IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

MICROSOFT CORPORATION, a Washington corporation, FS-ISAC, INC., a Delaware Corporation, HEALTH-ISAC, INC., a Florida corporation, Plaintiffs, v. DENIS MALIKOV, and JOHN DOES 1-7, Defendants.	)	Civil Action No: **FILED UNDER SEAL**

NOTICE OF HEARING RE APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Please take notice that should the Court find it appropriate to hear oral argument on Plaintiffs' Application for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction, Plaintiffs respectfully requests oral argument to be set for Tuesday, April 5, 2022 at 10:00 a.m., or as soon as the matter may be heard.

Dated: April 4, 2022

Respectfully submitted,

/s/ Joshua D. Curry
Joshua D. Curry

Joshua D. Curry (Georgia Bar No. 117378)
Jonathan D. Goins (Georgia Bar No. 738593
LEWIS BRISBOIS BISGAARD & SMITH LLP
600 Peachtree Street NE, Suite 4700
Atlanta, GA 30308
Tel: 404.348.8585
Fax: 404.467.8845
josh.curry@lewisbrisbois.com
jonathan.goins@lewisbrisbois.com

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

Emily Alban (*pro hac vice*)
Garylene Javier (*pro hac vice*)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Tel: (202) 624-2500
Fax: (202) 628-5116
ealban@crowell.com
gjavier@crowell.com

Richard Domingues Boscovich
(*pro hac vice*)
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399
Tel: (425) 704-0867
Fax: (425) 936-7329
rbosco@microsoft.com

Attorneys for Plaintiff Microsoft Corporation

CERTIFICATION OF COMPLIANCE

Pursuant to L.R. 7.1(D), N.D. Ga., counsel for Plaintiff hereby certifies that this Notice has been prepared with one of the font and point selections approved by the Court in L.R. 5.1, N.D. Ga.

Dated: April 4, 2022

Respectfully submitted,

/s/ Joshua D. Curry
Joshua D. Curry

Joshua D. Curry (Georgia Bar No. 117378)
Jonathan D. Goins (Georgia Bar No. 738593
LEWIS BRISBOIS BISGAARD & SMITH LLP
600 Peachtree Street NE, Suite 4700
Atlanta, GA 30308
Tel: 404.348.8585
Fax: 404.467.8845
josh.curry@lewisbrisbois.com
jonathan.goins@lewisbrisbois.com

Gabriel M. Ramsey (*pro hac vice*)
Kayvan Ghaffari (*pro hac vice*)

Anna Z. Saber (*pro hac vice*)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Tel: (415) 986-2800
Fax: (415) 986-2827
gramsey@crowell.com
kghaffari@crowell.com
asaber@crowell.com

Emily Alban (*pro hac vice*)
Garylene Javier (*pro hac vice*)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Tel: (202) 624-2500
Fax: (202) 628-5116
ealban@crowell.com
gjavier@crowell.com

Richard Domingues Boscovich
(*pro hac vice*)
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399
Tel: (425) 704-0867
Fax: (425) 936-7329
rbosco@microsoft.com

Attorneys for Plaintiff Microsoft Corporation

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

MICROSOFT CORPORATION, a Washington corporation, FS-ISAC, INC., a Delaware Corporation, HEALTH-ISAC, INC., a Florida corporation, Plaintiffs, v. DENIS MALIKOV, and JOHN DOES 1-7, Defendants.	)	Civil Action No: **FILED UNDER SEAL**

APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE: PRELIMINARY INJUNCTION

Plaintiffs Microsoft Corporation ("Microsoft"), FS-ISAC Inc. ("FS-ISAC"), and HEALTH-ISAC Inc. ("HEALTH-ISAC"), by counsel, pursuant to Federal Rule of Civil Procedure 65(b) and (c) as well as the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), Trademark Infringement under the Lanham Act (15 U.S.C. § 1114 *et seq.*) False Designation of Origin under the Lanham Act (15 U.S.C. § 1125(a)), Trademark Dilution under the Lanham Act (15 U.S.C. § 1125(c)), the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962), the Georgia

Computer Systems Protection Act (O.C.G.A. § 16-9-93), common law trespass to chattels, unjust enrichment, and conversion, respectfully move the Court for an emergency *ex parte* temporary restraining order, and order to show cause why a preliminary injunction should not issue.

As discussed in Plaintiffs' brief in support of this Application, Plaintiffs request an order disabling a number of Internet Domains through which Denis Malikov and John Does 1-7 ("Defendants") perpetuate the unlawful behavior of hacking into a victim's computer network, installing software on a victim's network that allows Defendants to achieve and maintain long-term and surreptitious access to that network, and exfiltrating sensitive information off of a victim's network.

Ex parte relief – and expedited consideration under Local Rule 7.2(b) – is necessary and essential to halt Defendants' unlawful activity. If Defendants are given prior notice, they will significantly impede, if not preclude, Plaintiffs' ability to obtain effective relief against Defendants. This is because Defendants are highly sophisticated cybercriminals capable of quickly adapting the command and control infrastructure used to secretly establish themselves on a victim's network.

Plaintiffs' Application is based on: (i) this Application, (ii) Plaintiff's Brief in Support of this Application, (iii) the declarations of Gabriel Ramsey,

Christopher Coy, Jason Lyons, Rodel Finones, Brian Tishuk, Errol Weiss, and Tomas Prochazka in support of this Application, and on such arguments and evidence as may be presented at the hearing on this Application.

