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: 1:20cv730

FILED UNDER SEAL PURSUANT TO LOCAL CIVIL RULE 5

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 Corp. ("Microsoft") seeks an emergency *ex parte* temporary restraining order ("TRO") and a preliminary injunction to stop cybercriminals from exploiting the COVID-19 pandemic in an attempt to steal information from Microsoft customers. Specifically, Microsoft respectfully seeks an order from this Court to halt the operation and growth of an online criminal network that sends phishing emails containing deceptive messages concerning the global COVID-19 pandemic or other socially engineered lures in order to induce targeted victims to click on malicious links in those emails. These phishing emails are designed to look like they come from an employer or other trusted source. Defendants also deceptively use Microsoft trademarks and brands in these emails in order to induce victims to click on the links.

Microsoft seeks to stop Defendants' illegal conduct, including its efforts to obtain unlawful access to Office 365 accounts and obtain sensitive communications from within the accounts. Defendants use domain names listed at **Appendix A** to orchestrate criminal activity on a global scale:

- Defendants use this infrastructure to deceive victims into clicking on links or otherwise interacting with malicious applications to attempt gain unauthorized access to the victims' online accounts.
- Defendants use this infrastructure to target victims' online accounts, to attempt theft of information from those accounts.
- Defendants hide behind this infrastructure, using the anonymity of the internet to conceal their locations and identities while causing injury to Microsoft and reaping illicit benefits through the continuing operation of the infrastructure.

Defendants cause great injury to Microsoft by damaging the products that Microsoft licenses to its customers and by exploiting Microsoft's famous and highly-regarded trademarks, products, and services to disguise and further Defendants' criminal conduct. 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 or use of harmful online infrastructure used by unidentified defendants for illegal operations. Courts in at least thirteen cases involving Microsoft and other plaintiffs have granted such extraordinary relief to deny defendants access to or use of harmful online infrastructure. For example, just last month, 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) (Ex. 17 to Declaration of Matthew Welling In Support Of Plaintiffs' Motion For TRO ("Welling Decl."). 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

[1] *See Microsoft v. John Does, 1-11*, No. 11CV00222 (W.D. Wash. Feb. 9, 2011) (Robart, J.), Dkt. No. 27 (involving the "Rustock" botnet); *Microsoft v. Piatti, et al.,* Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.), Dkt. No. 14 (involving the "Kelihos" botnet); *Microsoft Corp. et al. v. John Does 1-39 et al.*, No. 12-cv-1335 (E.D.N.Y. June 29, 2012) (Johnson, J.), Dkt. No. 11 (involving the "Zeus" botnets); *Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.), Dkt. No. 20 (involving the "Nitol" botnet); *Microsoft Corp. v. John Does 1-18 et al.,* No. 1:13CV139, 2013 WL 600512 (E.D. Va. Jan. 31, 2013) (Brinkema, J.), Dkt. No. 23 (involving the "Bamital" botnet); *Microsoft v. John Does 1-82 et al.*, No. 3:13-cv-319- (W.D.N.C. June 10, 2013) (Mullen, J.), Dkt. No. 11 (involving the "Citadel" botnets); *Microsoft Corp. v. John Does 1-8 et al.,* Case No. A13-cv-1014-SS (W.D. Tex. 2013) (Sparks, J.), Dkt. No. 17 (involving the "ZeroAccess" botnets.); *Microsoft et al. v. John Does 1-8*, No. 1:14-cv-811, 2015 WL 4937441 (E.D. V.a Aug. 17. 2015) (O'Grady, J.), Dkt. No. 16 (involving the "Shylock" botnets); *Microsoft v. John Does 1-5,* Case No. 1:15-cv-240-LMB/IDO (E.D. Va. 2015), Dkt. No. 27 (Brinkema, J.) (involving the "Ramnit" botnet); *Microsoft v. John Does 1-2,* Case No. 1:16-cv-993 (E.D. Va. 2016) (Lee, J.) (involving the "Strontium" botnet); *Microsoft v. John Does 1-2,* Case No. 1:19-cv-00716 (D.D.C. 2019) (Berman, Jackson, J.) (involving the "Phosphorus" network); *Microsoft v. John Does 1-2,* Case No. 1:19-cv-01582 (E.D. Va. 2019) (O'Grady, J.) (involving the "Thallium" network) (sample of recent orders attached as Exs. 10-17 to Appendix B to Welling Decl.).

hosting companies that provide Defendants' infrastructure.

