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

Microsoft Corporation, a Washington State Corporation and LF Projects, LLC, a Delaware State Series Limited Liability Company, Plaintiffs, v. Abanoub Nady (also known as MRxC0DER), and John Does 1-4, Controlling A Computer Network and Thereby Injuring Plaintiffs and Its Customers, Defendants.	Civil Action No.: 1:24-cv-2013-RDA

PLAINTIFFS' BRIEF IN SUPPORT OF MOTION FOR DEFAULT JUDGMENT AND PERMANENT INJUNCTION

Plaintiffs Microsoft Corp. ("Microsoft") and LF Projects, LLC (collectively, "Plaintiffs") seek a default judgment and permanent injunction to prevent Defendants Abanoub Nady (also known as MrXC0DER) and John Does 1-4 (collectively, the "Fake ONNX Defendants" and formerly known as "Caffeine") from continuing to operate the malicious computer network infrastructure and Internet-based cybercriminal operation known as "Fake ONNX."

As set forth in Plaintiffs' pleadings and the Court's previous orders, Defendants manufacture and sell phishing kits deceptively branded as "ONNX" 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 also referred to as "Phishing-as-a-Service" or "PhaaS." The Fake ONNX Defendants sell these PhaaS kits to downstream cybercriminals who set up their own internet domains to perpetrate phishing attacks and add their domains to the Fake ONNX

infrastructure. This results in a vast infrastructure overseen and administered by the Fake ONNX Defendants comprised of hundreds of domains that launch phishing attacks against Microsoft and its customers.

Each time a phishing kit is sold, it is done with the express purpose of attempting to infiltrate Microsoft systems.[1] Fake ONNX Defendants use Microsoft's logos in their phishing emails, such as Outlook and Microsoft 365 to further enhance the perceived legitimacy of the attack. In doing so, Fake ONNX Defendants capitalize on and misuse the brand recognition that Microsoft has cultivated, and the trust Microsoft has built with its customers. Further, Fake ONNX Defendants have stolen and misused the trademarks and logo of a legitimate and unrelated brand known as ONNX that is owned by Plaintiff LF Projects. Defendants illegally and without authorization use the ONNX marks and logo to traffic their phishing kits.

Prior to issuance of this Court's Temporary Restraining Order and Preliminary Injunction and Supplemental Preliminary Injunction, Fake ONNX Defendants used these domains to facilitate their cybercriminal activity. Plaintiffs now seek to bring this case to final conclusion by way of a permanent injunction that will prevent Fake ONNX Defendants from continuing to carryout out the Fake ONNX operation or retaking control of the infrastructure through the abuse of Plaintiffs' trademarks and brands.

Plaintiffs request a permanent injunction (1) prohibiting Defendants from operating or propagating the Fake ONNX infrastructure; and (2) permanently transferring ownership to Microsoft of known malicious Fake ONNX domains identified in the Court's prior injunction order (and identified in Appendix A to the Proposed Order). This injunctive relief is required to

[1] A selling/advertising point of the Fake ONNX-branded phishing kit is Defendants' claim the tool can circumvent Microsoft security. They cannot do so. In reality, the phishing kits rely on social engineering and deception to trick users into sharing credentials thus bypassing Microsoft security measures and entering a victim's network as though they were an authorized user.

prevent further harm to Microsoft, its customers, LF Projects, and the general public should Defendants continue to use the Fake ONNX domains and Plaintiffs' trademarks and brands to conduct their cybercriminal activity.

A permanent injunction is the only way to afford relief and abate future harm in this case. This is particularly the case, given that, in the absence of such relief, the existing domains would revert to Fake ONNX Defendants and Fake ONNX Defendants would certainly register new domains to support their phishing-as-a-service operation and the selling of their phishing kits.

Fake ONNX Defendants were properly served with Plaintiffs' complaint and other pleadings in this action and were provided with adequate notice of this action through means authorized by law, satisfying Due Process and Fed. R. Civ. P. 4, and reasonably calculated to provide Defendants with notice. Plaintiffs served Defendants Fake ONNX Defendants on December 1, 2024 and thereafter, by email and publication at the website https://noticeofpleadings.com/FAKEONNX/, and more than 21 days have elapsed since Plaintiffs effected service. The Clerk was directed to enter default pursuant to Fed. R. Civ. P. 55(a) against Nady and Joun Does 1-4 for failing to appear after being properly provided notice of the proceedings under Fed. R. Civ. P. 4(f)(3) on June 8, 2026 and did so on June 9. 2026. *See* Dkt. Nos. 44, 45. The factual allegations in the Complaint and the record in the case establish the elements of each of Plaintiffs' claims and also establish the need for the requested injunctive relief.

I. FACTUAL BACKGROUND

A. Overview of Fake ONNX Defendants

The Fake ONNX Defendants manufacture, sell, and facilitate the deployment of pre-packaged sets of tools ("phishing kits") that enable other cybercriminals to launch phishing

attacks with relative ease. This business model of selling phishing kits and services for use by other cybercriminals is also referred to as "Phishing-as-a-Service" or "PhaaS." Declaration of Jason B. Lyons ISO *Ex Parte* Application for TRO, Dkt. No. 15 ("Lyon Decl.") ¶ 8. These phishing kits include email templates, fake website templates, domain registration services, and customer support features designed to evade detection and lead victims to believe they are dealing with legitimate products. *Id.* The kits are essentially "how to" manuals for cybercriminals to develop and execute attacks on email systems through phishing campaigns. This action brought by Microsoft and LF Projects focuses on the ONNX-branded phishing kits that are used to target Microsoft's systems, products, and users. *Id.*

These phishing kits are particularly pernicious as they facilitate "adversary in the middle" ("AiTM") attacks whereby the attacker establishes a permanent presence in a victim's system with the ability to intercept communications and affirmatively circumvent the security features of Microsoft products to deceive victims into thinking that the email communication they receive, the files they are directed to open, or the links to websites used to enter their personal credentials are authentic and Microsoft-approved. *Id.* ¶ 9.