Plaintiffs further respectfully requests oral argument on this motion to be set for April 5, 2022 or as soon thereafter as the Court deems possible.

Dated: April 4, 2022

Respectfully submitted,

/s/ Joshua D. Curry
Joshua D. Curry

Joshua D. Curry (Georgia Bar No. 117378)
Jonathan D. Goins (Georgia Bar No. 738593
LEWIS BRISBOIS BISGAARD & SMITH LLP
600 Peachtree Street NE, Suite 4700
Atlanta, GA 30308
Tel: 404.348.8585
Fax: 404.467.8845
josh.curry@lewisbrisbois.com
jonathan.goins@lewisbrisbois.com

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

Emily Alban (*pro hac vice*)
Garylene Javier (*pro hac vice*)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Tel: (202) 624-2500
Fax: (202) 628-5116
ealban@crowell.com
gjavier@crowell.com

Richard Domingues Boscovich
(*pro hac vice*)
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399
Tel: (425) 704-0867
Fax: (425) 936-7329
rbosco@microsoft.com

Attorneys for Plaintiff Microsoft Corporation

CERTIFICATE OF COMPLIANCE

Pursuant to L.R. 7.1(D), N.D. Ga., counsel for Plaintiffs hereby certifies that this Application has been prepared with one of the font and point selections approved by the Court in L.R. 5.1, N.D. Ga.

Dated: April 4, 2022

Respectfully submitted,

/s/ Joshua D. Curry
Joshua D. Curry

Joshua D. Curry (Georgia Bar No. 117378)
Jonathan D. Goins (Georgia Bar No. 738593
LEWIS BRISBOIS BISGAARD & SMITH LLP
600 Peachtree Street NE, Suite 4700
Atlanta, GA 30308
Tel: 404.348.8585
Fax: 404.467.8845
josh.curry@lewisbrisbois.com
jonathan.goins@lewisbrisbois.com

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

Emily Alban (*pro hac vice*)
Garylene Javier (*pro hac vice*)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Tel: (202) 624-2500
Fax: (202) 628-5116
ealban@crowell.com
gjavier@crowell.com

Richard Domingues Boscovich
(*pro hac vice*)
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399

Tel: (425) 704-0867
Fax: (425) 936-7329
rbosco@microsoft.com

Attorneys for Plaintiff Microsoft Corporation

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

MICROSOFT CORPORATION, a Washington corporation, FS-ISAC, INC., a Delaware corporation and HEALTH-ISAC, INC., a Florida corporation, Plaintiffs, v. DENIS MALIKOV AND JOHN DOES 1-7, Defendants.	)	Case No.: **FILED UNDER SEAL**

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

Plaintiffs Microsoft Corporation ("Microsoft"), FS-ISAC, INC. ("FS-ISAC") and HEALTH-ISAC, INC. ("H-ISAC") seek an emergency *ex parte* temporary restraining order ("TRO") and a preliminary injunction designed to halt the operation and growth of far-reaching Internet-based cyber-theft criminal enterprise referred to as "ZLoader." Defendant Denis Malikov enables ZLoader to proliferate malicious financial malware and ransomware through the weaponization of macros

(as discussed more fully below) embedded within Microsoft Excel spreadsheets and other Microsoft documents that infects its victim's computers. Defendants John Does 1 through 7 distribute and operate three variants of the ZLoader malware and four families of ransomware that are distributed through ZLoader. The ZLoader botnet has infected hundreds of thousands of computing devices around the world, stealing and extorting countless innocent victims for millions of dollars.

The infected computers known as "bots" form a collective group of computers known as a "botnet," which is operated by Defendants using command and control ("C2") servers. The Defendants primarily use the ZLoader malware to surreptitiously infect victim computers with its code and functions as a platform for additional malware and ransomware to be plugged in and perform different tasks. Using these C2 servers, the Defendants can deliver instructions to and control these infected "bots" to carry out malicious acts that harm Plaintiffs, their customers and members, and the public.

The ZLoader Defendants cause substantial harm by misusing the trademarks of Microsoft and of the financial institution members of FS-ISAC, and by using other deceptive means to lull victims targeted by Defendants into believing that their malicious infrastructure is associated with Microsoft or financial institution members of FS-ISAC or otherwise deceiving owners of infected computers into

believing that their Windows operating system or their access to online financial websites are functioning normally when, in fact, Defendants have surreptitiously corrupted them, converting them into instruments of crime aimed at stealing sensitive and confidential information from the owners. Defendants, moreover, misuse the trademarks of Microsoft and the financial institution members of FS-ISAC to deceive computer users into allowing their computers to be compromised and thereafter stealing user login credentials for Microsoft online accounts and for online financial accounts of FS-ISAC's members and other sensitive information.