I. STATEMENT OF FACTS

Defendants send phishing emails containing deceptive messages concerning the global COVID-19 pandemic in order to induce targeted victims to click on malicious links in those emails. Declaration of Peter Anaman ("Anaman Decl."), ¶ 3. These emails are designed to look like they come from an employer or other trusted source. *Id.* Once the victims click on the malicious links, they are led to servers which present the victims with a malicious Web Application ("Web App").[2] *Id.* Having convinced the victims that the original phishing email was sent by a trusted source, the criminals then cause the victims to erroneously believe that the Web App also originates from the same trusted source and, most importantly, is approved or published by Microsoft. As a result, targeted victims are deceived into clicking a button that grants the malicious Web App, and therefore the criminals, access to the victims' Office 365 account including the account contents, such as email, contacts, notes and material stored in the victims' OneDrive for Business cloud storage space and corporate SharePoint document management and storage system. The attacker may also be able to access and alter account settings as the attacker has full control over the account. Until the Web App is disabled or token revoked, the attacker will have continued access to the Office 365 account. *Id.*

In this way, the attackers attempt to gain unauthorized access to Office 365 accounts of Microsoft's customers. Notably, as more fully described below, this scheme enables unauthorized access without explicitly requiring the victims to directly give up their login credentials at a fake website or similar interface. *Id.* ¶ 4. Rather, the victims input their credentials into legitimate Office 365 login pages that are not under the cybercriminals' control.

[2] For clarity, the references here to a "Web App" do not relate to mobile apps. Rather, the Web App is software running on servers controlled by Defendants and which can interact with and obtain access to Microsoft Office 365 accounts.

In some instances, the victim may alternatively be asked to confirm the identity linked to their device in lieu of entering credentials. Thereafter, the cybercriminals utilize the malicious Web Apps to gain access based on the victims' previous entry of credentials. *Id.* This highly deceptive scheme has the same practical effect as direct theft of credentials, except that the victims are not aware that they unintentionally provided cybercriminals access to their Office 365 account. *Id.* Defendants attempted to target Microsoft customers in both the private and public sectors, including businesses in different industries. *Id.* ¶ 8. Defendants frequently targeted the C-suite, senior managers, and regional leaders of a variety of businesses and organizations.

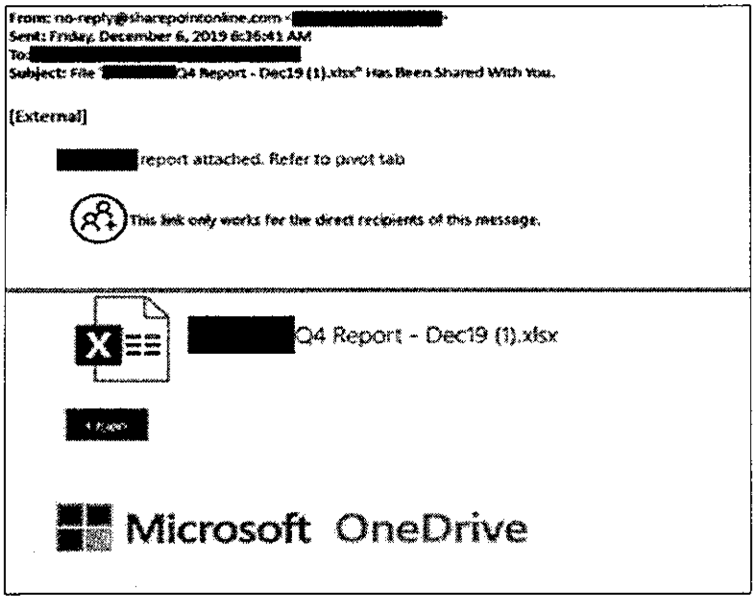
In December 2019, Microsoft first detected early instances of the Defendants' malicious phishing and Web App scheme. *Id.* ¶ 6. Based on patterns discovered at that time, Microsoft developed technical means to block the Defendants' activity and disabled the Web Apps that existed at that time. *Id.* In this way, Microsoft was, thus far, able to protect its customers. *Id.* However, recently, Defendants have begun creating new malicious Web Apps. Defendants' activities pose a persistent risk. *Id.* In just one week, Defendants sent phishing emails to millions of Office 365 users. Defendants continue to evolve their tactics, now leveraging messages purporting to be about important COVID-19 issues. *Id.* Defendants have designed these COVID-19-themed phishing emails, like the previous emails, to deceive recipients to click on a link and thereafter grant access to their Office 365 accounts via new versions of the malicious Web Apps. *Id.*

Defendants Use Deceptive COVID-19 Messages and Malicious Web Apps in an Attempt to Compromise Office 365 Accounts

Defendants send phishing emails to Microsoft's customers who are using its Office 365 email service. *Id.* ¶ 16. Defendants design these emails in a manner that deceptively impersonates legitimate communications originating from Microsoft's SharePoint or OneDrive for Business cloud storage services. *Id.* For example, in these emails, Defendants leverage the presence of the "Microsoft" and "OneDrive" trademarks, and the presence of the term "SharePoint" in the "From" email address to convince recipients that this is a legitimate communication from Microsoft. *Id.* Further, Defendants send phishing emails from email addresses that contain references to companies or entities associated with the recipient, such as the name of their employer. Defendants may send phishing emails from compromised accounts of parties, such as employers or colleagues, within the recipient's trusted network. *Id.*

