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

MICROSOFT CORPORATION, a Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING A COMPUTER NETWORK THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS,

Defendants.

Civil Action No: 1:21-cv-822

BRIEF IN SUPPORT OF APPLICATION OF MICROSOFT CORPORATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiff Microsoft Corporation ("Microsoft") seeks an emergency *ex parte* temporary restraining order ("TRO") and a preliminary injunction designed to disrupt the technical malicious infrastructure of a sophisticated online criminal network that is attacking Microsoft Corporation ("Microsoft"), its Office 365 ("O365") service, and its customers through malicious "homoglyph" domains that unlawfully impersonate legitimate Microsoft O365 customers and their businesses. Homoglyph attacks rely on elaborate deception that leverages the similarities of character scripts to create imposter domains used to deceive unsuspecting individuals. Defendants use malicious homoglyph domains together with stolen customer credentials to unlawfully access customer accounts, monitor customer email traffic, gather intelligence on pending financial transactions, and criminally impersonate O365 customers, all in an attempt to deceive their victims into transferring funds to the cybercriminals. The relief sought in this action is necessary to stop the cybercriminals and prevent irreparable and ongoing harm to

Microsoft and its customers.

Microsoft seeks to stop John Does 1-2 (collectively "Defendants") from targeting Microsoft's O365 customers and services and conducting malicious activity including business email compromise attacks ("BEC"), using the Internet domains set forth at **Appendix A** to the Complaint which are referred to as the "Malicious Infrastructure." These activities cause Microsoft irreparable reputational harm and loss of control over its relationships and brands, for which no monetary recourse is available.

Ex parte relief is essential. Notice to Defendants would provide them with an opportunity to destroy, move, conceal, or otherwise make inaccessible the instrumentalities they use to carry out their attacks and the evidence of their unlawful activity. Giving Defendants that opportunity would render further prosecution of this lawsuit entirely fruitless.

This type of requested *ex parte* relief is not uncommon when denying defendants access to harmful online infrastructure used by unidentified defendants for illegal operations. This Court has repeatedly in cases involving Microsoft and other plaintiffs granted such extraordinary relief to deny defendants access to or use of harmful online infrastructure. For example, in a similar case, this Court (Judge O'Grady) adopted an approach where:

1. The Court issued a tailored *ex parte* TRO, including provisions sufficient to effectively transfer control of defendants' harmful domain names and deny defendants access to or use of the harmful infrastructure, preserve all evidence of its operations and stop the irreparable harm being inflicted on the plaintiff and its customers;

2. Immediately after implementing the TRO, the plaintiff undertook a comprehensive effort to provide notice of the preliminary injunction hearing and to effect service of process on the defendants, including Court-authorized alternate service by email, electronic messaging services, mail, facsimile, publication, and treaty-based means; and

3. After notice, the Court held a preliminary injunction hearing and granted the preliminary injunction while the case proceeded in order to ensure that the injury caused by the harmful infrastructure would not continue during the action.

See Sophos v. John Does 1-2, Case No. 1:20-cv-000502 (E.D. Va. May 1, 2020) (granting preliminary injunction order), Dkt. No. 15. Federal courts have repeatedly followed this approach and should do so here as well.[1]

If the Court grants Microsoft's requested relief, immediately upon execution of the TRO, Microsoft will make a robust effort in accordance with the requirements of Due Process to provide notice of the preliminary injunction hearing and to serve process on Defendants. Microsoft will immediately serve the complaint and all papers in this action on Defendants, using known contact information and contact information maintained by domain registrars and hosting companies that provide Defendants' infrastructure.

I. STATEMENT OF FACTS

Microsoft seeks to stop Defendants' illegal conduct, including the complex scheme to target Microsoft's O365 customers and services and conduct malicious activity including business email compromise attacks, using stolen credentials to access O365 customer email accounts, imitate customer employees, and target their trusted networks, vendors, contractors, and agents in an effort to deceive them into sending or approving fraudulent financial payments. Declaration of Donal Keating ("Keating Decl.") in Support of *Ex Parte* Application for an Emergency Temporary Restraining Order and Order to Show Cause re Preliminary Injunction.

A. Overview of Microsoft's Efforts to Protect Customers and Defendants' Attempts to Evade Such Efforts

Microsoft commits tremendous resources to detecting and blocking threats to its O365 service, its customers and their accounts. *Id.* ¶ 10. Microsoft recently detected evidence of Defendants' malicious activity and promptly began to identify patterns and attempted to block

[1] Declaration of Matthew Welling ("Welling Decl.") in Support of *Ex Parte* Application for an Emergency Temporary Restraining Order and Order to Show Cause re Preliminary Injunction at Exs. 8-13 (citing cases granting emergency injunctive relief).

Defendants' activity through the technical tools at its disposal. *Id.* Defendants' activities victimize Microsoft's customers in two ways –first, they use stolen credentials to gain unauthorized access to and compromise accounts of O365 customers ("compromised account victim"), and second, they use this unauthorized access to O365 accounts to exfiltrate information and develop intelligence about financial transactions from the compromised account victim's wider network – including customers, vendors, or agents ("financial fraud victims") whether they are other O365 users or those on other email platforms. *Id.* Defendants frequently target senior managers, financial roles (accountants, bookkeepers, etc.), and sales positions (purchasing and services) in a variety of industries. *Id.*

Further, to the extent Defendants have registered homoglyph imposter domains (hereinafter, "homoglyph imposter domains") and are hosting those malicious domains on O365 tenants that Defendants have fraudulently set up to carry out their criminal schemes, Microsoft takes steps to identify and block the ability of Defendants to use such fraudulent tenants and related accounts for malicious purposes. *Id.* ¶ 11.

Yet, even with such self-help measures, the risk of irreparable harm still exists because, even after Microsoft prevents and disables use of a fraudulent O365 tenant. Defendants are nonetheless able to move these homoglyph imposter domains to other third-party domain registrars and hosting facilities outside the Microsoft ecosystem and continue to direct criminal activities at Microsoft and O365 customers. *Id.* ¶ 12. It is also possible that Defendants register domains and host them from inception outside of Microsoft's ecosystem, placing them beyond Microsoft's internal mitigation measures. *Id.* In all such scenarios, Defendants continue to target Microsoft's customers and others for financial fraud and other cybercrime. *Id.*

Defendants' ability to mobilize and move homoglyph imposter domains presents an ongoing threat to Microsoft's customers and others and undermines Microsoft's efforts to protect its customers and networks. *Id.* ¶ 14. Without the relief requested from this Court, Microsoft will be engaged in a constant game of whack-a-mole where it attempts to protect its customers by shutting down Defendants' malicious activity using tools at its disposal within O365, only to have Defendants move their homoglyph imposter domains to another domain registrar or hosting company, where the domain can be administered and email services set up by Defendants on other companies email services, thus enabling Defendants to continue their attacks against Microsoft and Microsoft customers and their networks. *Id.* This risk is not theoretical, as there is already evidence that Defendants have moved one of the domains from the O365 environment to another hosting company and thereby taken it outside Microsoft's reach.