B. The Court's Injunction

On November 13, 2024, the Court entered a Temporary Restraining Order ("TRO") that disabled much of the Defendants' technical infrastructure. Dkt. No. 16.

To disable Fake ONNX's infrastructure, this Court ordered that these Fake ONNX-controlled Internet domains be redirected to secure Microsoft servers. *Id.* On December 12, the Court subsequently entered an order granting a Preliminary Injunction to ensure that Defendants' infrastructure cannot cause further harm. Dkt. No. 31.

In executing the Court's Temporary Restraining Order and Preliminary Injunction Order, Microsoft was able to cut communications between Defendants' existing infrastructure and the victim computers and networks that Defendants attacked and from which Defendants had been stealing information. This effectively stymied Defendants' efforts to exploit the computers and networks they had targeted or already broken into. In connection with the TRO and Preliminary Injunction Order, 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 have continued to use domains identified by Plaintiffs throughout this case to control the Fake ONNX infrastructure;
- Defendants have used and continue to use domains containing Plaintiffs' trademarks and brands to deceive victims and control the Fake ONNX infrastructure;
- Defendants' activities concerning the domains has violated or is likely to violate the Computer Fraud and Abuse Act (18 U.S.C. § 1020), the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. §§ 1962, 1962(d), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), and the common law doctrines of trespass to chattels, unjust enrichment, and conversion;
- Unless enjoined, Defendants are likely to continue to engage in conduct that violates the Computer Fraud and Abuse Act (18 U.S.C. § 1020), the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. §§ 1962, 1962(d)), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), and the common law doctrines of trespass to chattels, unjust enrichment, and conversion;
- Defendants have received notice of the injunction and, despite that fact, have continued to and are likely to continue to register and use domains containing Plaintiffs' trademarks and brands to deceive victims and control the Fake ONNX infrastructure; and
- Defendants' conduct causes irreparable harm and such irreparable harm will continue unless the domains used by Defendants are disabled.

See Dkt. No. 16 at 2-3; Dkt, No. 31 at 2-3.

C. Plaintiffs' Discovery Efforts

Following the Order authorizing limited discovery, Plaintiffs served subpoenas on Internet service providers ("ISPs"), domain registrars, and hosting companies seeking account information, identifying information, payment information, device information, and communications with the account holders in an effort to obtain additional information regarding the Fake ONNX Defendants' identities. Declaration of Anna Z. Saber ISO Request for Entry of Default. Dkt No. 43-1 ("06/04/26 Saber Decl.") ¶ 23.

However, given (a) Defendants' use of aliases and false information, (b) use of anonymous proxy computers or anonymization networks to create and maintain the infrastructure at issue in the case, (c) the absence of or limitations on the ability to carry out U.S.-style civil discovery outside of the U.S., (d) the ease with which anonymous activities can be carried out through the Internet, and (e) the sophistication of the Defendants in using tools to conceal more specific indicia of their identities or further contact information, Plaintiffs were unable to specifically and definitively determine the "real" names and physical addresses of Defendants. *Id.* ¶ 24.

Plaintiffs have exhausted their ability to investigate Defendants' true identities using civil discovery tools, despite their best efforts and the exercise of reasonable diligence to determine Defendants' identities. *Id.* ¶ 25.

D. Service of Process on Defendants

When the Court issued the TRO and Preliminary Injunction, the Court found good cause to permit service of Plaintiffs' Complaint and related materials by alternative means pursuant to Rule 4(f)(3). Dkt. No. 16 at 10; Dkt. No. 31 at 9. The Court has directed that, under the circumstances, appropriate means of service sufficient to satisfy Due Process include emails to

email accounts associated with Defendants and publication on a publicly available Internet website. *Id.* Both have been done in this case.

The Court authorized service by email and publication on November 13, 2024. Dkt. No. 16 at 10. On December 1, 2024, Plaintiffs served copies of the Complaint, TRO, Preliminary Injunction Order, and all other pleadings, declarations, evidence, orders, and other submissions in this action, by attaching those documents to the emails sent to the email addresses associated with the domain names used by the Fake ONNX Defendants (the email addresses listed as "registrant emails" on Appendix A to the Complaint, Dkt. No. 1-1). 06/04/26 Saber Decl. ¶¶ 4, 13-24. Plaintiffs used an email tracking service to monitor whether service emails were received and opened. *Id.* ¶ 15. The service of process emails were repeatedly opened and viewed by the Fake ONNX Defendants between December 1, 2024 and the present. *Id*. Plaintiffs also provided notice of this action by publication beginning on November 21, 2024 at the website https://noticeofpleadings.com/FAKEONNX/. *Id.* ¶¶ 17-21.

The time for the Fake ONNX Defendants to answer or respond to the complaint expired on December 23, 2024 (22 days after email service, effected on December 1, 2024).[2] 06/04/26 Saber Decl. ¶ 4. The Fake ONNX Defendants have not contacted Microsoft or counsel about this case. *Id.* ¶¶ 8, 16. Nor have the Fake ONNX Defendants appeared in this case or responded in any way to the Complaint. *Id.* ¶ 4. To the best of Plaintiffs' information and belief, no Defendant is a minor or incompetent person, or unable to respond due to absence caused by military service. *Id.* ¶ 5. The Clerk was directed to enter default pursuant to Fed. R. Civ. P. 55(a) against Abanoub Nady and John Does 1-4 for failing to appear after being properly provided notice of the proceedings under Fed. R. Civ. P. 4(f)(3) on Jube 8, 2026, and did so on June 9, 2026. *See* Dkt.

[2] The service email was sent on a Sunday. Accordingly, Plaintiffs have added 22 days to the service date to calculate the time to respond.

Nos. 44, 45.