The ZLoader operation is a particularly destructive enterprise. At the core of the ZLoader enterprise are Defendants Malikov[1] and John Does 1 through 7 (the "Defendants"). Defendants have carried out a deceptive campaign to deceive

[1]Defendant Malikov was identified by analyzing the telemetry from deployments of the ZLoader malware in victim environments. This led to the identification of a file related to the ZLoader ecosystem named "ExcelGenerator.exe." Further analysis revealed a "PDB" file path called "ExcelGenerator.pdb" with the user name "KROKONAVT" in the file path. Open source research regarding the name KROKONAVT was linked to the "mining" of Etherium cryptocurrency and the associated email address krokonavt[@]gmail.com. The online nickname "KROKONAVT" and the email address krokonavt[@]gmail.com are associated with Denis Malikov of the city of Simferopol, Crimea. Social media and other online presence further linked Denis Malikov to the name KROKONAVT and email address krokonavt[@]gmail.com and established that he had the technical capabilities to create and operate the ZLoader-associated ExcelGenerator.exe program. Thus, Mr. Denis Malikov of Simferopol, Crimea was concluded to be the party associated with the ExcelGenerator application that is used to weaponize Excel files to distribute the ZLoader malware to victims.

customers of Microsoft and FS-ISAC's financial institution members in order to obtain access to their online accounts. Defendants have also developed malware designed to steal account credentials, personal information, and monetary funds. Over the past several years. Defendants have expanded the capabilities of the ZLoader operation to commit fraud and steal information and have aggressively expanded this operation to target victim computers around the world. Defendants sell the entire operation to other threat actors as "malware-as-a-service."

Defendants have also designed ZLoader to deploy dangerous and destructive ransomware. This ransomware, including the notorious Ryuk deployment, are singularly designed to encrypt a victim's device and extort unsuspecting victims to release control of the device. The ransomware deployed by Defendants have been used throughout the world against individuals, public education centers, government contractors, and hospitals (during COVID). In particular, ransomware has targeted health care members of H-ISAC, financial institution members of FS-ISAC and customers of Microsoft.

To control and coordinate the targeting of user accounts and computers. Defendants have developed a central ZLoader command and control infrastructure comprised of server computers located at certain Internet domains. Together, these computers and domains comprise the ZLoader command and control infrastructure.

Through this infrastructure. Defendants communicate with the infected computers and thereby orchestrate criminal activity on a global scale:

- Defendants use the command and control infrastructure to deceive users into clicking on links or otherwise interact with malicious websites, resulting in the theft of victims' online credentials and installation of malicious code.
- Defendants use the command and control infrastructure to send instructions and commands to infected user computers, directing those computers to steal users' online credentials.
- Defendants use the command and control infrastructure to upload stolen files, online account credentials, and other information from the infected user computers.
- Defendants hide behind the command and control infrastructure, using the anonymity of the Internet to conceal their locations and identities while causing injury to Microsoft and its customers and reaping illicit benefits through the continuing operation of the ZLoader infrastructure.

Plaintiffs therefore respectfully request a TRO directing the disablement of the ZLoader command and control infrastructure which will cut communications between Defendants and the infected user computers and accounts, thereby halting the criminal activity that is harming Plaintiffs, their customers and members, and the public.

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 direct the ZLoader operation and the evidence of their unlawful activity. Defendants can easily redirect infected user computers away from

the currently used (and identified) ZLoader command and control infrastructure if they learn of the impending action. Giving Defendants that opportunity would render further prosecution of this lawsuit fruitless.

This type of requested *ex parte* relief is not uncommon when disabling an online command and control infrastructure used by unidentified defendants for illegal operations and cybercrime schemes. Courts in numerous cases involving Microsoft, FS-ISAC and other plaintiffs have granted such relief.[2]

If the Court grants Plaintiffs' requested relief, immediately upon execution of the TRO, Plaintiffs 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. Plaintiffs will immediately serve the complaint and all

[2] *See Microsoft v. John Does, 1-11,* Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.) (involving the "Rustock" botnet); *Microsoft v. Piatti, et al.,* Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (involving the "Kelihos" botnet); *Microsoft Corp. et al. v. John Does 1-39 et al.,* Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) (involving the "Zeus" botnets); *Microsoft Corp. v. Peng Yong et al.,* Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (involving the "Nitol" botnet); *Microsoft Corp. v. John Does 1-18 et al.,* Case No. 1:13-cv-139-LMB/TCB (E.D. Va.) (Brinkema, J.) (involving the "Bamital" botnet); *Microsoft v. John Does 1-82 et al.,* Case No. 3:13-CV-00319-GCM (W.D.N.C.) (Mullen, J.) (involving the "Citadel" botnets); *Microsoft Corporation v. John Does 1-8 et al.,* Case No. A13-cv-1014-SS (W.D. Tex. 2013) (Sparks, J.) (involving the "ZeroAccess" botnets.); *Microsoft et al. v. John Does 1-8,* Case No. 1-14-CV-811-LOG/TCB (E.D.V.A.) (O'Grady, J.) (involving the "Shylock" botnets); *Microsoft v. John Does 1-3,* Case No. 1:15-cv-240-LMB/IDO (Brinkema, J.) (E.D. Va. 2015) (involving the "Ramnit" botnets); *Microsoft v. John Does 1-5,* 1:15-cv-06565-JBW-LB (E.D.N.Y. 2015) (involving the "Dorkbot" botnets); *Microsoft Corporation v. John Does. 1-2,* Case No. 1:16-cv-993 (E.D. Va., 2016) (Lee, J.) (involving "Strontium" threat actors); *Microsoft v. John Does 1-2,* Case No. 1:19-cv-716-ABJ (D.D.C.) (involving "Phosphorus" threat actors).

papers in this action on Defendants, using known contact information and contact information maintained by domain registrars that leased domains to Defendants, which they use for their command and control infrastructure.