Defendants also include in the phishing emails other deceptive content, usually what appears to be a link to "Open" a Microsoft Excel document. *Id.* ¶ 17. In fact, this icon in the email is a malicious link that begins the process of Defendants attempting to obtain access to the victims' Office 365 accounts. Because victims are usually familiar and experienced with the legitimate file-share method using OneDrive for Business or SharePoint, and because the email appears to originate from a trusted entity (such as an employer) and contains typical data that might appear in a legitimate file-sharing email, the victims are tricked into clicking the malicious link. *Id.*

When Defendants first began carrying out this scheme, the phishing emails contained deceptive themes associated with generic business activity. *Id.* ¶ 18. For example, the malicious Excel link would be named in a manner that uses information suggesting it is associated with a trusted entity and business terms such as "Q4 Report – Dec19." *Id.* ¶ 19. An example of an earlier phishing email is reproduced as **Figure 1**:



From: no-reply@sharepointonline.com <[redacted]>
Sent: Friday, December 6, 2019 6:36:41 AM
To: [redacted]
Subject: File "[redacted]Q4 Report - Dec19 (1).xlsx" Has Been Shared With You.

[External]

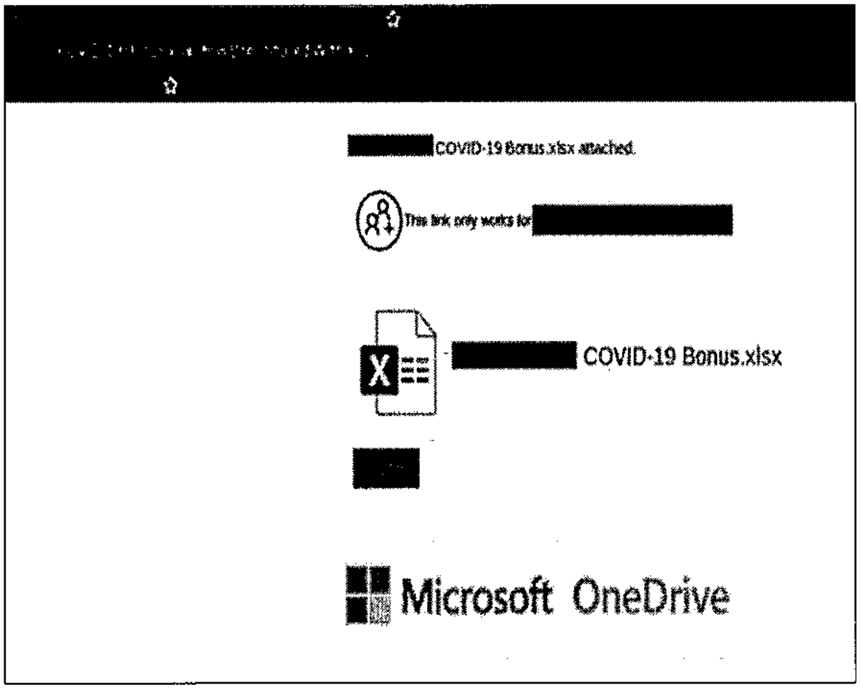
[redacted] report attached. Refer to pivot tab

This link only works for the direct recipients of this message.

[redacted]Q4 Report - Dec19 (1).xlsx

Figure 1

Recently, as Defendants have renewed their efforts to target Microsoft and its customers, Defendants have created phishing emails containing deceptive themes associated with COVID-19. *Id.* ¶ 20. For example, Defendants now name the malicious Excel link in a manner suggesting it is associated with a trusted entity and use terms such as "COVID-19 Bonus." *Id.* . An example of a such a COVID-19 related phishing email is reproduced as **Figure 2**:



[redacted]COVID-19 Bonus.xlsx attached.

This link only works for [redacted]

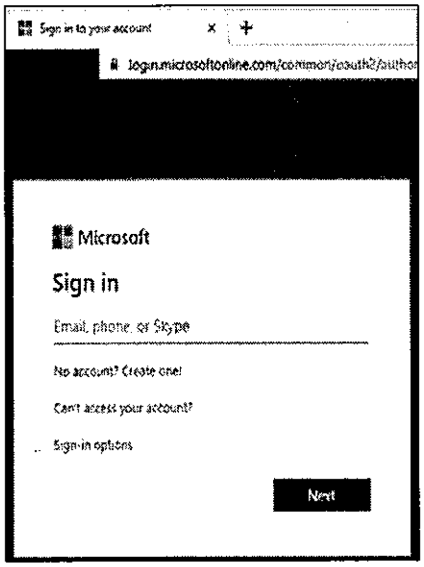
[redacted] COVID-19 Bonus.xlsx

Figure 2

The scale of these phishing attacks is immense. In just one week, Defendants sent phishing emails to millions of Office 365 users. The scale of Defendants' attempts to reach potential victims and Defendants' ability to continuously create and deploy new malicious Web Apps from existing infrastructure, discussed below, demonstrates the substantial ongoing risk posed by Defendants. *Id.* ¶ 22.