III. LEGAL STANDARD

Rule 55 of the Federal Rules of Civil Procedure provides that the clerk of the court must enter a party's default "[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." Fed. R. Civ. P. 55(a). The Clerk's interlocutory "entry of default" pursuant to Federal Rule of Civil Procedure 55(a) provides notice to the defaulting party prior to the entry of default judgment by the court. In turn, Federal Rule of Civil Procedure 55(b)(2) "authorizes courts to enter a default judgment against a properly served defendant who fails to file a timely responsive pleading." *LPS Default Solutions, Inc. v. Friedman & MacFadyen, P.A.*, 2013 U.S. Dist. LEXIS 108486, at *2-3 (D. Md. Aug. 2, 2013). Default judgment is appropriate when the adversary process has been halted because of an unresponsive party. *SEC v. Lawbaugh*, 359 F. Supp. 2d 418, 421-22 (D. Md. 2005) (default judgment "clearly appropriate" where defendants were not responsive for over a year).

Upon default, the well-pled allegations in a complaint as to liability are taken as true. *Id.* Here, the Clerk has entered Defendants' default under Rule 55(a) (Dkt. No. 44), and Defendants have received notice of same.[3]

In reviewing motions for default judgment, courts have referred to the following factors: (1) the amount of money involved in the litigation; (2) whether there are material issues of fact in the case needing resolution; (3) whether the case involves issues of great public importance; (4) whether the grounds for the motion for a default judgment are highly technical; (5) whether the party asking for a default judgment has been prejudiced by the non-moving party's actions or

[3] In connection with the Order Granting Plaintiffs' Request for Entry of Default, the Court direct Plaintiffs to serve notice via email service and publication. Plaintiffs have complied with this

omissions; (6) whether the actions or omissions giving rise to the motion for a default judgment are the result of a good-faith mistake on the part of the non-moving party; (7) whether the actions or omissions giving rise to the motion for a default judgment are the result of excusable neglect on the part of the non-moving party; and (8) whether the grounds offered for the entry of a default judgment are clearly established. *Tweedy*, 611 F. Supp. 2d at 605-606 (citing *Faulknier v. Heritage Financial Corp.*, 1991 U.S. Dist. LEXIS 15748 (W.D. Va. May 20, 1991)) and 10 C. Wright, A. Miller & M. Kane, Federal Practice and Procedure §§ 2684-85 (1990)).

Courts may also order permanent injunctive relief in conjunction with default judgments. *E.g.*, *Trs. of the Nat'l Asbestos Workers Pension Fund v. Ideal Insulation, Inc.*, 2011 U.S. Dist. LEXIS 124337, at *12 (D. Md. Oct. 27, 2011) (collecting cases). 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 America Online v. IMS*, 1998 U.S. Dist. LEXIS 20645 (E.D. Va. Dec. 30, 1998); *Microsoft Corp. v. Doe*, 2015 U.S. Dist. LEXIS 109729 (E.D. Va. Aug. 17, 2015); *Microsoft Corp. v. Doe*, 2015 U.S. Dist. LEXIS 110145 (E.D. Va. July 20, 2015) (Report and Recommendation); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 46951 (E.D. Va. Apr. 2, 2014); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398 (E.D. Va. Jan. 6, 2014) (Report and Recommendation); *see also Microsoft Corp. v. Does*, 2013 U.S. Dist. LEXIS 168237 (W.D.N.C. Nov. 21, 2013).

IV. ARGUMENT

A. Due Process Has Been Satisfied

Plaintiffs have served the complaint and other pleadings in this action on Defendants using the methods ordered by the Court under Rule 4(f)(3), including service by email and publication. It is well settled that legal notice and service by email, facsimile, mail and

---

directive.

publication satisfies Due Process where these means are reasonably calculated, in light of the circumstances, to put defendants on notice. *See, e.g.*, *FMAC Loan Receivables v. Dagra*, 228 F.R.D. 531, 534 (E.D. Va. 2005) (acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means, including email); *Mullane v. Central Hanover Bank & Trust Co.*, 339 U.S. 306, 314 (1950) (discussing Due Process requirements). Email service and Internet publication are particularly appropriate here given the nature of Defendants' conduct and use of email as the primary means of communication in connection with establishing and managing the IP addresses and domains used to operate the Fake ONNX domains and infrastructure. *FMAC Loan Receivables*, 228 F.R.D. at 534; *Rio Props., Inc. v. Rio Int'l Interlink*, 284 F.3d 1007, 1014-15 (9th Cir. 2002) ("[Defendant] had neither an office nor a door; it had only a computer terminal. If any method of communication is reasonably calculated to provide [Defendant] with notice, surely it is email…"); *BP Prods. N. Am., Inc. v. Dagra*, 236 F.R.D. 270, 271-273 (E.D. Va. 2005) (approving notice by publication in two Pakistani newspapers circulated in the defendant's last-known location); *Microsoft Corp. v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va. 2010) at Dkt. No. 38 at 4 (authorizing service by email and publication in similar action).

In this case, the email addresses provided by Defendants to the domain registrars in the course of obtaining services that support Defendants' Fake ONNX infrastructure are the most accurate and viable contact information and means of notice and service. Indeed, the physical addresses provided by Defendants to domain registrars and other service providers are false and Defendants' whereabouts are unknown, and are not ascertainable despite the exercise of diligent formal and informal attempts to identify Defendants, which further supports service by email and publication. *FMAC Loan Receivables v. Dagra,* 228 F.R.D. 531, 535-36 (E.D. Va. 2005)

(following *Rio Properties* and acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means); *BP Products N. Am., Inc. v Dagra*, 236 F.R.D. 270, 271-73 (E.D. Va. 2006) (approving notice by publication); *AllscriptsMisys, LLC v. Am. Dig. Networks*, LLC, 2010 U.S. Dist. LEXIS 4450, at *3 (D. Md. 2010) (granting *ex parte* TRO and order prompting "notice of this Order and Temporary Restraining Order [] can be effected by telephone, electronic means, mail or delivery services.").