Given the risk posed by Defendants reconstituting and moving their operations to commit further malicious acts, Defendants pose a current and ongoing threat to Microsoft and the security of its customers such that it is necessary to seek immediate relief in this action. *Id.* ¶ 15.

B. Defendants Use Unauthorized Access to Microsoft Office 365 Customers' Accounts to Target Their Businesses and Larger Networks

Through various investigative techniques, Microsoft recently uncovered Defendants' scheme to gain unauthorized access and compromise O365 accounts, create homoglyph imposter domains, and use this malicious infrastructure and surveillance efforts to target compromised account victim's wider network – including customers, vendors, or agents – for fraudulent financial transactions. *Id.* ¶ 18.

1. Phase One: Unauthorized Access to Office 365 Using Stolen Credentials

The first phase of the business email compromise scheme involves stealing Microsoft O365 credentials through among other means sending credential phishing emails, using malicious websites to socially engineer victims into divulging their account login credentials, or purchasing stolen credentials. *Id.* ¶¶ 19-21. Regardless of the method of compromise, Defendants are using credentials to cause severe harm to Microsoft and its customers. *Id.*

2. Phase Two: Monitoring Compromised Office 365 Account Email Traffic and Contacts to Identify Opportunities for Further Criminal Activities

In the second phase, once Defendants unlawfully gain access to an Office 365 account using stolen credentials, they begin reconnaissance of the compromised account and the compromised account victim's networks in a few ways. *Id.* ¶ 22. Defendants either directly access or forward emails with keywords such as "invoice," "accounts receivable," "funds," "overdue," "payroll," or "IBAN" to a collection email account controlled and monitored by Defendants for further analysis. *Id.* ¶ 23.

Defendants identify key emails and senders to impersonate and identify recipients to target. *Id.* ¶ 24. Defendants then register homoglyph imposter domains and set up spoof email addresses on those domains to fraudulently insert themselves into ongoing business transactions or socially engineer opportunities to interact with the financial or billing department of victims. *Id*. Defendants take advantage of the fact that these emails are designed to appear legitimate and imitate legitimate email addresses that are trusted or known contacts of the recipient, and are part of existing, legitimate communications. *Id.*

3. Phase Three: Impersonating O365 Account Owners or Members of Their Networks to Solicit Fraudulent Financial Transactions

In the final phase, Defendants set up homoglyph imposter domains together with spoofed email addresses to impersonate compromised O365 account owners or members of their networks and solicit fraudulent financial transactions. *Id.* ¶ 26. Defendants created malicious domains that are "homoglyphs" of legitimate domain names. *Id.* ¶ 28. Homoglyphs are a technique by which attackers abuse similarities of character scripts to create deceptively similar domains. *Id*. For example, a homoglyph domain may utilize characters with shapes that appear identical or very similar to the characters of a legitimate domain. *Id*. Defendants' efforts to imitate legitimate domains using fraudulent homoglyph variants are clear from the examples below.

- **Defendants add adding a single letter:**

Legitimate	**Impersonation**
junctionfueling.com	junctionfuelings.com (Adds an "s")

- **Defendants replace letters with similar appearing letters:**

Legitimate	**Impersonation**
leaseaccelerator.com	leaseacceierator.com (Changes "l" to "i")
lithiumamericas.com	lithlumamericas.com (Changes "i" to "l")
sliao.ca	sllao.ca (Changes "i" to "l")

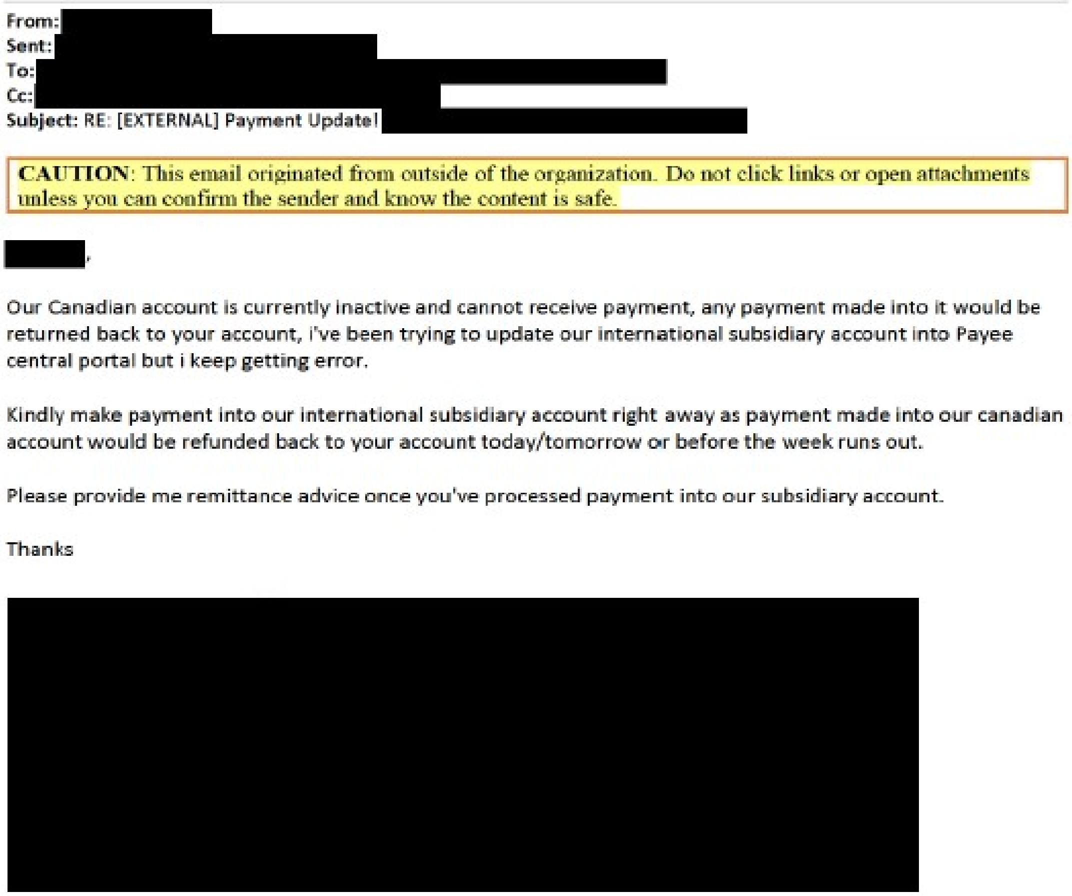
- **Defendants change top level domain information:**

Legitimate	**Impersonation**
ccp.edu	ccp-edu.com (Adds .com)

Once Defendants' homoglyph imposter domains are registered and operational, they can send spoofed emails from these homoglyph imposter domains which impersonate the compromised account victim or other legitimate contacts of the target – who might typically respond to requests to pay wire transfer requests, invoices, or billing statements. *Id*. ¶ 29.