Defendants Attempt to Access Office 365 Through Malicious Web Apps

After Defendants socially engineer the victim to click the link in the body of the email, the victim is then prompted to sign into Microsoft's legitimate Office 365 portal at login.microsoftonline.com. *Id.* ¶ 23. The login portal presented to the victim at this point is reflected at **Figure 3** below, where the victim enters their user name, and at **Figure 4**, where the victim enters their password:


Sign in to your account

login.microsoftonline.com/common/oauth2/authoi

[redacted]

Microsoft

Sign in

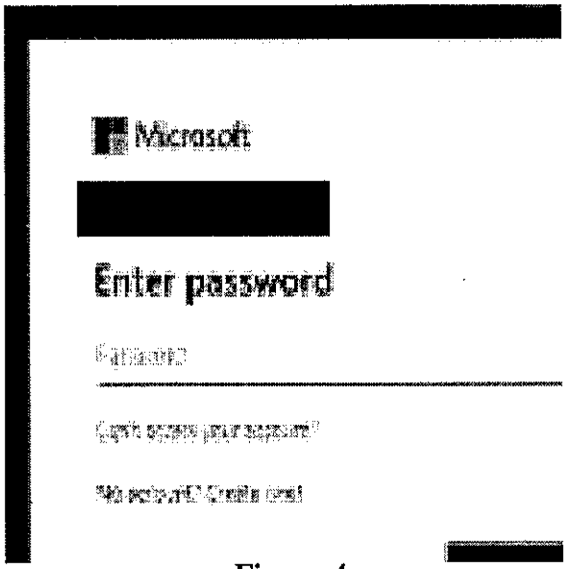
Email, phone, or Skype

No account? Create one!

Can't access your account?

Sign-in options

Figure 3


[redacted]

Microsoft

[redacted]

Enter password

Password

Can't access your account?

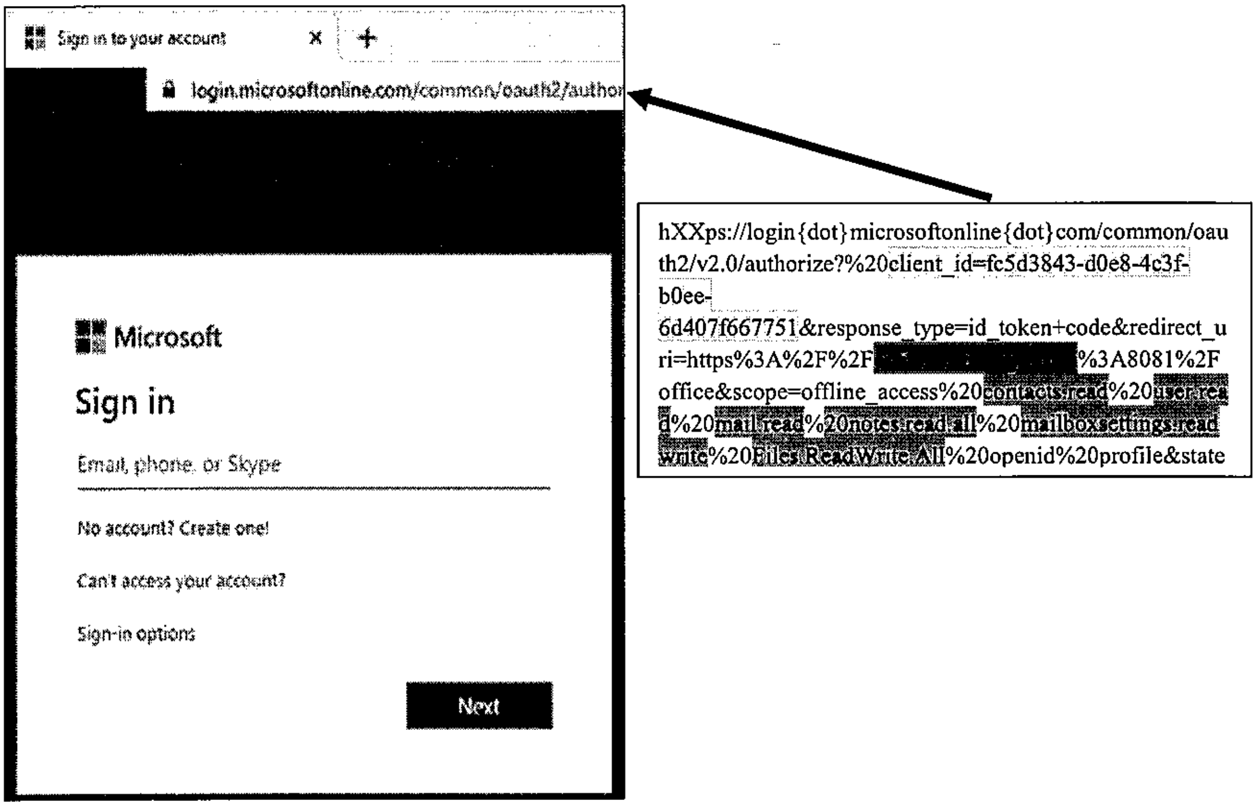
No account? Create one!