Moreover, Defendants will expect notice regarding their use of the domain registrars' services to operate their Fake ONNX infrastructure by email, as Defendants agreed to such in their agreements with the service providers who provided the domains for Defendants' use. *See Nat'l Equip. Rental, Ltd. v. Szukhent,* 375 U.S. 311 (1964) ("And it is settled … that parties to a contract may agree in advance to submit to the jurisdiction of a given court, to permit notice to be served by the opposing party, or even to waive notice altogether.").

Given the circumstances and Plaintiffs' diligent efforts to locate Defendants, Due Process has been satisfied by Plaintiffs' service by publication and multiple email notices.

B. Default Judgment is Appropriate

All of the relevant considerations point towards issuance of a default judgment against Defendants. First, the amount of money at stake weighs in favor of default judgment because Plaintiffs are not requesting any monetary relief, and indeed it is not possible for Plaintiffs to obtain any meaningful monetary relief under the circumstances. Accordingly, default judgment poses no risk of undue cost, prejudice, or surprise to Defendants.

Second, there are no material facts in dispute. Plaintiffs have put forth a strong factual showing supported by forensic evidence and documentary evidence from researchers who have studied the Fake ONNX infrastructure and its impact on victims. The allegations and evidence in

the detailed Complaint and otherwise in the record establish that Defendants' conduct in operating the Fake ONNX infrastructure violated and is likely in the future to violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030); Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. §§ 1962, 1962(d)); Electronic Communications Privacy Act (18 U.S.C. § 2701); False Designation of Origin, Trademark Infringement, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114, et seq.); and the common law claims of trespass to chattels, conversion, and unjust enrichment.

Third, this case involves a matter of substantial public importance. Defendants are perpetrating serious offenses and civil torts that cause substantial harm to hundreds if not thousands of victims. In addition to the general public interest in abating such harm, the public also has a strong interest in the integrity and enforcement of federal laws designed to deter cybercrime and enhance data security.

Fourth, default here is not merely technical. This is not a situation where Defendants have accidentally missed a deadline by a few days; nor is default the result of a good faith mistake or excusable neglect. Rather, Defendants have affirmatively chosen not to appear and defend this action, despite ample notice and opportunity to do so. Plaintiffs have made extraordinary efforts over the course of many months to ensure that Defendants were provided notice, and the evidence indicates that Defendants are actually aware of this action but affirmatively chose not to appear.

Fifth, Plaintiffs and other victims of the Fake ONNX infrastructure have been prejudiced by Defendants' actions and omissions. Defendants have refused to make their identities known and have refused to participate in this lawsuit. Defendants' disregard for this Court's process and refusal to communicate have caused Plaintiffs to incur significant expense.

Each of the factors weigh in favor of entering default judgment. The grounds offered for the entry of a default judgment are clearly established.

C. Plaintiffs Have Adequately Plead Each of its Claims

The Complaint alleges that Defendants have violated the Computer Fraud and Abuse Act (18 U.S.C. § 1030); Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. §§ 1962, 1962(d)); Electronic Communications Privacy Act (18 U.S.C. § 2701); False Designation of Origin, Trademark Infringement, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114, *et seq.*); and the common law claims of trespass to chattels, conversion, and unjust enrichment. Each of these claims is adequately pled.

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 "used in or affecting interstate or foreign commerce or communication." 18 U.S.C. 1030(e)(1); *see also See Estes Forwarding Worldwide LLC v. Cuellar*, 239 F. Supp. 3d 918, 926 (E.D. Va. 2017). "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.* at 923 (citing 18 U.S.C. § 1030(e)(6)). In order to prosecute a civil claim under the CFAA, a plaintiff must demonstrate loss or damage in excess of $5,000. The CFAA defines loss as "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." *Sprint Nextel Corp. v. Simple Cell, Inc*., No. CIV. CCB-13-617, 2013 WL 3776933, at *6 (D. Md. July 17, 2013) (citing 18 U.S.C. § 1030(e)(8)). The CFAA permits plaintiffs to aggregate multiple intrusions or violations for the purposes of meeting the $5,000 statutory threshold. *Id.*, *7 (citations omitted).

Plaintiffs established each of the elements of a CFAA claim: Fake ONNX Defendants knowingly and intentionally accessed and continue to access protected computers without authorization and knowingly caused the transmission of a program, information, code, and commands, resulting in damage to the protected computers, the software residing thereon, and Microsoft. Lyons Decl. ¶¶ 21-45. As a result of these acts by the Fake ONNX Defendants, Microsoft spent at least $650,000 to investigate and remediate Fake ONNX Defendants' activities. *Id.* ¶ 64. LF Project spent at least $27,000 investigating and remediating the same. Declaration of Michael Dolan ISO *Ex Parte* Application for TRO, Dkt. No. 16 ("Dolan Decl.") ¶ 15.

The Fake ONNX Defendants' conduct is precisely the type of activity the CFAA is designed to prevent. *See e.g*., *Global Policy Partners, LLC v. Yessin*, 2009 U.S. Dist. LEXIS 112472, *9-13 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant was actionable under the CFAA); *Facebook, Inc. v. Fisher*, 2009 U.S. Dist. LEXIS 122578 (N.D. Cal. 2009) (CFAA violation where defendants allegedly engaged in a phishing and spamming scheme that compromised the accounts of Facebook users); *Physicians Interactive v. Lathian Sys., Inc.*, 2003 U.S. Dist. LEXIS 22868, *25 (E.D. Va. 2003) (CFAA

violation where the defendant hacked into a computer and stole confidential information); *Microsoft Corp. v. Doe*, 2015 U.S. Dist. LEXIS 109729 (E.D. Va. Aug. 17, 2015) (CFAA violation for operating botnet); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 46951 (E.D. Va. Apr. 2, 2014) (same).