Microsoft respectfully requests the Court grant a TRO and preliminary injunction to cease the harm caused by Defendants' malware attacks of Microsoft Window operating systems on victim computers and their attacks directed at the financial institution members of FS-ISAC and the health care organization members of H-ISAC, and terminate the proliferation of malicious malware and ransomware by the botnet.

I. STATEMENT OF FACTS

Plaintiffs seek to stop Defendants' illegal conduct, including the hijacking of Microsoft's Windows operating system on infected computers, and targeting of FS-ISAC's and H-ISAC's members, including the installation of malware, the distribution of ransomware, the theft of users' funds, account credentials and sensitive information. Declaration of Christopher Coy in Support of Plaintiffs' Application for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction ("Coy Decl.") at ¶ 16. Defendants conduct this activity through a set of infrastructure and operations that is referred to as the "ZLoader" botnet. *Id*. ¶¶ 3-6, 9.

A. Overview of ZLoader

ZLoader is a "botnet." A botnet is a network made up of end user computers connected to the Internet that have been infected with a certain type of malicious software ("malware" or a "Trojan") that places them under the control of the individuals or organizations who utilize the infected end user computers to conduct illegal activity. *Id*. ¶ 7. These infected computers are sometimes referred to as "bots." *Id*. A botnet network may be compromised of as few as hundreds or as many as tens of thousands or millions of infected end-user computers, thus creating a network of bots. *Id*.

Once an individual or organization has created a botnet, they can use its scale, combined computing power, and ability to monitor online activities of the infected computing devices to engage in malicious, illegal activity. *Id*. ¶ 8. These illegal activities range from attacking other computers on the Internet; installing other forms of malicious software; sending spam email; stealing credentials for online accounts, including financial accounts; stealing personal identifying information; stealing confidential data; selling or renting access to the infected computer devices to other cybercriminals; and other illegal activities. *Id.*

Plaintiffs' investigations uncovered that a central group of botnet developers wrote the code for ZLoader and commercialized it by offering other criminals use of

ZLoader on a "malware-as-a-service" basis. *Id*. ¶ 10. Plaintiffs' investigations also discovered that Defendant Malikov wrote the code to generate malicious Excel files used to distribute ZLoader (*see supra* pg. 3, fn. 1),

The ZLoader botnet is a prolific and globally dispersed financial malware distribution botnet. *Id*. ¶ 9. Microsoft investigators have been able to identify full details about the ZLoader botnet, including its command and control infrastructure, the methods of communications amongst infected computers, how the botnet transmits malicious threats to innocent computers, and the ZLoader botnet's methods to evade detection and attempts to disrupt the botnet's operation. *Id*. ZLoader is a complex and constantly evolving botnet, delivering malware and ransomware, providing backdoor access to infected machines, and acting as a gateway malware dropper to deploy additional ransomware. *Id*. For example, once installed, beyond its own financial theft functionality, ZLoader can further deliver the ransomware families such as Ryuk, Egregor, Nefilim, and DarkSide ransomware to the victim's machine. *Id*. ZLoader also has the capacity to leverage victim machines to steal online banking credentials with a variety of tools, including Man in the Browser (MITB) capabilities. Declaration of Rodelio G. Fiñones in Support of Plaintiffs' Application for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction ("Fiñones Decl.") at ¶ 4.

The primary purpose of the ZLoader botnet and the Defendants' operation is to be a malware-as-a-service for distributing ransomware, stealing account credentials, personal identification information, monetary funds as well as to further propagate the botnet infrastructure itself. Further, ZLoader is a malware that has a "modular" design that allows other types of malware to plug into it and perform different tasks. *Id*. ¶ 7. ZLoader itself is a malware device that is designed to steal the end-user's banking credentials and other personal identifying information in order to access the end-user's bank accounts and siphon funds to the Defendants or other criminal organizations. *Id*. ¶ 12. ZLoader has Man-In-The Browser capabilities to monitor the victim's activity, identify and exfiltrate cookies and credentials from browsers and Microsoft Outlook, and detects when the victim is navigating via their browser to the online portals of a wide variety of financial institutions, including banks, brokerage firms and credit card companies. *Id*. ¶ 13.

Beyond the financial institutions, ZLoader's Man-in-the-Browser functionalities targets webpages associated with Microsoft. Specifically, ZLoader targets *http://login.microsoftonline[.]com*. *Id*. ¶ 25. When ZLoader detects that the user is visiting a financial institution website or a Microsoft sign-in website, the malware alters or replaces content as it appears to the victim in their browser. In this way, the victim believes that they are at the legitimate online financial website, when

in fact they are seeing either an entirely fake version of the website to which the ZLoader module has diverted them, or a version of the website that has been manipulated by Defendants. The targeted financial institutions are FS-ISAC members and Defendants' attacks in this regard reproduce the trademarks, names and logos of the financial institutions in fake or manipulated web pages, in order to deceive victims. Declaration of Brian Tishuk in Support of Plaintiffs' Application for an Ex Parte Temporary Restraining Order and Order to Show Cause re Preliminary Injunction ("Tishuk Decl.") ¶ 21. When the user types their login credentials into the website or types additional information into fraudulent fields injected by the Defendants (such as pin codes, answers to security questions or other personal information), the Defendants intercept that information and use it to log into the user's online accounts. Finones Decl. ¶ 13.