Defendants' fraudulent email communications build on existing, legitimate email communications, course of dealings, or business relationships. *Id*. ¶ 31. Defendants have access to prior email chains, can familiarize themselves with key terminology or terms of art, relevant documents, invoices, or account numbers. *Id*. Defendants commonly use an excuse about why new financial transfer information is being provided or threaten the victim for failure to provide payment or other strategies to create urgency and justify new payment arrangements. *Id*. These strategies often include providing doctored invoice documents and tampered banking information. *Id*. The financial fraud victims have no reason to suspect anything malicious, as the email appears to be from a known, legitimate email address, references existing conversations or prior communications, and provides doctored imitations of real financial documents. *Id*.

One example of a business compromise email is included below and demonstrates how it mirrors genuine email traffic and instructs the financial fraud victim to redirect an invoice payment. Defendants identified a legitimate email communication from the compromised account of an Office 365 customer referencing payment issues and asking for advice on processing payment:



From: [redacted]
Sent: [redacted]
To: [redacted]
Cc: [redacted]
Subject: RE: [EXTERNAL] Payment Update! [redacted]

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you can confirm the sender and know the content is safe.

[redacted],

Our Canadian account is currently inactive and cannot receive payment, any payment made into it would be returned back to your account, i've been trying to update our international subsidiary account into Payee central portal but i keep getting error.

Kindly make payment into our international subsidiary account right away as payment made into our canadian account would be refunded back to your account today/tomorrow or before the week runs out.

Please provide me remittance advice once you've processed payment into our subsidiary account.

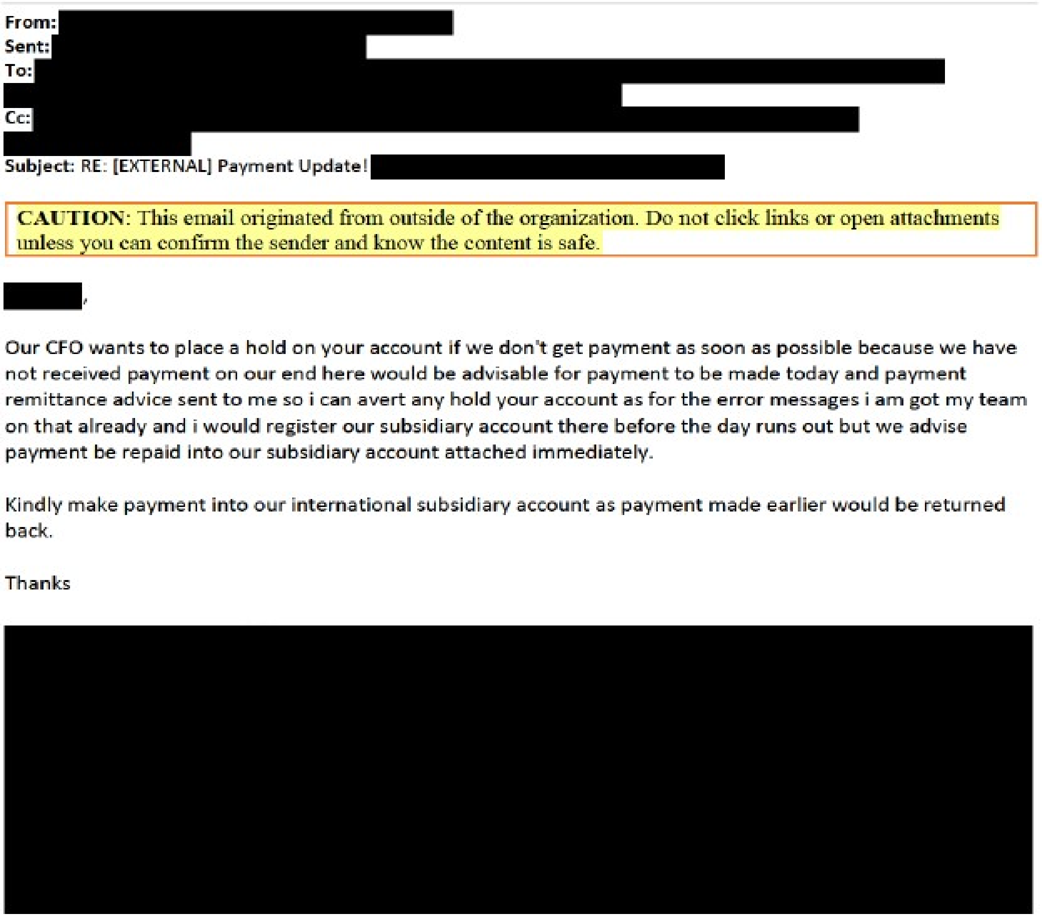
Thanks

[redacted]

Figure 1

Defendants capitalized on this opportunity and sent an impersonation email from a homoglyph imposter domain using the *same sender name* and *nearly identical domain*. *Id.* ¶ 35. The only difference between the genuine communication and the imposter communication was a single letter changed in the mail exchange domain – changing sliao.ca to sllao.ca – done to escape notice of the recipient and deceive them into believing the email was a legitimate communication from a known trusted source. *Id.*

Defendants used the same subject line and format of an email from the earlier, legitimate conversation, but falsely claimed a hold was placed on the account by the CFO, time was running out, and payment needed to be received as soon as possible:



From: [redacted]
Sent: [redacted]
To: [redacted]
Cc: [redacted]
Subject: RE: [EXTERNAL] Payment Update! [redacted]

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you can confirm the sender and know the content is safe.

[redacted],

Our CFO wants to place a hold on your account if we don't get payment as soon as possible because we have not received payment on our end here would be advisable for payment to be made today and payment remittance advice sent to me so i can avert any hold your account as for the error messages i am got my team on that already and i would register our subsidiary account there before the day runs out but we advise payment be repaid into our subsidiary account attached immediately.