[redacted]

Figure 4

Once the Microsoft identity platform recognizes the credentials, the Defendants leverage an industry standard technical facility used by Microsoft known as "OAuth 2.0" to request access to victims' Office 365 accounts and to deceive victims into providing such access. *Id.* ¶ 24. The following describes the process by which Defendants misuse OAuth 2.0 to obtain access to victims' Office 365 accounts. *Id.*

The first step in Defendants' misuse of OAuth 2.0 involves processing information contained within the URL that the Defendants used in the phishing email to take the victim to the legitimate Office 365 portal. *Id.* ¶ 25. That URL contains additional information that defines the level of access requested by the malicious Web App and to be granted by the unsuspecting user. *Id.* As seen in **Figure 5** the malicious URL contains several elements, highlighted below:



hXXps://login{dot}microsoftonline{dot}com/common/oauth2/v2.0/authorize?%20client_id=fc5d3843-d0e8-4c3f-b0ee-6d407f667751&response_type=id_token+code&redirect_uri=https%3A%2F%2F[redacted]%3A8081%2Foffice&scope=offline_access%20contacts.read%20user.read%20mail.read%20notes.read.all%20mailboxsettings.readwrite%20Files.ReadWrite.All%20openid%20profile&state

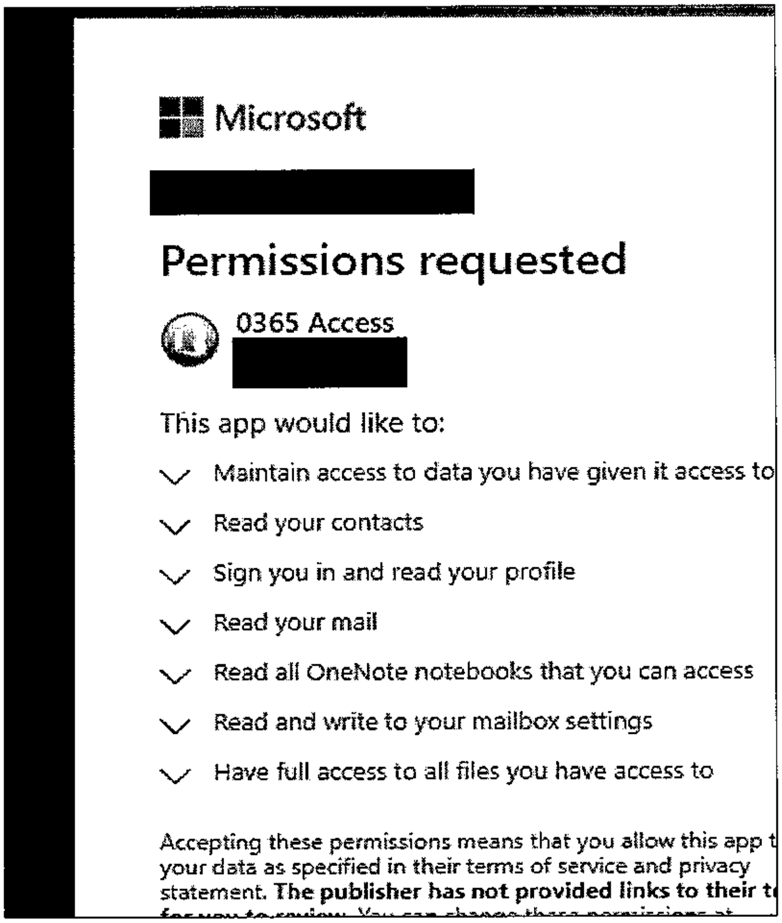
Figure 5

First, the malicious URL contains a parameter called **"client_id"** (highlighted in yellow above). The "client_id" is an identifier which is processed by the OAuth 2.0 facility to identify the Defendants' malicious Web App. *Id.* ¶ 26.