ZLoader Defendants use a common technique known as "hook browser processes" to support its "man-in-the-browser" functionality. This process is where an application intercepts an application program interface call between two other applications. In effect, the hooking process effectively passes control of the API calls to the control of the malware. This process allows ZLoader to intercept victim data, evade detection mechanisms, and maintain persistence over victim machines. *Id*. ¶ 15. Once ZLoader infiltrates a victim device, its initial process is to navigate through

core functionalities within the Window's system. For example, ZLoader runs processes that enable the operators to inject codes to target browser processes discovered. *Id*. ¶ 21.

Once installed on an end-user computer, the malicious software detects when the user of that computer navigates to an online banking website (or any other website specified in the configuration files). When a user visits their online banking website, the malicious software may do one of the following:

a. Access the real banking website, but unknown to the user, execute instructions that modify or extend the website.
b. Intercept the request from the user's web browser and present the user with a fake website, based on the template, which appears to be the legitimate website.

Id. ¶ 23.

ZLoader also targets Microsoft's Outlook application. The ZLoader malware contains functions that queries several entries in Window's registry to extract information about email-related credentials. *Id*. ¶ 24.

Based on Microsoft's investigation and analysis, Microsoft has determined that ZLoader is a substantial and robust delivery mechanism for distributing ransomware and financial targeted malware, carrying out user credential harvesting, and engaging in exploit campaign attacks. Coy Decl. ¶ 16. Further, Defendants must have known and intended that the botnet code, the ZLoader botnet and Defendants'

operation of such botnet was to defraud end-user victims of the ZLoader botnet, by means of fraudulent pretenses and representations transmitted over the Internet, as further described below. As further described below, Microsoft has been directly injured in its business and property by these Defendants' acts and their coordinated pattern of attacks.

B. Organization of ZLoader

Like other botnets, the ZLoader botnet is comprised of a large number of victim computers that have been infected by the Defendants with the ZLoader malware. *Id*. ¶ 18. Further, the ZLoader botnet includes computers that have a "command and control" purpose. *Id*. These command and control computers are utilized by the Defendants to transfer command and control instructions to the infected victim computers, in order to maintain control over the operation of those victim computers and to carry out the numerous types of harmful activities described more fully below. *Id*. Defendants control the ZLoader botnet through command and control infrastructure comprised of Internet domains and name servers that are all maintained on an interconnected network. *Id*. ¶ 6.

1. Infected Victim Computers

The ZLoader botnet is comprised of over 200,000 infected end user computers for the period of 12 months, of the type commonly found in businesses, living rooms,

schools, libraries, and Internet cafes around the world. *Id*. ¶ 9. ZLoader is suspected of using various means of infecting end-user computers. *Id*. Microsoft's investigation determined ZLoader is disseminated via technical exploits of victim computers, malicious spam email or spearphishing campaigns. *Id*. ¶ 10. These campaigns send unsolicited emails that direct users to download malware from malicious websites or trick the user into opening malware through an attachment, such as a malicious Microsoft Word document or malicious Microsoft Excel spreadsheet. *Id*. ¶¶ 4, 10, 19-20. The spam email and spearphishing campaigns used to distribute the ZLoader malware have also been using deceptive themes involving public topics of discussion, such as COVID-19, job applications and resume distribution, in order to trick users into clicking on documents or links. *Id*. ¶ 20.

More recently, Microsoft has seen new methods by which ZLoader infects victim devices. *Id*. ¶ 21. For example, while ZLoader previously relied upon phishing emails, ZLoader now leverages online ad platforms. *Id*. Specifically, the ZLoader Defendants purchase online ads that can point victims to websites that host malware posing as legitimate installers. *Id*.

The infected victim computers are responsible for performing the daily work of the botnet. *Id*. ¶ 22. Further, owners of the infected victim computers are targets of the Defendants, as Defendants can use these computers to install financial theft

malware which enables them to ultimately steal money directly from these individuals' bank accounts, as well as to steal personal information from the owners of the infected computers, encrypt the computers with ransomware and demand a ransom or to engage in other malicious activity directed at these victims. *Id.*

2. Command and Control Computers

The command and control computers are specialized computers and/or software ("servers"). *Id.* ¶ 23. Defendants purchased or leased these servers and use them to send commands to control the ZLoader botnet's infected victim computers. *Id*. The command and control computers send the most fundamental instructions, modules, updates, and commands, and overall control of the botnet is carried out from these computers. *Id*. Command and control computers include the servers located at the domain listed in **Appendix A** to the Complaint, which are described more fully below.

To create the command and control computers, Defendants set up accounts with web-hosting providers (i.e., usually legitimate companies) that provide facilities where computers can be connected through high-capacity connections to the Internet and locate their servers in those facilities. *Id*. ¶ 25. By contacting a command and control server, the ZLoader malware can receive updated commands and modules from and communicate with the Defendants. *Id*.

a) Overview of Command and Control Communications Channels

After the ZLoader malware infects a victim computing device, it connects over the Internet to one of its pre-programmed command and control servers. *Id.* ¶ 26. The Defendants can send and receive communications between their command and control servers and the infected victim computers in the ZLoader botnet. **Figure 2** below illustrates the communication channels of the ZLoader botnet, between the command and control servers and infected victim computers. *Id.* ¶ 27.