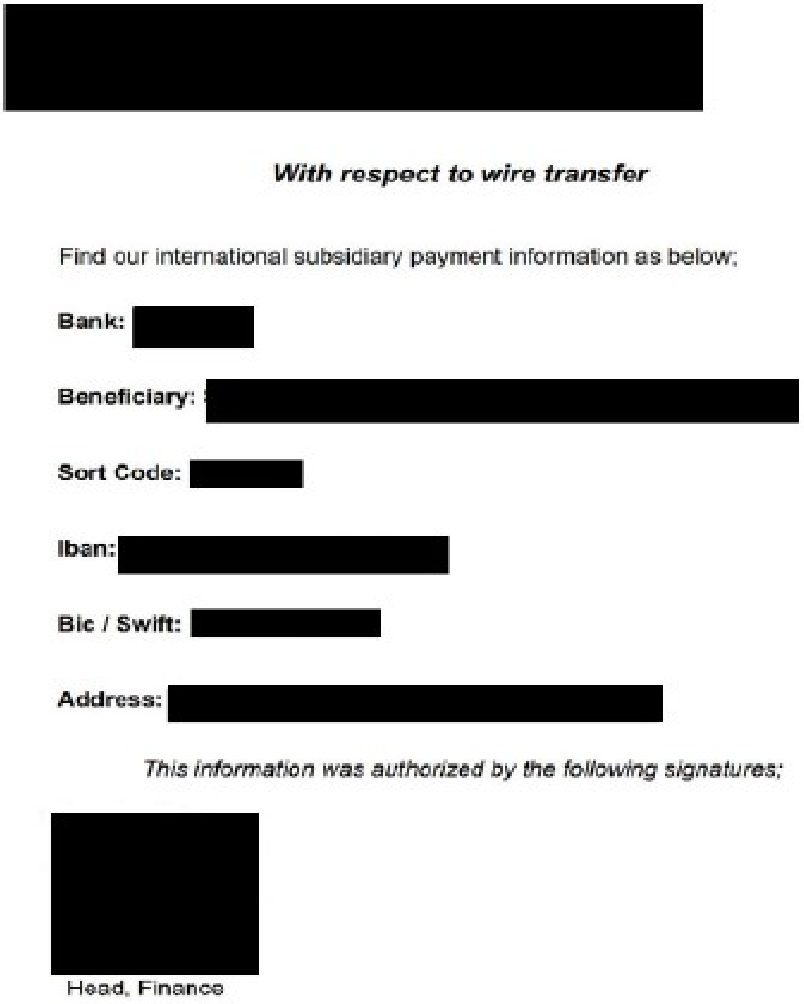
Kindly make payment into our international subsidiary account as payment made earlier would be returned back.

Thanks

[redacted]

Figure 2

Defendants then solicit a fraudulent wire transfer by sending new wire transfer information appearing to be legitimate and including company logo information, requesting funds be sent to Defendants:



[redacted]

With respect to wire transfer

Find our international subsidiary payment information as below;

Bank: [redacted]

Beneficiary: [redacted]

Sort Code: [redacted]

Iban: [redacted]

Bic / Swift: [redacted]

Address: [redacted]

This information was authorized by the following signatures;

[redacted]

Head, Finance

Figure 3

Defendants do not rely on malicious links or attachments in these communications – instead, using the intelligence needed to imitate legitimate business transactions gathered after unlawfully accessing a compromised account – in an effort to evade detection and makes it more difficult for customers to identify malicious emails. *Id.* ¶ 38. Defendants are aware that their conduct violates Microsoft's terms and conditions and is against the law. *Id.* ¶ 41. As a result, once detected or addressed by Microsoft through technical tools at its disposal, Defendants will often move their malicious infrastructure (and domains) outside the Microsoft ecosystem in an attempt to continue their illegal activities, or register and host domains wholly outside Microsoft's ecosystem from the outset. *Id.*

C. Defendants Register Homoglyph Imposter Domain Names to Impersonate Domains of Legitimate Microsoft Customers

Defendants registered multiple homoglyph imposter domains listed below including the one used above in soliciting a fraudulent wire transfer:

Homoglyph Imposter Domains	**Registrar**
ccp-edu.com	NameSilo, LLC
junctionfuelings.com	NameSilo, LLC
lverk.com	NameSilo, LLC
tattersails.com	NameSilo, LLC
cupidoconstructlon.com	NameSilo, LLC
thegiaint.com	NameSilo, LLC
leaseacceierator.com	NameSilo, LLC
kimballlnternational.com	NameSilo, LLC
nationalsafetyconsuiting.com	NameSilo, LLC
ldisuperstore.com	NameSilo, LLC
lithlumamericas.com	NameSilo, LLC
usgeomatlcs.com	NameSilo, LLC
ldimn.com	NameSilo, LLC
aerocerts.com	NameSilo, LLC
napieslegal.com	NameSilo, LLC
sllao.ca	KS Domains Ltd./Key Systems GmbH
exarr.co	NameSilo, LLC

These domain names used by Defendants are identified in **Appendix A** to the Complaint.

D. Microsoft's Office 365 Services and Protection Measures

Office 365 is an online service that provides access to Microsoft's Office software on a subscription basis. *Id.* ¶ 16. Customers purchase a subscription to Office 365 that may provide access to both cloud and locally stored versions of the software. *Id.* Use of Office 365 requires an online account. *Id.*

Microsoft goes to great lengths to protect customer accounts. In particular, Microsoft engineered Office 365 with the intent to eliminate threats before reaching Office 365 users. Microsoft uses real-time anti-spam and multiple anti-malware engines to prevent threats from reaching their inboxes. *Id.* ¶ 17. Microsoft also offers Microsoft Defender for Office 365,[2] which helps protect customers against new, sophisticated attacks in real time. *Id.* In addition to incorporating tools to stop phishing emails before they reach users, Microsoft also investigates the underlying phishing attacks to identify and prevent malicious attacks carried out by criminal organizations. *Id.*

E. Harm to Microsoft

Microsoft® is a provider of the Office 365® cloud-based business and productivity suite of services. *Id.* ¶ 47. Microsoft has invested substantial resources in developing and marketing resilient and secure cloud services. *Id.* Due to the security and effectiveness of Microsoft's services, Microsoft has generated substantial trust with its customers to protect their data, has established a strong brand as a leader in the security market, and has developed the Microsoft name and the names of its services into famous world-wide symbols that are well-recognized within its channels of trade. *Id.*

Defendants' attack – in registering the homoglyph imposter domains – results in portable, weaponized mail exchange domains that can be associated to any email service provider and then used in the future to attack Microsoft customers, a threat that is ongoing and pervasive and causes injury to Microsoft. *Id.* ¶ 50. Customers expect Microsoft to provide safe and trustworthy products and services. There is a great risk that Microsoft's customers may incorrectly attribute Defendants' malicious activities to Microsoft's products and services. *Id.* ¶ 51. Further, Defendants' ability to damage Microsoft's reputation extends even after they are detected and

[2] *See generally* https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description.

lose access to O365 since they can take their weaponized domains to other platforms and continue attacks. *Id*.

Microsoft is similarly injured because Defendants frequently attempt to launch their scheme from within Microsoft's Office 365 service in an effort to victimize Microsoft customers. *Id*. ¶ 52. Microsoft must bear an extraordinary burden to address cybercrime directed at its services and customers. Microsoft must develop technical countermeasures and defenses, to suppress Defendants' activities, address customer service issues caused by Defendants and must expend substantial resources dealing with the injury and confusion and to resist ongoing attempted attacks on its infrastructure, products, services, and customers. *Id*.