Second, the malicious URL contains a domain name, in this case "**officeinventorys.com**" (highlighted in green above). That is a domain name controlled by Defendants and one of the domain names that is the subject of this action. The Defendants' malicious Web App is hosted on servers associated with this domain name. *Id.* ¶ 27. In addition, once the user is deceived into accepting the Web App, authorization codes and/or tokens are sent to the servers associated with this domain name. *Id.*

Third, the malicious URL contains other access parameters that operate as instructions regarding what Office 365 resources to access. Highlighted in blue in the example above are parameters that define the level of access to Office 365 "**mail**," "**contacts**," "**files**" and "**notes**". Further, the parameters define access to "**read**" those resources and to "**write**" (*i.e.* make changes to) Office 365 mailbox settings and files. Access is only granted once the unsuspecting user accepts an OAuth 2.0 request, as discussed further below. *Id.* ¶ 28.

Upon login, the Defendants cause the OAuth 2.0 facility to use the "client_id" and the access parameters noted above to produce a deceptive user interface that displays the name of the malicious Web App and displays a list of access levels for which the malicious Web App is requesting consent. *Id.* ¶ 29. Defendants leverage this user interface in a manner that deceptively presents the trademark "Microsoft" and the deceptive formulation "0365," designed to look like the genuine Office 365. *Id.* The deceptive Web App user interface, which the victim still believes to be an authorized process associated with a trusted entity (such as an employer), requests the victim to grant the following permissions regarding Office 365 access: read contacts, read user profile, read user emails, modify mailbox settings (i.e. forwarding rules) and all files. *Id.* An example of a deceptive Web App user interface is shown at **Figure 6**.



Microsoft

[redacted]

Permissions requested

0365 Access

[redacted]

This app would like to:

- Maintain access to data you have given it access to
- Read your contacts
- Sign you in and read your profile
- Read your mail
- Read all OneNote notebooks that you can access
- Read and write to your mailbox settings
- Have full access to all files you have access to

Accepting these permissions means that you allow this app t your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their t**

Figure 6

After the user clicks "Accept," the OAuth 2.0 system generates an authorization code which is subsequently redeemed for one or more authentication tokens for that victim. This authentication token effectively serves the same function as the victim's credentials, communicating to the OAuth 2.0 system that the victim is authorized to have access to Office 365 account. In this way, the attacker is able to access the compromised Office 365 accounts by enabling the malicious Web App to gain access to the account in accordance with designated access parameters indicated in the graphical user interface depicted in Figure 6. *Id.* ¶ 31.

In this way, Defendants deceive victims to not only log into Office 365 and generate needed OAuth 2.0 tokens, but to further click on the "Accept" button, providing Defendants unauthorized access to defined resources within the Office 365 account. *Id.* ¶ 32. In this case, the victim will have granted access to all of the resources set forth above in Figure 6. *Id.* Once Defendants deceive the victim into clicking "Accept," the OAuth 2.0 facility sends the previously generated OAuth 2.0 token and associated permissions to the Defendants' malicious Web App located at the Defendants' malicious domain name ("officeinventorys.com" in the example above). *Id.* Once the malicious Web App receives the OAuth 2.0 token and associated permissions, this enables the Defendants to use the malicious Web App to make API calls to access the victim's Office 365 account. *Id.* In accessing Microsoft's Office 365 servers in this way, Defendants are accessing, without valid authorization, computers that can be used in interstate commerce. *Id.*

If Defendants were able to successfully access the content of Office 365 accounts pursuant to this phishing attack, it would be possible for them to carry out activities such as sending deceptive emails from the compromised user, monitoring communications and transactions in order to carry out wire fraud or other forms of fraud, or simply stealing further financial credentials, account credentials or other valuable information that may be available. *Id.* ¶ 33.

Defendants' Harmful Domain Names Used to Carry Out Attacks Against Microsoft Office 365 Accounts

Defendants use various domain names to host and deliver malicious Web Apps. Defendants have also registered domain names to prepare for other illegal activities, such as attempts to access the content of victims' emails. The following are domain names that Defendants are currently leveraging in their infrastructure, each of which is a .COM top-level domain (TLD) operated by Verisign as the Internet Corporation for Assigned Names and Numbers (ICANN) accredited registry within the Eastern District of Virginia. *Id.* ¶ 34.