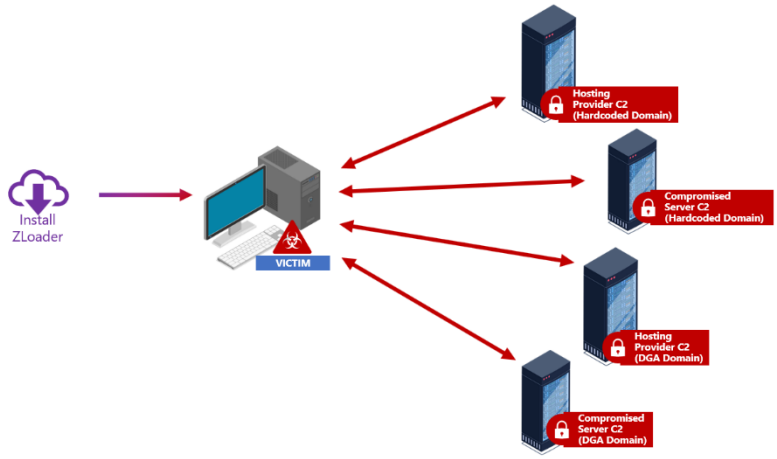

FIGURE 2

The primary command and control communications channel between infected victim computers and Defendants' command and control computers (sometimes abbreviated in this declaration as "C2") is comprised of "hardcoded" domain names associated with servers directly controlled by Defendants. *Id.* ¶ 28.

Once ZLoader infiltrates a victim's computer and the malware is installed, the

victim computer receives instructions from the botnet command and control servers associated with a hardcoded domain directly controlled by Defendants. *Id*. ¶ 29. The Defendants have used the command and control domain to distribute and propagate the botnet code, to receive communications from the botnet and to control the botnet. During its investigation into ZLoader, Microsoft identified approximately 70 command and control hardcoded domains that have been used to propagate the botnet. *Id*.

The relief sought in this case is directed at disabling these malicious domain names registered and used by Defendants. *Id*. ¶ 30. The command and control domain can be disrupted by transferring the domain to a domain registrar account under Plaintiffs' control, as requested in Plaintiffs' proposed temporary restraining order in this matter. *Id*.

b) <u>The ZLoader Command and Control Communications is Designed to Evade Technical Counter-Measures</u>

Microsoft investigators observed that certain features of the command and control infrastructure enable the botnets to better withstand technical counter-measures. To avoid detection, ZLoader evolved to include capabilities that would disable Windows services, including any security and antivirus software, including antivirus software provided by Microsoft. *Id*. ¶ 62. For example, ZLoader is designed to target Windows Defender by attacking the Registry settings and implementing

powershell commands that disable Windows Defender. *Id*. Additionally, the "hook browser processes" that supports the "man-in-the-browser" functionality allows ZLoader to intercept victim data, maintain persistence over victim machines, and notably, evade detection mechanisms. *Id*.

C. ZLoader has Attacked Victims in Georgia

Through its investigation, Microsoft determined that ZLoader affirmatively targeted its customers in Georgia, including the Northern District of Georgia. *Id*. ¶ 33. Microsoft investigated IP addresses known to be associated with ZLoader and identified as logging into accounts compromised by ZLoader. *Id*. ¶ 34. Through its investigation, Microsoft determined the geographical location of these IP addresses and has plotted the location of the relevant activity on maps of the Northern District of Georgia and the state of Georgia, which reveals that there are numerous computers in the District to which Defendants have directed the ZLoader malware. *Id*.

D. ZLoader Causes Severe Harm

ZLoader inflicts severe harm on individuals whose computing devices it infects. *Id*. ¶ 35. Once a computing device is infected with ZLoader, Defendants can use the victim's computer to steal the victim's online banking credentials and funds from their online financial accounts, constantly monitor their online activities, send commands and instructions to the infected computing device to control it

surreptitiously and deliver malware that, among other things, enables Defendants to take control of the victim's computer and extort money from them. *Id*. Defendants' primary goal, as made evident by ZLoader's functionality, is to deliver financial theft malware, ransomware, enable attacks against other computers, steal online account login IDs, passwords, and other personal identifying information. *Id*.

1. ZLoader Causes Severe Harm by Deceiving Users, Infringing Trademarks and Stealing Funds

Defendants' primary goal, as made evident by ZLoader's functionality, is to deliver financial theft malware, ransomware, enable attacks against other computers, steal online account login IDs, passwords, and other personal identifying information. *Id*. In effect, once infected, altered, and controlled by ZLoader, the Windows operating system ceases to operate normally and becomes tools for Defendants to conduct their theft. *Id*. ¶ 72. Similarly, Defendants create web pages mimicking FS-ISAC's members which are manipulated to cease to operate normally and to become part of Defendants' scheme. Finones Decl. ¶¶ 13, 22-23; Tishuk Decl. ¶ 21. However, Windows and the web pages still bear the Microsoft and Windows trademarks, or the trademarks, names and logos of FS-ISAC's financial institution members. Coy Decl. ¶ 72; Tishuk Decl. ¶ 21. This is obviously meant to and does mislead customers of Microsoft and FS-ISAC's financial institution members, and it causes extreme damage to these parties' brands and trademarks that represent the

quality of its products and services. *Id*.

