024 WL 1708328, at *12.

I therefore recommend that the district judge enter a permanent injunction that prohibits Defendants, and those acting in concert with them who receive actual notice of the order, from (1) operating, controlling, or propagating the Fake ONNX infrastructure, including the domains listed in Appendix A to the Complaint; (2) using the ONNX Mark or the Microsoft Marks in connection with any phishing kit, domain, website, or email; and (3) accessing, without authorization, computers belonging to Microsoft or its customers, or transmitting malicious code to them. See Fed. R. Civ. P. 65(d)(1)–(2).

2. Transfer of the Fake ONNX Domains

Plaintiffs also ask the Court to transfer the Fake ONNX domains to Microsoft. (ECF No. 54 at 7–8.) The Court's equitable authority supports that relief. The Lanham Act authorizes injunctions "according to the principles of equity and upon such terms as the court may deem reasonable," 15 U.S.C. § 1116(a), and the CFAA authorizes "injunctive relief or other equitable relief," 18 U.S.C. § 1030(g).

Transfer is the only effective way to keep Defendants from reviving the scheme. An injunction alone would leave the domains with concealed foreign operators who have ignored this action. The registries for the domains, VeriSign and Public Interest Registry, are in this district (ECF No. 1 ¶ 17), and they can permanently carry out the transfer as they did during the pendency of this action as required under the preliminary injunction. (ECF No. 31 at 9.) Courts in this district have granted the same relief in similar Microsoft actions. *See Microsoft Corp.*, 2015 WL 4937441, at *2; *Microsoft Corp.*, 2024 WL 1708328, at *12 *report and recommendation adopted*, 2024 WL 1708323 (E.D. Va. Jan. 30, 2024).

I therefore recommend that the district judge order the Fake ONNX domains listed in Appendix A to the Complaint transferred to Microsoft, and direct the registries to cooperate in that transfer.

IV. Recommendation

I recommend that the district judge enter default judgment for Plaintiffs and against Defendants on all counts: the CFAA, 18 U.S.C. § 1030; RICO, 18 U.S.C. §§ 1962(c), (d); the ECPA, 18 U.S.C. § 2701; the Lanham Act, 15 U.S.C. §§ 1114, 1125(a), and § 1125(c) as to the MICROSOFT, WINDOWS, OUTLOOK, and OFFICE Marks; and Virginia common-law trespass to chattels, conversion, and unjust enrichment. I also recommend that the district judge permanently enjoin Defendants from the conduct described in Part III.E.1. Finally, I recommend that the district judge transfer ownership of the Fake ONNX domains listed in Appendix A to the Complaint to Microsoft. (ECF No. 1 App'x A-2.)

V. Notice

The Court will serve this Report and Recommendation on all parties through its electronic filing system. Plaintiffs must also send a copy to Defendants in the same manner they

served Defendants (ECF No. 27) and must certify compliance to the Court within three days of service.

Any party may object to this Report and Recommendation within 14 days of service. *See* 28 U.S.C. § 636(b)(1); Fed. R. Civ. P. 72(b)(2). Failure to file timely objections waives appellate review of both the substance of this Report and Recommendation and any judgment entered on it. *See Thomas v. Arn*, 474 U.S. 140, 155 (1985).

Entered this 13th day of November 2026.



William B. Porter
United States Magistrate Judge

Alexandria, Virginia