Domain Names	Domain Registry	Registry Operator	Registry Location	Domain Registrar	Registrar Location
officeinventorys.com	.COM	Verisign	VA, United States	NameCheap, Inc.	AZ, United States
officehnoc.com	.COM	Verisign	VA, United States	NameCheap, Inc.	AZ, United States
officesuited.com	.COM	Verisign	VA, United	NameCheap, Inc.	AZ, United

			States		States
officemtr.com	.COM	Verisign	VA, United States	NameCheap, Inc.	AZ, United States
officesuitesoft.com	.COM	Verisign	VA, United States	NameCheap, Inc.	AZ, United States
mailitdaemon.com	.COM	Verisign	VA, United States	GoDaddy.com, LLC	AZ, United States

As can be seen, many of these domain names are masquerades of Microsoft's Office products and services, such as "officeinventorys.com", "officesuitesoft.com", and "officehnoc.com". *Id.* ¶ 35. This approach is consistent with the deceptive nature of the fraud targeting Office 365. *Id.* These domain names are used to create malicious Web Apps, consistent with their deceptive theme. *Id.* Defendants also registered the domain name "mailitdaemon.com," which has been and is used to receive mail forwarded by Office 365 accounts successfully compromised by Defendants. *Id.* In this domain name, Defendants use generic nomenclature seen in regular network administration, such as "mail," "IT" (information technology) and "daemon" (a process used in an email server). *Id.*

Harm to Microsoft and Microsoft Customers

Microsoft® is a provider of the Office 365,® OneDrive,® and SharePoint® cloud-based business and productivity suite of services, all offered under those trademarks and in connection with the Microsoft mark and the Microsoft corporate logo. Microsoft has invested substantial resources in developing high-quality products and services. *Id.* ¶ 41. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. *Id.* Microsoft has registered trademarks representing the quality of its products and services and its brand, including the Microsoft, Office 365, OneDrive and SharePoint trademarks. *Id.*

Defendants use these trademarks, brands and confusingly similar variants in phishing emails and web interfaces presented to Microsoft's customers and potential victims. Defendants' use of Microsoft trademarks and brands is meant to confuse and does cause confusion among Microsoft's customers and recipients of these communications, as those parties incorrectly perceive a relationship between Microsoft and the malicious activities of Defendants. *Id.* ¶ 42.

Defendants activities' dilute and tarnish the value of these Microsoft trademarks and brands. The activities carried out by Defendants, described above, injure Microsoft and its reputation, brand and goodwill because victims targeted by this scheme are likely to incorrectly believe that Microsoft is the source of problems caused by Defendants. *Id.* ¶ 43. Microsoft is similarly injured because Defendants direct their attempted intrusions to accounts hosted on Microsoft's servers. *Id.* ¶ 44. Microsoft must bear this extraordinary burden. Microsoft must develop technical countermeasures and defenses, to suppress Defendants' activities, respond to customer service issues caused by Defendants and must expend substantial resources dealing with the injury and confusion. *Id.* Microsoft has had to expend substantial resources to resist the ongoing attempted attacks on its infrastructure, products, services, and customers. *Id.* Given that Defendants are continuing their targeting of Microsoft, and that such will be ongoing, this poses severe risk of injury to Microsoft, in that it ultimately threatens Microsoft's brands and customer relationships. *Id.*

II. LEGAL STANDARD

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. MICROSOFT'S REQUESTED RELIEF IS WARRANTED

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 steal victims' access tokens and their sensitive and confidential information, and 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 accesser 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. Peter Anaman'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, Defendants' malicious Web Apps and the associated scheme are designed to access such computers, particularly Microsoft's Office 365 servers and associated user accounts, without authorization. Defendants deceive victims to take actions that enable such access, but without the victims understanding the nature of Defendants' activity. 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.").

In Defendants' scheme, a stolen access token—procured by fraud—is effectively the same as the CFAA cases involving actionable stolen credentials. An access token acts as a security authentication mechanism to provision access to computing resources and data in a manner that is technically and practically analogous to a password, and is technically and practically analogous. Thus, fraudulently obtaining control over an access token to obtain access to a protected computer violates the CFAA. For example, in one case the court recognized a CFAA claim where defendant "gain[ed] access to [plaintiff's servers] by using credentials fraudulently obtained from [the owners of the credentials]." *Elsevier Inc. v. WWW.Sci-Hub.org*, 2015 U.S. Dist. LEXIS 147639, at *5 (S.D.N.Y. Oct. 28, 2015)

Finally, attempted intrusion into Microsoft customer accounts is carried out for the purpose of obtaining user credentials and sensitive information and for the purpose of defrauding users. *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 to legislative history omitted).

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

2. Defendants' Conduct Violates the Lanham Act

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 JFJ Toys, Inc. v. Sears Holdings Corp.,* 237 F. Supp. 3d 311, 340 (D. Md. 2017) (citing 15 U.S.C. § 1114(1)(a)). Defendants distribute copies of Microsoft's registered, famous and distinctive trademarks in fraudulent schemes designed to mislead victims into clicking on malicious links or otherwise interacting with malicious Web Apps, causing the victims confusion and causing them to mistakenly associate Microsoft with this activity.