2. ZLoader Causes Severe Harm by Making Unauthorized Changes to Victim Computers and The Windows Operating System

ZLoader inflicts substantial damage on Microsoft whose products and trademarks Defendants systematically abuse as part of the botnet's fraudulent operations. Coy Decl. ¶ 58. During the infection process, the ZLoader malware will copy itself to the user's computer. *Id*. ¶ 59. Depending on the variant, the file can be installed in any one of several possible locations. *Id*. For example, in the context of Microsoft Windows 8, the ZLoader malware changes a number of settings in the user's Windows registry, including encrypting files that contain registry keys used by the Defendants to propagate their botnet. *Id*. Defendants fraudulently compromise a specific component of the Microsoft Windows 8 operating system that both uses the "Microsoft" and "Windows" trademarks, in order to conceal the activities of the botnet, trade on Microsoft's trademarks and deceive end-user victims of the operating system.

The compromised Windows operating system does not appear any different to the user of the infected computer. *Id*. ¶ 60. As a result, the user presumes the compromised operating system is developed and distributed by Microsoft, even though it is the operators of the botnet that are compromising the operating system.

Id.

In addition to these unauthorized changes, Defendants also embed small programs called macros. Macros are designed to run within a larger program for the purposes of automating a task on a user's behalf. *Id*. ¶ 37-39. Macros are transmitted through ZLoader phishing emails that contains an attachment such as a Word or Excel document with malicious software when the victim is prompted to "Enable Editing" and then "Enable Content." *Id*. ¶ 39. Once the victim clicks on "Enable Content," the macro malware will immediately download onto the victim device the ZLoader malware. *Id*. Once the malware is installed, it reaches back out to the command and control servers to retrieve further instructions. *Id*. ¶ 40. It is at this point that the theft of information or funds takes place and will greatly impact the security of the victim's computing device and their sensitive personal information.

3. ZLoader Causes Severe Harm by Distributing and Installing Other Types of Dangerous Malware

ZLoader is used in a variety of illegal activities, but it is well-known known as a downloader/dropper for delivering major malware families in what is known as a "malware-as-a-service" criminal business model that delivers ransomware that locks a victim's computer and demands payment to unlock it, banking Trojans that steal funds from victim accounts, and a wide range of other types of malware. *Id*. ¶ 61. The malware distributed by ZLoader that Microsoft identified includes Ryuk,

Egregor, Nefilim, and DarkSide, which is a type of crypto-ransomware. *Id*. This ransomware, in particular, has been targeted at health care institution members of H-ISAC and financial institution members of FS-ISAC, as well as numerous customers of Microsoft, in order to extort large sums of money from such victims. *See e.g.*, Errol Weiss in Support of Plaintiffs' Application for an Ex Parte Temporary Restraining Order and Order to Show Cause re Preliminary Injunction ("Weiss Decl.") ¶¶ 8-10.

The ZLoader malware can be commanded to download and install additional malware on the infected computing device, causing users whose computing devices are infected with ZLoader to be victimized by other types of malware as well. *Id*. ¶ 63. Each of these secondary malware infections makes further changes to the user's computing device, including by adding files, changing registry settings, opening additional backdoors that allow control by other cybercriminals, and allowing further sets of malware to be downloaded onto the computing device. *Id*. All of these malware variants are designed to attack computing devices running Microsoft Windows operating systems and may themselves be connected to other criminal botnet infrastructure beyond ZLoader receiving additional commands. *Id*.

Microsoft's investigation also uncovered evidence that the ZLoader botnet engages in downloading the same type of secondary malware over the same period.

This evidence confirms that the ZLoader botnet is being used in coordinated malware campaigns to infect computers of innocent victims. *Id*. ¶ 64.

4. ZLoader Causes Severe Harm to Plaintiffs' And Their Members Reputation, Brands, And Goodwill With Customers

Microsoft invested substantial resources in developing high-quality products and services, and holds registered trademarks representing the quality of its products and services and its brand, including Microsoft, Windows, Word and Outlook. *Id*. ¶ 73. Due to the high quality and effectiveness of Microsoft's products and services and the expenditures of significant resources by Microsoft to market those products and services, Microsoft generated substantial goodwill with its customers, established strong brands, 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. Similarly, FS-ISAC's financial institution members invest heavily in establishing their trademarks, brands, names and logos and their online account infrastructure as symbols of high-quality financial service products and services. Tishuk Decl. ¶ 21. However, the activities of the ZLoader botnet injure Microsoft and FS-ISAC's financial institution members and their reputation, brand, and goodwill because users subject to the negative effects of these malicious applications incorrectly believe that Microsoft and Windows, or the

financial institutions and their online services are the sources of these problems. Coy Decl. ¶ 74; Tishuk Decl. ¶¶ 21-24.