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).

Microsoft and LF Projects have established that 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 2020 when Abanoub Nady and 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. John Does 3-4 joined the conspiracy and began participating in the Racketeering Enterprise at various times thereafter. *See also United States v. Eppolito,* 543

F.3d 25, 49 (2d Cir. 2008) (an enterprise "may continue to exist even though it undergoes changes in membership"). The Racketeering Enterprise has continuously and effectively carried out its purpose of operating their PhaaS business model, with use of the ONNX-branded phishing kits at the core of the operation ever since and will continue to do so absent the relief Plaintiffs request.

A pattern of racketeering activity "requires at least two acts of racketeering activity, one of which occurred after [October 15, 1970,] and the last of which occurred within ten years ... after the commission of a prior act of racketeering activity." *H.J Inc. v. Northwestern Bell Tel. Co.,* 492 U.S. 229, 237 (1989). A threat of continuing activity "is generally presumed 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). Fake ONNX Defendants have conspired to conduct, and have conducted, and participated in the operations of the Racketeering Enterprise through a continuous pattern of racketeering activity. Each predicate act is related and in furtherance of the common unlawful purpose shared by the members of the Racketeering Enterprise. These acts are continuing and will continue unless and until this Court grants Plaintiffs' request for a temporary restraining order.

Fake ONNX Defendants' racketeering acts include persistent violations of the Computer Fraud and Abuse Act (CFAA). Fake ONNX Defendants' conduct is also "racketeering activity" in the form of wire fraud under 18 U.S.C. § 1343 (violation where one "having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire … communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice."). Fake

ONNX Defendants transmitted communications amongst themselves and to their victims via wire (email communications and online Telegram messages) that crossed U.S. state and international boundaries.

Microsoft and LF Projects have been forced to spend at least $650,000 and $27,000 respectively to investigate and remediate the harms caused by the RICO violation. Accordingly, "there [is] a direct relationship between [the] injury and the defendant's injurious conduct" and "the RICO violation was the but-for (or transactional) cause of [the] injury." *UFCW Local 1776 v. Eli Lilly & Co.,* 620 F.3d 121, 132 (2d Cir. 2010) (citing *Holmes v. Sec. Investor Prat. Corp.,* 503 U.S. 258, 268 (1992)).

ECPA Claim. The ECPA 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). ECPA is violated when a defendant logs into plaintiffs' customers' account without permission (including with stolen credentials) and intentionally accesses the contents of an inbox. *McPherson v. Harker*, 2021 WL 1820290, at *11 (D.D.C. May 6, 2021) (husband violated ECPA "when he 'intentionally access[ed]' Facebook's servers, by logging into his wife's account without her permission, in order to 'obtain[ ] ... a[n] electronic communication,' namely the Facebook messages between Mrs. Thomas and plaintiff, in 'electronic storage' on those servers) (alteration in original). Persons injured by violations of the ECPA may bring a civil suit to obtain injunctive relief and damages. *E.g.*, *Council on American-Islamic Relations Action Network, Inc. v. Gaubatz*, 31 F. Supp. 3d 237 (D.D.C. 2014).

Plaintiffs alleged that Fake ONNX Defendants violated ECPA because they broke into

computer networks using ill-obtained credentials with the direct intention of acquiring the contents of the victims' email inbox and exfiltrating sensitive business or personal information. Microsoft's Windows operating system software and Microsoft's customers' computers running such software are facilities through which electronic communication services are provided to users and customers. *See* Lyons Decl. ¶ 25, n.5. Fake ONNX Defendants knowingly and intentionally accessed the Windows operating system and associated software, services, and computers upon which this software and services run without authorization or in excess of any authorization granted by Microsoft. *See* Lyons Decl. ¶ 44. Through this unauthorized access, Fake ONNX Defendants intercepted, had access to, obtained and altered, and/or prevented legitimate, authorized access to, wire and electronic communications transmitted through the computers and infrastructure of Microsoft and its users. *See* Lyons Decl. ¶¶ 9, 25.

Obtaining stored electronic information in this way, without authorization, constitutes a violation of the Electronic Communications Privacy Act. *See Council on American-Islamic Relations*, 667 F. Supp. 2d at 71-73; *Microsoft Corp. v. Does 1-18,* No. 1:13CV139 LMB/TCB, 2014 WL 1338677, at *7 (E.D. Va. Apr. 2, 2014) (finding violation of ECPA where "Defendant's Bamital botnet used computer codes to hijack internet browsers and search engines by intercepting communications to and from Microsoft servers, and forcing end-users to visit certain websites" which was done "without the end-users' consent, and allowed defendant to monetize end-users' forced activities"). Accordingly, Plaintiffs properly alleged an ECPA claim and default judgment on this claim is warranted.

Lanham Act Claims. Section 1114(1) 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. *See* § 15 U.S.C. § 1114; *see also Two Pesos, Inc. v. Taco Cabana, Inc.*, 505 U.S. 763, 763 (1992); *JFJ Toys, Inc. v. Sears Holdings Corp.,* 237 F. Supp. 3d 311, 340 (D. Md. 2017).

Plaintiffs alleged that the Fake ONNX Defendants misuse Plaintiffs' registered, famous, and distinctive trademarks in a number of fraudulent ways. Fake ONNX Defendants distribute copies of Plaintiffs' registered and distinctive trademarks in fraudulent schemes designed to mislead victims into clicking on links to interact with malicious websites, and in fraudulent versions of Defendants' websites, which deceive victims, cause them confusion, and cause them to mistakenly associate Plaintiffs with this activity. Fake ONNX Defendants make use of counterfeit reproductions of Plaintiffs' marks, *inter alia*, by causing the deceptive use of such marks in domain names and websites, and by causing consumers to engage with malicious phishing domains that bear the Microsoft trademarks. Lyons Decl. ¶¶ 56-62. Fake ONNX Defendants also stole the name and logo belonging to the Open Neural Network Exchange, one of LF Projects' projects. *See* Dolan Decl. ¶¶ 6, 7, 10, 11. An online search of "ONNX" results in articles discussing Fake ONNX Defendants' malicious activities on the same results page as the work conducted by the Open Neural Network Exchange. *Id.* ¶¶ 10-11. Fake ONNX Defendants' creation and use of counterfeit LF Projects' trademarks in connection with its phishing operation is likely to cause confusion and mistake and to deceive the public.