Defendants make use of counterfeit reproductions of Microsoft's marks, *inter alia*, by causing the deceptive use of such marks in phishing emails, domain names and Web App interfaces. Defendants' creation and use of counterfeit trademarks in connection with such severe fraud is likely to cause confusion and mistake and to deceive consumers. 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).

In addition to constituting infringement under section 1114 of the Lanham Act, Defendants' conduct also constitutes false designation of origin under section 1125(a), which prohibits use of a registered mark that:

> is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person.

15 U.S.C. § 1125(a)(1)(A). Defendants' misleading use of Microsoft's trademarks causes confusion by deceptively suggesting an affiliation between Microsoft and Defendants' malicious conduct. *See supra*. This activity is a clear violation of Lanham Act § 1125(a), and Microsoft is likely to succeed on the merits. *See Garden & Gun, LLC v. TwoDalGals, LLC*, 2008 WL 3925276, at *1 (W.D.N.C. Aug. 21, 2008) (granting preliminary injunction against misleading use of trademarks under Section 1125(a)); *Brookfield Commc'ns, Inc. v. W. Coast Entm't Corp.*, 174 F.3d 1036, 1065 (9th Cir. 1999) (entering preliminary injunction under Lanham Act §1125(a) for infringement of trademark in software and website code); *Hotmail Corp. v. Van$ Money Pie Inc.*, 1998 WL 388389, at *5 (N.D. Cal. Apr. 16, 1998) (granting preliminary injunction; copying the Hotmail trademarks in "e-mail return

addresses" constituted false designation of origin; also constituted trademark "dilution" under §1125(c)).

Thus, Microsoft is likely to succeed on the merits of its Lanham Act claims.

3. <u>Defendants' Conduct is Tortious</u>

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

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 Microsoft's proprietary Office 365 property by intruding into the Office 365 technical login facilities and servers. These acts deprived Microsoft of its right to control the content, functionality, and nature of those servers 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*, 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).

Further, Defendants' conduct amounts to unjust enrichment because plaintiff has demonstrated that (1) plaintiffs conferred a benefit on the defendant; (2) defendant's knowledge of the conferring of the benefit; and, (3) defendant's 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 4937441, at *12.

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

B. <u>Defendants' Conduct Causes Irreparable Harm</u>

It is well-settled that consumer confusion and injury to business goodwill constitute irreparable harm. *See 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"); *Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.*, 22 F.3d 546 (4th Cir. 1994)), *abrogated on other grounds*, *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 24, 129 S. Ct. 365, 376, 172 L. Ed. 2d 249 (2008). A finding of irreparable harm usually follows a finding of unlawful use of a trademark and a likelihood of confusion. *Ledo Pizza Sys., Inc. v. Singh*, 2013 WL 5604339, at *3 (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 … where likelihood of confusion is established likelihood of success on the merits as well as risk of irreparable harm follow.").

Here, Defendants tarnishes Microsoft's valuable trademarks, injuring Microsoft's reputation and customer goodwill, creating confusion as to the source of Defendants' malicious activity and false messages. Defendants' actions damage Microsoft's reputation and confidence in Microsoft's services. 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. <u>The Balance of Equities Strongly Favor Injunctive Relief</u>

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 successfully intruding upon the millions of individuals targeted by Defendants' phishing and Web App scheme. 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); *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 ECPA); *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. (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."); *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).

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, (3) does not deprive the third parties of any tangible or significant property interests and (4) requires Microsoft to compensate the third parties for the assistance rendered. 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 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, Anaman Decl. at ¶ 50, 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. Anaman Decl. at ¶ 50. 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 Corp. v. John Does 1-27* and *Microsoft Corp. v. Piatti*, 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. 10-17 to Welling Decl.

Similarly, in *FTC v. Pricewert LLC*, the district court issued an *ex parte* TRO suspending internet connectivity of a company enabling botnet activity and other illegal computer-related conduct on the basis that "Defendant is likely to relocate the harmful and malicious code it hosts and/or warn its criminal clientele of this action if informed of the [plaintiff's] action." *See* Exs. 8-9 to Welling Decl. (*FTC v. Pricewert LLC et al.*, Case No. 09-2407) (*Ex Parte* TRO and preliminary injunction disconnecting service to botnet hosting company at 3)). Moreover, 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. *Id.* 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.* ¶¶ 8-9.

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, publically 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: June 30, 2020

Respectfully submitted,

Julia Milewski (VA Bar No. 82426)
Matthew Welling (*pro hac vice*)
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*)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Telephone: (415) 986-2800
Fax: (415) 986-2827
gramsey@crowell.com

Attorneys for Plaintiff Microsoft Corporation