II. <u>LEGAL STANDARD</u>

The purpose of a preliminary injunction is to protect the status quo and to prevent irreparable harm during the pendency of a lawsuit and to preserve the court's ability to render a meaningful judgment on the merits. *United States v. South Carolina*, 720 F.3d 518, 524 (4th Cir. 2013) (citations omitted). "Parties seeking a preliminary injunction must demonstrate that (1) they are likely to succeed on the merits, (2) they are likely to suffer irreparable harm, (3) the balance of hardships tips in their favor, and (4) the injunction is in the public interest." *Metro. Reg'l Info. Sys. v. Am. Home Realty Network, Inc*., 722 F.3d 591, 595 (4th Cir. 2013) (citing *Winter v. Natural Res. Def. Council, Inc.,* 555 U.S. 7, 20 (2008)).

III. <u>MICROSOFT'S REQUESTED RELIEF IS WARRANTED</u>

This matter presents a quintessential case for injunctive relief. Defendants' conduct causes irreparable harm to Microsoft, its customers, and the general public. Every day that passes gives Defendants an opportunity to expand their illegal operations. Unless enjoined, Defendants will continue to cause irreparable harm to Microsoft and its customers.

A. Microsoft Is Likely To Succeed On The Merits Of Its Claims

Even at this early stage in the proceedings, the record demonstrates that Microsoft will be able to establish the elements of each of its claims. The evidence supporting Microsoft's TRO application is based on the diligent work of experienced investigators and supported by substantial empirical evidence and forensic documentation. Given the strength of this evidence, the likelihood of success on the merits weighs heavily in favor of granting injunctive relief.

1. Defendants' Conduct Violates The CFAA

Congress enacted the Computer Fraud and Abuse Act (the "CFAA") specifically to address computer crime. *See, e.g., Big Rock Sports, LLC v. AcuSport Corp.*, No. 4:08-CV-159-F, 2011 WL 4459189, at *1 (E.D.N.C. Sept. 26, 2011). "Any computer with Internet access [is] subject [to] the statute's protection." *Id. Inter alia*, 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); or (4) attempts any of the foregoing. 18 U.S.C. § 1030(b).

A "protected computer" is a computer "used in interstate or foreign commerce or communication." *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*., 2013 WL 3776933, at *6 (D. Md. July 17, 2013) (citing 18 U.S.C. § 1030(e)(8)). "'[D]amage . . . means any impairment to the integrity or availability of data, a program, a system, or information.'" *Id.* (citing 18 U.S.C. § 1030(e)(11)). The Fourth Circuit has recognized that this "broadly worded provision plainly contemplates consequential damages" such as "costs incurred as part of the response to a CFAA violation, including the investigation of an offense." *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009). The CFAA permits plaintiffs to aggregate multiple intrusions or violations for the purposes of meeting the $5,000 statutory threshold. *See Sprint Nextel Corp.,* 2013 WL 3776933, at *7 (citations omitted).

In sum, in order to prevail on their CFAA claim, Microsoft must establish that Defendants (1) accessed and/or attempted to access a protected computer; (2) without authorization; (3) for the purpose of obtaining information or defrauding others; (4) resulting in loss or damage in excess of $5,000. Donal Keating's Declaration establishes that Defendants' conduct satisfies each of these elements. First, each of the computers that Defendants have attempted to access is, by definition, a protected computer, because only computers that connect to the internet can possibly be targeted. *See supra*; 18 U.S.C. § 1030(e)(2)(B) (defining "protected computer" as a computer "used in interstate or foreign commerce or communication”).

Second, Defendant use stolen credentials to imitate O365 customers and target their trusted networks, vendors, contractors, and agents in an effort to deceive them into sending or approving fraudulent financial payments. *See Elsevier Inc. v. WWW.Sci-Hub.org*, 2015 U.S. Dist. LEXIS 147639, at *5 (S.D.N.Y. Oct. 28, 2015) (recognizing a CFAA claim where defendant “gain[ed] access to [plaintiff’s servers] by using credentials fraudulently obtained from [the owners of the credentials]”). Defendants set up malicious imposter domains that are “homoglyphs” – using similar shapes, characters, and letters to imitate legitimate domains and email addresses impersonating one or more of the foregoing parties – which enables Defendants to deceive such parties into sending financial payments. Thus, any such access is without the victims’ and without Microsoft’s knowledge or consent. *See e.g. United States v. Nosal*, 844 F.3d 1024, 1039 (9th Cir. 2016) (“Had a thief stolen an employee’s password and then used it to rifle through [server resources], without doubt, access would have been without authorization.”). Finally, attempted intrusion into Microsoft’s customers’ O365 accounts is carried out for the purpose of soliciting fraudulent financial transactions. *See supra.* Finally, the amount of harm caused by Defendants exceeds $5,000. *See supra.*

Defendants’ conduct is precisely the type of activity that the Computer Fraud and Abuse Act is designed to prevent. *See, e.g.*, *Physicians Interactive v. Lathian Sys., Inc.,* No. CA 03-1193-A, 2003 WL 23018270, at *1 (E.D. Va. Dec. 5, 2003) (granting TRO and preliminary injunction under CFAA where defendant hacked into a computer and stole confidential information); *Glob. Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant actionable under the

CFAA); *see also United States v. Phillips,* 477 F.3d 215, 219 (5th Cir. 2007) (noting that CFAA is concerned with "outside hackers who break into a computer") (citations omitted).

Thus, Microsoft is likely to succeed on the merits of its CFAA claim.

2. Defendants' Conduct Violates the Stored Communications Act (18 U.S.C. § 2701)

The Stored Communications Act prohibits "intentionally access[ing] without authorization a facility through which electronic communications are provided" or doing so in excess of authorization, and, in so doing, obtaining, altering, or preventing authorized access to an electronic communication while it is in electronic storage. 18 U.S.C. § 2701(a). Microsoft's servers and its licensed operating system at end user computers are facilities through which electronic communication services are provided. Defendants' conduct violates the Stored Communications Act because Defendants use stolen credentials to gain unauthorized access to Office 365 accounts, monitor account activity, and identify additional victims either in the compromised O365 customer's business or their wider network (typically, customers, vendors, or agents), who routinely deal with wire transfer requests, invoices, or billing statements to target for fraudulent requests for payment imitating legitimate payment communications. Obtaining stored electronic information in this way, without authorization, is a violation of the Stored Communications Act. *See Council on Am.-Islamic Relations v. Gaubatz*, 667 F. Supp. 2d 67, 71-73 (D.D.C. 2009) (granting preliminary injunction in case where plaintiff brought claims under 18 U.S.C. § 2701 after defendant removed 12,000 internal, sensitive documents including emails and other documents and made video and audio recordings of private meetings and published this information); *Microsoft Corp. v. John Does 1-18*, 2014 WL 1338677, at *7 (E.D. Va. 2014) (finding violation of 18 U.S.C. § 2701 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"). Thus, Microsoft is likely to succeed on the merits of its claims.