This is a clear violation of the Lanham Act and Microsoft is likely to succeed on the merits. Indeed, "courts have almost unanimously presumed a likelihood of confusion upon a showing that the defendant intentionally copied the plaintiff's trademark *or* trade dress." *Larsen v. Terk Techs. Corp.*, 151 F.3d 140, 149 (4th Cir. 1998) (emphasis included). Defendants' conduct also constitutes false designation of origin under section 1125(a), causing confusion and mistakes as to Microsoft's affiliation with Defendants' malicious conduct. *See, e.g.*, *Brookfield*

Commc'ns., 174 F. 3d at 1066-67 (entering preliminary injunction under Lanham Act §1125(a) for infringement of trademark in software and website code).

The Fake ONNX Defendants' conduct also constitutes 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 . . . or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities." 15 U.S.C. § 1125(a)(1)(A). The Fake ONNX Defendants' misleading use of Plaintiffs' marks causes confusion and mistake as to Plaintiffs' affiliation with the Fake ONNX Defendants' malicious conduct. *Hotmail Corp. v. Van$ Money Pie Inc.,* No. C 98-20064 JW, 1998 WL 388389, at *5 (N.D. Cal. Apr. 16, 1998) (copying the Hotmail trademarks in "e-mail return addresses" constituted false designation of origin; also constituted trademark "dilution" under §1125(c)).

Thus, Plaintiffs properly alleged these Lanham Act claims and default judgment is warranted.

Tort Claims. The Fake ONNX Defendants' conduct is tortious under the common law doctrines of conversion, trespass to chattels, and unjust enrichment.

Conversion and Trespass to Chattel.

Under Virginia law, the tort of conversion "encompasses any wrongful exercise or assumption of authority . . . over another's goods, depriving him 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 (Va. 1994) (quotation omitted); *Microsoft Corp. v. Does 1-2*, No. 1:16CV993, 2017 WL 5163363, at *5 (E.D. Va. Aug. 1, 2017), *report and recommendation adopted*, No. 1:16-CV-00993 (GBL/TCB), 2017 WL 3605317 (E.D. Va. Aug. 22, 2017); *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—sometimes referred to as "the little brother of conversion"—applies where personal property of another is used without authorization, but the conversion is not complete. *Dpr Inc. v. Dinsmore*, 82 Va. Cir. 451, 458 (Va. Cir. Ct. 2011). Courts have found trespass to chattels where a party intentionally uses or interferes with personal property in rightful possession of another without authorization. *Physicians Interactive v. Lathian Sys., Inc.*, 2003 WL 23018270, at *9 (E.D. Va. Dec. 5, 2003) (E.D. Va. 2003). Courts have expressly found that computer hacking constitutes trespass to chattel. *Jones v. United States*, 168 A.3d 703, 717 (D.D.C. 2017); *Matter of Search of Info. Associated with [Redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 13 F. Supp. 3d 145, 151 (D.D.C.) (trespass to chattels when data is copied without authorization).

Here, Fake ONNX Defendants exercised dominion and authority over Microsoft's proprietary services like Outlook and Azure by intruding into its servers supporting those services and over Microsoft's proprietary systems in order to gain access to content stored on those servers like email and access to other applications on the Azure platform. These acts deprived Microsoft of its right to control the content, functionality, and nature of its software and services. District courts in the Fourth Circuit have recognized that computer hacking can amount to tortious conduct under the doctrines of conversion and trespass to chattels. *See supra*; *see also Microsoft Corp. v. Does 1-18*, No. 1:13CV139 LMB/TCB, 2014 WL 1338677, at *9 (E.D. Va. Apr. 2, 2014) ("The unauthorized intrusion into an individual's computer system through hacking, malware, or even unwanted communications supports actions under these claims");

Microsoft Corp. v. John Does 1-8, No. 1:14-CV-811, 2015 WL 4937441, at *12 (E.D. Va. Aug. 17, 2015).

Unjust Enrichment. Under Virginia law, a claim for unjust enrichment requests the plaintiff to establish "(1) the plaintiff conferred a benefit upon the defendant; (2) the defendant knew that the plaintiff conferred the benefit; and (3) the defendant accepted or retained the benefit under circumstances that render it inequitable for the defendant to retain the benefit without paying for its value." *Seale & Assocs., Inc. v. Ingersoll-Rand Co.*, No. 115CV01282GBLIDD, 2016 WL 4435083, at *9 (E.D. Va. Aug. 16, 2016). Here, Plaintiffs Microsoft and LF Projects have demonstrated that that (1) Plaintiffs conferred a benefit on the Fake ONNX Defendants; (2) Defendants' knowledge of conferring the benefit; and (3) Fake ONNX Defendants' acceptance or retention of the benefit under circumstances that "'render it inequitable for the defendant to retain the benefit without paying for its value.'" *Microsoft Corp. v. John Does 1-8*, 2015 WL 49037441, at *12. The Fake ONNX 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. ¶¶ 56-62; Dolan Decl. ¶¶ 8-13. In order to ensure greater efficacy of their criminal operation, Fake ONNX Defendants usurp this goodwill. Moreover, once Fake ONNX Defendants complete a phishing attack and gain access to a victims' account, Fake ONNX Defendants are further unjustly enriched through the access they have obtained through ill-gotten means.