3. Defendants' Conduct Violates the Virginia Computer Crimes Act (Virginia Code Ann. § 18.2-152.5:1, 18:2-152.4)

The Virginia Computer Crimes Act ("VCCA") makes it unlawful for any person with malicious intent or intentionally deceptive means and without authority to "[e]ffect the creation or alteration of a financial instrument or of an electronic transfer of funds" or "[u]se a computer or computer network to cause physical injury to the property of another" or "[u]se a computer or computer network to make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs or computer software residing in, communicated by, or produced by a computer or computer network." Va. Code § 18.2-152.4. A private right of action is available to any person or entity "whose property or person is injured by reason of a violation . . . regardless of whether such act is committed with malicious intent[.]" Va. Code 18.2-152.12(A). A person is "without authority" under the VCCA when "he knows or reasonably should know that he has no right, agreement, or permission or acts in a manner knowingly exceeding such right, agreement, or permission." Va. Code § 18.2-152.2. Those persons or entities with private rights of action under the VCCA may recover "any damages sustained and the costs of suit." *Id.*

For the same reasons discussed above, Defendants use stolen credentials to gain unauthorized access to Office 365 accounts, monitor email and account activity, forward communications involving key words relating to financial transactions, and target

Microsoft's O365 customer's business or their wider network (typically, customers, vendors, or agents), who routinely deal with wire transfer requests, invoices, or billing statements, to solicit financially fraudulent transactions. Defendants' conduct is unlawful and done without authority and damages Microsoft and its customers. Thus, Microsoft is likely to succeed on the merits of its claims.

4. Defendants' Conduct is Tortious

Defendants' conduct is tortious under the common law doctrines of conversion and trespass to chattels.

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." *Microsoft Corp. v. Does 1-2,* 2017 WL 5163363, at *5 (E.D. Va. Aug. 1, 2017), *report and recommendation adopted*, 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. *Id.*; *see also Vines v. Branch*, 418 S.E.2d 890, 894 (1992). Here, Defendants exercised dominion and authority over the accounts of Microsoft's O365 customers and used this access to solicit financially fraudulent transactions. These acts deprived Microsoft of its right to control the content, functionality, and nature of its 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*, 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).

Thus, Microsoft is likely to succeed on the merits of its common law claims.

B. Defendants' Conduct Causes Irreparable Harm

Defendants' conduct causes injury to Microsoft and its customers. There is a great risk that Microsoft's customers, whose credentials were stolen and accounts unlawfully accessed, and their businesses and larger networks of customers, vendors, and agents, who were targeted for financial fraud by Defendants, may incorrectly attribute Defendants' malicious activities and the result of those activities to Microsoft's products and services. Further, Defendants' ability to damage Microsoft's reputation extends even after they are detected and lose access to O365 since they can take their weaponized domains to other platforms and continue the attacks. Victims of Defendants' malicious attacks may incorrectly believe that Microsoft is the source of problems, harming customer relationships, or devaluing O365 as a platform, which further causes reputational injury to Microsoft – all because of Defendants' malicious activity and financial fraud.

These injuries are sufficient in and of themselves to constitute irreparable harm. In addition, Defendants are causing monetary harm that is unlikely to ever be compensated—even after final judgment—because Defendants are elusive cybercriminals whom Microsoft is unlikely to be able to enforce judgments against. "[C]ircumstances[] such as insolvency or unsatisfiability of a money judgment, can show irreparable harm." *Khepera-Bey v. Santander Consumer USA, Inc*., No. CIV. WDQ-11-1269, 2013 WL 3199746, at *4 (D. Md. June 21, 2013); *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*, No. 3:11-CR-00617-W, 2012 WL 181439, at *2 (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.").

C. The Balance of Equities Strongly Favor Injunctive Relief

Because Defendants are engaged in an illegal scheme to defraud consumers and injure Microsoft, the balance of equities clearly tips in favor granting an injunction. *See, e.g., US Airways, Inc. v. US Airline Pilots Ass'n,* 813 F. Supp. 2d 710, 736 (W.D.N.C. 2011); *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 and its customers caused by Defendants, while on the other side, Defendants can claim no legally cognizable harm because an injunction would only require Defendants to cease illegal activities. *US Airways,* 13 F. Supp. 2d at 736.

D. The Public Interest Favors an Injunction

It is clear that an injunction would serve the public interest here. Every day that passes, Defendants attempt to deceive many potential victims. An injunction will prevent Defendants from targeting Microsoft, its customers, and their larger networks for financial fraud. Moreover, the public interest is clearly served by enforcing statutes designed to protect the public, such as the CFAA and the Stored Communications Act. *See, e.g.*, *Dish Network LLC v. Parsons,* 2012 U.S. Dist. LEXIS 75386, at **8-9 (W.D.N.C. May 30, 2012) (public interest weighed in favor of injunction to enforce Stored Communications Act); *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).

Notably, most courts that have confronted requests for injunctive relief targeted at disabling malicious computer infrastructure, such as that used by botnets, which is very similar to the infrastructure used by Defendants, have granted such relief. *See generally* Welling Decl. Ex. 8-13 (citing cases where courts granted *ex parte* TRO and preliminary injunction against similar cyberattacks). Microsoft respectfully submits that the same result is warranted here.

E. The All Writs Act Authorizes the Court to Direct Third Parties to Perform Acts Necessary to Avoid Frustration of the Requested Relief

Microsoft's Proposed Order directs that the third-parties whose infrastructure Defendants rely on to operate Defendants' infrastructure reasonably cooperate to effectuate the order. Critically, these third parties are the primary entities that can effectively disable infrastructure, and thus their cooperation is necessary.

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). The Supreme Court has recognized that narrow direction to third parties necessary to effect the implementation of a court order is authorized by the All Writs Act:

> The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice, and encompasses even those who have not taken any affirmative action to hinder justice.

United States v. New York Tel. Co., 434 U.S. 159, 174 (1977) (order to telephone company to assist in implementation of a pen register warrant was authorized under the All Writs Act) (citations omitted); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398 at *30 (invoking All Writs act and granting relief similar to that requested herein); *United States v. X,* 601 F. Supp. 1039, 1042 (D. Md. 1984) (All Writs Act permits the district court to order a third party to provide "nonburdensome technical assistance" in aid of valid warrant); *Moore v. Tangipahoa Parish Sch. Bd*., 507 Fed. App'x. 389, 396 (5th Cir. 2013) (unpublished) ("The All Writs Act provides 'power [to] a federal court to issue such commands . . . as may be necessary or appropriate to effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained.'") (citing *New York Tel. Co*., 434 U.S. at 172); *see also In re Application of United States of Am. for an Order Authorizing An In-Progress Trace of Wire Commc'ns Over Tel. Facilities*, 616 F.2d 1122, 1129 (9th Cir. 1980) (same; noting of *New York Tel. Co*., 434 U.S. at 175, "the Court made the commonsense observation that, without the participation of the telephone company, 'there is no conceivable way in which the surveillance authorized could have been successfully accomplished'");

As the Second Circuit stated, "[a]n important feature of the All-Writs Act is its grant of authority to enjoin and bind non-parties to an action when needed to preserve the court's ability to reach or enforce its decision in a case over which it has proper jurisdiction." *In re Baldwin-United Corp*., 770 F.2d 328, 338-39 (2d Cir. 1985) ("[The Court does] not believe that Rule 65 was intended to impose such a limit on the court's authority provided by the All-Writs Act to protect its ability to render a binding judgment.").

Requiring these third parties to reasonably assist in the execution of this order will not offend Due Process as the Proposed Order (1) requires only minimal assistance from the third parties in executing the order (acts that they would take in the ordinary course of their operations), (2) requires that it be implemented with the least degree of interference with the normal operation of third parties, and (3) does not deprive the third parties of any tangible or significant property interests. If, in the implementation of the Proposed Order, any third party wishes to bring an issue to the attention of the Court, Microsoft will bring it immediately. The third parties will have an opportunity to be heard at the preliminary injunction hearing, which must occur shortly after the execution of the Proposed Order. Fed. R. Civ. P. 65(b)(2). The directions to third parties in the Proposed Order are thus narrow, satisfy Due Process, and are necessary to effect the requested relief and ensure that the relief is not rendered fruitless.

F. An *Ex Parte* TRO and Preliminary Injunction Is the Only Effective Means of Relief, and Alternative Service Is Warranted Under the Circumstances

The only way to practically effect relief in this case is to order the suspension of the domains at issue. Without this relief, Defendants will be able to continue their fraudulent schemes. The court has inherent equitable authority to craft a remedy that accomplishes mitigation of the injury caused by Defendants' conduct. *See CFTC v. Kimberlynn Creek Ranch, Inc.*, 276 F.3d 187, 193 (4th Cir. 2002) (district court possesses "inherent equitable powers to order preliminary relief … in order to assure the availability of permanent relief"). The TRO that Microsoft requests must issue *ex parte* for the relief to be effective at all because of the extraordinary factual circumstances here—namely, Defendants' technical sophistication and ability to move their malicious infrastructure if given advance notice of Microsoft's request for injunctive relief. Rule 65 of the Federal Rules of Civil Procedure permits an *ex parte* TRO where the moving party sets forth facts that show an immediate and irreparable injury and why notice should not be required. Fed. R. Civ. P. 65(b)(1); *see Granny Goose Foods, Inc. v. Brotherhood of Teamsters & Auto Truck Drivers, Local No. 70*, 415 U.S. 423, 439 (1974) ("Ex parte temporary restraining orders are no doubt necessary in certain circumstances….").

If notice is given prior to issuance of a TRO, it will render attempts to disable the infrastructure futile, Welling Decl. at ¶ 3, and undoubtedly facilitate efforts by the Defendants to continue to operate. It is well established that *ex parte* relief is appropriate under circumstances such as the instant case, where notice would render the requested relief ineffective. *See, e.g., AllscriptsMisys, LLC v. Am. Dig. Networks, LLC,* 1:10-cv-00111, 2010 U.S. Dist. LEXIS 4450, at *2 (D. Md. Jan. 20, 2010) (granting an *ex parte* TRO where "Defendant may dissipate the funds and/or take action to render it difficult to recover funds."); *Crosby v. Petromed, Inc*., No., 2009 WL 2432322, at *2 (E.D. Wash. Aug. 6, 2009) (granting *ex parte* TRO as "notice to Defendants of this TRO request could result in further injury or damage to Plaintiffs...."); *AT&T Broadband v. Tech Commc'ns, Inc*. 381 F.3d 1309, 1319-20 (11th Cir. 2004) (affirming *ex parte* search and seizure order to seize contraband technical equipment, given evidence that in the past defendants and persons similarly situated had secreted evidence once notice given); *Little Tor Auto Ctr. v. Exxon Co., USA*, 822 F. Supp. 141, 143 (S.D.N.Y. 1993) (*ex parte* TRO appropriate where contraband "may be destroyed as soon as notice is given"); *In re Vuitton Et Fils S.A*., 606 F.2d 1, 4-5 (2d Cir. 1979) (per curiam) (holding that notice prior to issuing TRO was not necessary where notice would "serve only to render fruitless further prosecution of the action"; prior experience taught that once one member of the counterfeiting enterprise received notice, contraband would be transferred to another unknown counterfeiter, perpetuating the harm and rendering judicial efforts pointless).

Defendants' techniques are designed to resist technical mitigation efforts, eliminating straightforward technical means to curb the injury being caused. Keating Decl. at ¶ 58. Further, when Defendants become aware of efforts to mitigate or investigate their activities, they take steps to conceal their activities, making it more difficult for victims to adequately assess the damage or take steps to mitigate that injury going forward. *Id.* When Defendants become aware of efforts to mitigate or investigate their activities, they take steps to conceal their activities and to conceal the injury that has been caused to victims, which makes *ex parte* relief appropriate. Particularly instructive here are cases such as *Microsoft v. John Does 1-2,* Case No. 1:19-cv-01582 (E.D. Va. 2019) and *Microsoft and FS-ISAC v. John Does 1-2,* Case No. 1:20-cv-1171 (E.D. Va. 2020), all cases in which the district court issued *ex parte* TROs, recognizing the risk that the defendants in those cases would have moved the botnet infrastructure and destroyed evidence if prior notice had been given. *See, e.g.,* Exs. 9, 13 to Welling Decl.

Similarly, the court in *Dell Inc. v. BelgiumDomains, LLC,* No. CIV. 07-22674, 2007 WL 6862341, at *1 (S.D. Fla. Nov. 21, 2007) issued an *ex parte* TRO against domain registrants where persons similarly situated had previously concealed such conduct and disregarded court orders by, *inter alia*, using fictitious businesses, personal names, and shell entities to hide their activities. *Id.* at *2. In *Dell*, the Court explicitly found that where, as in the instant case, Defendants' scheme is "in electronic form and subject to quick, easy, untraceable destruction by Defendants," ex parte relief is particularly warranted. *Id.*

To ensure Due Process, immediately upon entry of the requested *ex parte* TRO, Microsoft will undertake extraordinary efforts to effect formal and informal notice of the preliminary injunction hearing to Defendants and to serve the complaint.

Microsoft Will Provide Notice By E-mail, Facsimile And Mail: Microsoft has identified or will identify email addresses, mailing addresses and/or facsimile numbers provided by the Defendants, and will further identify such contact information pursuant to the terms of the requested TRO. Welling Decl. ¶ 10. Microsoft will provide notice of the preliminary injunction hearing and will affect service of the Complaint by immediately sending the same pleadings described above to the e-mail addresses provided to the hosting companies, registrars, and registries, and to any other email addresses, facsimile numbers and mailing addresses that can be identified. Welling Decl. ¶ 11. Based on Microsoft's investigation, it appears that the most viable means of contacting the Defendants are the email addresses used to register the domains at issue. When Defendants registered for domain names, they agreed not to engage in abuse such as that at issue in this case and agreed that notice of disputes regarding hosting could be provided to them by sending complaints to the e-mail, facsimile and mail addresses provide by them. *Id.* ¶ 24.