In sum, the well-pled allegations in Microsoft's Complaint, which set forth the elements of each of Microsoft's claims, are taken as true given Defendants default. *SEC v. Lawbaugh*, 359

F. Supp. 2d 418, 421 (D. Md. 2005). Accordingly, the only question is what remedy to afford Microsoft.

D. A Permanent Injunction Should Issue to Prevent Further Irreparable Harm

A permanent injunction is appropriate where: (1) plaintiff has suffered an irreparable injury; (2) remedies available at law (e.g. monetary damages) are inadequate to compensate for that injury; (3) considering the balance of hardships between plaintiff and defendant, a remedy in equity is warranted; and (4) the public interest would not be disserved by a permanent injunction. *Monsanto Co. v. Geerton Seed Farms*, 561 U.S. 139, 156-57 (2010) (quoting *eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 391 (2006)); *see also EMI April Music, Inc. v. White*, 618 F. Supp. 2d 497, 509 (E.D. Va. 2009) (citing *Phelps & Assocs., LLC v. Galloway*, 492 F.3d 532, 543 (4th Cir. 2007)).

1. Plaintiffs Have Suffered Irreparable Injury That Cannot Be Compensated Monetarily.

Consumer confusion and injury to business goodwill constitute irreparable harm. *PBM Prods., LLC v. Mead Johnson & Co.*, 639 F.3d 111, 127 (4th Cir. 2011) (false and misleading representations constituted irreparable harm, and warranted permanent injunction); *Int'l Labor Mgmt. Corp. v. Perez*, 2014 U.S. Dist. LEXIS 57803, 35 (M.D.N.C. Apr. 25, 2014) (damage to "reputation and loss of goodwill constitutes irreparable harm for purposes of injunctive relief") (citing *In Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.*, 22 F.3d 546 (4th Cir. 1994)); *MicroAire Surgical Instruments, LLC v. Arthrex, Inc.*, 726 F. Supp. 2d 604, 635 (W.D. Va. 2010) ("The loss of goodwill is a well-recognized basis for finding irreparable harm"). A finding of irreparable harm usually follows a finding of unlawful use of a trademark and a likelihood of confusion. *Ledo Pizza Sys. v. Singh*, 2013 U.S. Dist. LEXIS 146938, 9 (D. Md. Oct. 10, 2013); *Nabisco Brands, Inc. v. Conusa Corp.*, 722 F. Supp. 1287, 1290 (M.D.N.C.

1989) ("In the context of a trademark infringement dispute, several courts have held that where likelihood of confusion is established likelihood of success on the merits as well as risk of irreparable harm follow.").

To carry out its criminal operation, Fake ONNX Defendants use Microsoft based software and services. This is done intentionally to improperly leverage Microsoft's brandings, trademarks, and reputation and to deceive victims into believing that Fake ONNX Defendants' malicious phishing attacks are associated or endorsed by Microsoft. Lyons Decl. ¶ 60. If a customer mistakenly believes that Microsoft endorses the cybercriminal behavior of Fake ONNX Defendants, Microsoft's reputation and goodwill is harmed beyond repair—indeed, in such circumstances the customer may be lost forever. *Id.* ¶ 62. Fake ONNX Defendants have also stolen their name and logo from LF Projects' ONNX Exchange. Dolan Decl. ¶¶ 6, 7. The "ONNX" name and logo are registered by LF Projects. *Id.* ¶ 5. ONNX Exchange and the ONNX-branded phishing kit share not only the same name, but also the same geometric shape as the logo. *Id.* ¶ 6. This causes significant confusion between Plaintiff LF Projects' ONNX Exchange and Fake ONNX Defendants' ONNX-branded phishing kits. *Id.* ¶¶ 9-11. The mere fact that Plaintiffs had to create artificial names to describe Plaintiff LF Projects' Open Neural Network Exchange project and Fake ONNX Defendants to distinguish the parties establishes the very real likelihood of confusion.

The Court previously found that this harm caused to Plaintiffs by the Fake ONNX operations, in particular the confusing and misleading use of Plaintiffs' trademarks and brands, constitutes irreparable harm. Dkt. No. 16 at 2-4. To the extent that Defendants are able to continue to use domains bearing Plaintiffs' trademarks and brands in furtherance of their activities, such irreparable harm would certainly continue in the future.

This finding is consistent with several cases that have concluded that computer malware operations and associated use of Microsoft's trademarks cause irreparable harm. *See, e.g., Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (injunction to dismantle botnet command and control servers); *Microsoft v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (injunction to dismantle botnet command and control servers); *Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va., Brinkema J.) (same); *Microsoft v. John Does 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.) (same); *Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) (same); *FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal. 2009) (Whyte J.) (injunction disconnecting service to botnet hosting company).

In addition to the irreparable harm caused to Plaintiffs' goodwill, even the monetary harm caused by Defendants is and will be irremediable absent an injunction because Defendants are elusive cybercriminals against whom Plaintiffs are unlikely to be able to enforce a judgment. *See, e.g.*, *Khepera-Bey v. Santander Consum. USA, Inc.*, 2013 U.S. Dist. LEXIS 87641, 13-14 (D. Md. June 21, 2013) ("circumstances[] such as insolvency or unsatisfiability of a money judgment, can show irreparable harm."); *accord Burns v. Dennis-Lambert Invs., Ltd. P'ship*, 2012 Bankr. LEXIS 1107, 9 (Bankr. M.D.N.C. Mar. 15, 2012) ("a preliminary injunction may be appropriate where 'damages may be unobtainable from the defendant because he may become insolvent before final judgment can be entered.'"); *Rudolph v. Beacon Indep. Living LLC*, 2012 U.S. Dist. LEXIS 7075, 5 (W.D.N.C. Jan. 23, 2012) ("Irreparable harm exists here because of Defendant Beacon's continued occupancy of the Facility without paying any rents, particularly in light of the threat of insolvency by one or more Defendants.").

2. The Balance of Equities Strongly Favors an Injunction.

Because Defendants are engaged in an illegal scheme to defraud computer users and injure Plaintiffs, the balance of equities clearly tips in favor granting a permanent injunction. *See, e.g.*, *PBM Prods., LLC v. Mead Johnson & Co.*, 639 F.3d 111, 127 (4th Cir. 2011) (where defendant had no legitimate interest in "perpetuating the false and misleading" representations, balance of equities warranted injunction); *US Airways, Inc. v. US Airline Pilots Ass'n,* 813 F. Supp. 2d 710, 736 (W.D.N.C. 2011) (injunction appropriate where, in balance of the equities, denying injunction would result in "enormous disruption and harm" to plaintiff and the public, granting injunction would only require defendant to comply with existing legal duties); *Pesch v. First City Bank of Dallas*, 637 F. Supp. 1539, 1543 (N.D. Tex. 1986) (balance of hardships clearly favors injunction where enjoined activity is illegal). On one side of the scales of equity rests the harm to Microsoft, its customers, LF Projects, and the public caused by Defendants' ongoing Fake ONNX operation, including deceptive use of Plaintiffs' trademarks and brands in the Fake ONNX domains and the Fake ONNX-branded phishing kit. By contrast, on the other side, rests no legally cognizable harm to Defendants because an injunction would only require them to cease illegal activities. For this reason, an ongoing permanent injunction is appropriate. *See US Airways*, 13 F. Supp. 2d at 736.

3. An Injunction is in the Public Interest.

It is clear that an injunction would serve the public interest here. In the absence of a permanent injunction, Defendants would be able to reconstitute their cybercriminal network, which means they could continue their unlawful activities, including intruding into more victim accounts and infecting more computers, deceiving more members of the public, and stealing more information from the accounts and computers of their innocent victims. Moreover, the

public interest is clearly served by enforcing statutes designed to protect the public, such as the Lanham Act and CFAA. *See, e.g.*, *BSN Med., Inc. v. Art Witkowski*, 2008 U.S. Dist. LEXIS 95338, at *10 (W.D.N.C. Nov. 21, 2008) ("In a trademark case, the public interest is 'most often a synonym for the right of the public not to be deceived or confused.' . . . the infringer's use damages the public interest.") (citation omitted); *accord Meineke Car Care Ctrs., Inc. v. Bica,* 2011 WL 4829420 (W.D.N.C. Oct. 12, 2011) (similar); *PBM Prods., LLC v. Mead Johnson & Co.*, 639 F.3d 111, 127 (4th Cir. 2011) (preventing false or misleading representations constitutes a "strong public interest" supporting permanent injunction); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, at *32 (E.D. Va. Jan. 6, 2014) (public interest weighed in favor of injunction to enforce CFAA).

Here, Plaintiffs request an injunction that will transfer permanent control of the existing Fake ONNX domains to Microsoft. As a result of such injunction, Microsoft will be able to protect itself and its customers from the threat of Defendants' operations and can continue to assist victims in cleaning infected computers. Absent the requested injunction, the Defendants' existing infrastructure would be released back into Defendants' control, and Defendants would be able to use that infrastructure to deceive computer users, issue instructions to infected computers, take control over them, and exfiltrate high value, sensitive and confidential information. Given the risks the public will face absent an injunction, the calculus is clear.

There is no risk that the injunction will impact any legitimate interest of any party. Neither Defendants nor any other party have come forward to assert any undue impact by Microsoft's control of the existing Fake ONNX domains. In particular, the third-party domain registries responsible for administering the Fake ONNX Defendants' domains must simply carry out routine actions that they would take in the ordinary course of their business, namely

transferring the domains to the permanent control of Plaintiffs.

Directing such routine actions and reasonable cooperation to vindicate the public's interest, and ensure that the permanent injunction is not rendered fruitless, is authorized by the All Writs Act (28 U.S.C. § 1651(a)) and the Court's equitable authority, will not offend Due Process, does not interfere with normal operations, does not deprive any third party of any property interest and requires Plaintiffs to compensate the third parties for the assistance rendered.[4] Indeed, Plaintiffs have conferred with relevant domain registries, and they have no objection to the requested relief.

V. 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.

[4] The All Writs Act provides that a court may issue all writs necessary or appropriate for the administration of justice. 28 U.S.C. § 1651(a); *see United States v. New York Tel. Co*., 434 U.S. 159, 174 (1977) (authorizing order to third-party telephone company to assist in implementation of a pen register warrant); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 30 (E.D. Va. Jan. 6, 2014) (authorizing relief similar to that requested herein); *Sarnecka-Crouch v. Billington,* No. 06-1169 ESH, 2012 WL 3060165, at *2 (D.D.C. July 26, 2012) (ordering Commissioner of the Social Security Administration to provide the Library of Congress with all documents pertaining to plaintiff's Social Security benefits account for the period 2005-2009); *Evans v. Williams,* No. 76-293, 1999 WL 1212884, at *3 (D.D.C. Aug. 20, 1999) (finding no other effective means exists to address specifically the continuing unwillingness of the Superior Court to provide access to the information required by District of Columbia Court other than using power under the All Writs Act) (citing *New York Tel. Co*., 434 U.S. at 172); *Dell, Inc. v. Belgiumdomains, LLC*, 07-22674, 2007 WL 6862341, at *6 (S.D. Fla. Nov. 21, 2007) (All Writs Act applied in conjunction with trademark seizure under Rule 65 and Lanham Act).

Dated: July 28, 2026

Robbie Rogart Jost (VA Bar No. 84377)
David J. Ervin (VA Bar No. 34719)
Jeffrey L. Poston (*pro hac vice*)
CROWELL & MORING LLP
600 Fifth Street NW
Washington, DC 20001
T: 202-624-2500
F: 202628-5116
RJost@crowell.com
DErvin@crowell.com
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

Counsel for Plaintiffs Microsoft Corporation and LF Projects LLC