Microsoft Will Provide Notice To Defendants By Publication: Microsoft will notify the Defendants of the preliminary injunction hearing and the complaint against their misconduct by publishing the materials on a centrally located, publicly accessible source on the internet for a period of 6 months. *Id.* ¶ 11.

Microsoft Will Provide Notice To Defendants By Personal Delivery: Microsoft has identified domains names from which Defendants' infrastructure operates, and, pursuant to the TRO, will obtain from the domain registrars any and all physical addresses of the Defendants. Pursuant to Rules 4(e)(2)(A) and 4(f)(3), Microsoft plans to attempt formal notice of the preliminary injunction hearing and service of the complaint by hand delivery of the summons, Microsoft's Complaint, the instant motion and supporting documents, and any Order issued by this Court to such addresses in the United States, to the extent such are uncovered**.** *Id.* ¶ 13.

Microsoft Will Provide Notice By Personal Delivery And Treaty If Possible: If valid physical addresses of Defendants can be identified, Microsoft will notify Defendants and serve process upon them by personal delivery or through the Hague Convention on service of process or similar treaty-based means. *Id.* ¶ 14.

Notice and service by the foregoing means satisfy Due Process; are appropriate, sufficient, and reasonable to apprise Defendants of this action; and are necessary under the circumstances. Microsoft hereby formally requests that the Court approve and order the alternative means of service discussed above.

Legal notice and service by e-mail, facsimile, mail and publication satisfies Due Process as these means are reasonably calculated, in light of the circumstances, to apprise the interested parties of the TRO, the preliminary injunction hearing, and the lawsuit. *See Mullane v. Cent. Hanover Bank & Tr. Co.,* 339 U.S. 306, 314 (1950). Such methods are also authorized under Federal Rule of Civil Procedure 4(f)(3), which allows a party to serve defendants by means not prohibited by international agreement.

The methods of notice and service proposed by Microsoft have been approved in other cases involving international defendants attempting to evade authorities. *See e.g.*, *Rio Properties, Inc. v. Rio Int'l Interlink,* 284 F.3d 1007, 1014-1015 (9th Cir. 2002) (authorizing service by e-mail upon an international defendant); *Microsoft Corp.*, 2014 WL 1338677, at *3 (finding service was proper where plaintiff sent "copies of the original Complaint, Russian translations, a link to all pleadings, and the TRO notice language to all email addresses associated with the Bamital botnet command and control domains" and "published in English and Russian the Complaint, Amended Complaint, Summons, and all orders and pleadings in this action at the publicly available website www.noticeofpleadings.com") (citing Fed. R. Civ. P. 4(f)(3)); *AllscriptsMisys, LLC,* 2010 U.S. Dist. LEXIS 4450, at *3 (granting ex parte TRO and order prompting "notice of this Order and Temporary Restraining Order as can be effected by telephone, electronic means, mail or delivery services."); *Bazarian Int'l Fin. Assocs., L.L.C. v. Desarrollos Aerohotelco, C.A.,* 168 F. Supp. 3d 1, 13-16 (D.D.C. 2016) (noting Rule 4(f) is "concerned with providing a method of service that is reasonably calculated to 'notif[y] a defendant of the commencement of an action against him" and upholding service through U.S. counsel).

Such service is particularly warranted in cases such as this involving internet-based misconduct, carried out by international defendants, causing immediate, irreparable harm. As the Ninth Circuit observed:

> [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 e-mail-the method of communication which [Defendant] utilizes and prefers. In addition, e-mail was the only court-ordered method of service aimed directly and instantly at [Defendant] ... Indeed, when faced with an international e-business scofflaw, playing hide-and-seek with the federal court, e-mail may be the only means of effecting service of process.

Rio Properties, Inc., 284 F.3d at 1018. Notably, *Rio Properties* has been followed in the Fourth Circuit. *See FMAC Loan Receivables*, 228 F.R.D. at 534 (following *Rio*); *BP Products N. Am., Inc. v. Dagra*, 232 F.R.D. 263, 264 (E.D. Va. 2005) (same); *Williams v. Adver. Sex LLC*, 231 F.R.D. 483, 486 (N.D. W. Va. 2005) ("The Fourth Circuit Court of Appeals has not addressed this issue. Therefore, in the absence of any controlling authority in this circuit, the Court adopts the reasoning of the Ninth Circuit in *Rio Properties, Inc.*").

In this case, the e-mail addresses provided by Defendants to the hosting companies and domain registrars, in the course of obtaining services that support Defendants are likely to be the most accurate and viable contact information and means of notice and service. Moreover, Defendants will expect notice regarding their use of the hosting providers' and domain registrars' services to operate Defendants by those means, as Defendants agreed to such in their agreements. *See Nat'l Equip. Rental, Ltd. v. Szukhent,* 375 U.S. 311, 315-16 (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.").

For these reasons, notice and service by e-mail and publication are warranted and necessary here.[3]

For all of the foregoing reasons, Microsoft respectfully requests that the Court enter the requested TRO and Order to Show Cause why a preliminary injunction should not issue, and further order that the means of notice of the preliminary injunction hearing and service of the complaint set forth herein meet Fed. R. Civ. Pro. 4(f)(3) satisfy Due Process and are reasonably calculated to notify Defendants of this action.

IV. CONCLUSION

For the reasons set forth herein, Microsoft respectfully requests that this Court grant the instant motion for a TRO and issue an order to show cause regarding a preliminary injunction. Microsoft further respectfully requests that the Court permit notice of the preliminary injunction hearing and service of the Complaint by alternative means.

[3] Additionally, if the physical addressees provided by Defendants to domain registrars turn out to be false and Defendants' whereabouts are unknown, the Hague Convention will not apply in any event and alternative means of service, such as email and publication, would be appropriate for that reason as well. *See BP Prods. N. Am., Inc.,* 236 F.R.D. 270, 271 ("The Hague Convention does not apply in cases where the address of the foreign party to be served is unknown.").

Dated: July 13, 2021

Respectfully submitted,

Julia Milewski (VA Bar No. 82426)
Matthew Welling (*pro hac vice pending*)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
jmilewski@crowell.com
mwelling@crowell.com

Gabriel M. Ramsey (*pro hac vice pending*)
Kayvan M. Ghaffari (*pro hac vice pending*)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Telephone: (415) 986-2800
Fax: (415) 986-2827
gramsey@crowell.com
kghaffari@crowell.com

Attorneys for Plaintiff Microsoft Corporation