The ZLoader malware infection itself harms Microsoft and Microsoft's customers by damaging the customers' computing devices and the software installed on their computing devices, including Microsoft's proprietary Windows operating systems. Coy Decl. ¶ 66. The ZLoader malware is designed to infect and run on computer devices equipped with the Windows operating system and is licensed by Microsoft to its users. *Id.*

Microsoft's customers whose computing devices are infected with ZLoader are damaged by these changes to Windows, which alter the normal and approved settings and functions of the user's operating system, place hooks into the operating system so ZLoader can hide its presence and activities, destabilize it, and forcibly conscript the computing device into the botnet. *Id.* ¶ 68. Defendants alter and corrupt Microsoft products such that it impacts the Microsoft user experience

Customers are usually unaware of the fact that their computing devices are infected and have become part of the ZLoader botnet. *Id.* ¶ 69. Even if aware of the infection, they often lack technical resources or skills to resolve the problem, allowing their computing devices to by misused indefinitely, as manual steps to remove the malicious software may be difficult for ordinary users. *Id.*

As explained above, because of the ZLoader botnet, users of infected computing devices will experience degraded device performance. *Id*. ¶ 74. There is a great risk that users may attribute this problem to Microsoft and associate these problems with Microsoft's Windows products, thereby diluting and tarnishing the value of the Microsoft and Windows trademarks and brands. *Id*. There is a similar risk that users will incorrectly attribute financial theft from online accounts to the financial institution members of FS-ISAC, whose websites are copied and used to deceive users. Tishuk Decl. ¶ 21.

To carry out the intrusion into computing devices, Defendants cause the ZLoader malware to make repeated copies of Microsoft's trademarks onto computing devices, in the form of file names, domain names, target names, and/or registry paths containing the trademarks "Microsoft" and "Windows." *Id*. ¶ 75. For example, the main method of infecting a victim's device is through a phishing campaign that exploits and infringes Microsoft's Excel and Word trademarks. *Id*. These uses of Microsoft's trademarks are designed to cause the intrusion into the user's computing device and to confuse the user into believing that the software installed is a legitimate part of the Windows operating system, when it is not. *Id*.

Customers may, and often do, incorrectly attribute to Microsoft the negative impact of the ZLoader botnet and other malware downloaded to their computing

devices because of having their computers hijacked and infected with a variety of malware, described earlier in this declaration. *Id*. ¶ 76. The same is true of the confusion caused to users of FS-ISAC members' financial services. Tishuk Decl. ¶ 21. Further, there is a serious risk that customers may move away from Microsoft's and FS-ISAC's financial institution members' products and services because of such activities. Coy Decl. ¶ 76; Tishuk Decl. ¶ 21. There may be significant challenges to having such customers return, given the cost they bear to switch to new products and perceived risks. *Id*. ZLoader irreparably harms Microsoft and FS-ISAC's members by damaging their reputation, brands, and customer goodwill as a result. *Id*.

E. The ZLoader Command and Control Communications Tier Is Designed to Evade Technical Counter-Measures

As discussed earlier, ZLoader employs several tactics to evade technical counter-measures. During an initial infection, Microsoft observed ZLoader malware making injections to "msiexec[.]exe," an application programming interface that provides users the means to install, modify, and perform operations on Windows Installer from the command line. Coy Decl. ¶ 41. The malicious implant running inside msiexec attempts to connect to the C2 server, and download the important elements such as additional modules and configuration. *Id*. Once a connection with the C2 server is made, the ZLoader Defendants will transmit further malware onto the victim's device. *Id*. ¶ 42. Depending on the malware being pushed from the

command and control infrastructure, the malware file will be installed in any one of a few possible locations. *Id*. For example, Microsoft has observed certain malware making changes to several settings on the user's Windows Registry. *Id*.

Microsoft's investigations uncovered certain malware executing cmd.exe process for powershell commands that affirmatively modify basic settings for Internet Explorer. *Id*. ¶¶ 42-43. Modifying these settings enables the ZLoader defendants to establish persistence on the victim computers. *Id*. ¶ 42. One such powershell command is designed to target Windows Defender by attacking the Registry settings and disabled Window's anti-virus program. *Id*. ¶ 43.

F. Disrupting ZLoader

ZLoader botnet's primary command and control infrastructure is hardcoded domains. *Id*. ¶ 77. These are the domains from which the infected computers get their instructions on how to engage in the illegal activity. *Id*. These command and control domains, listed in **Appendix A**, can be disrupted by transferring them to a domain registrar account under Plaintiffs' control, as requested in Plaintiffs' proposed temporary restraining order in this matter. *Id*. Granting Plaintiffs possession of such domains in **Appendix A** will enable Plaintiffs to channel all communications to these domains to secure servers, and thereby cut off one of the only remaining means that Defendants have to communicate with the infected

computers. *Id*.

Once the command and control hardcoded domains are disrupted and removed from the control of the Defendants, the remaining mechanism for the Defendants to attempt to regain control of the ZLoader botnet are the numerous Domain Generation Algorithm (DGA) domains. *Id*. ¶ 78. These domains can be disrupted by preventing their registration, through collaboration with domain registries and others in the security community, thus preventing Defendants from gaining control of them. *Id*. Preventing Defendants from registering these domains will thereby cut off the last remaining fallback means that Defendants will use to communicate with the infected computers. *Id*.

In the aggregate, the foregoing steps, which will be carried out upon entry of the requested temporary restraining order, will prevent the Defendants from accessing their command and control infrastructure, will cut off Defendants' ability to communicate with the infected victim computers, and will effectively disable the operation of the ZLoader botnet. This is the only means by which the ZLoader botnet can be disabled and the serious harm to Microsoft and to millions of computer users can be mitigated and prevented. Once the command and control infrastructure is disabled, and Microsoft has control of that infrastructure, this will enable Microsoft to assist users impacted by the ZLoader malware in cleaning the malware off of their

systems. *Id*. ¶ 79.

The only way to suspend the injury caused to Microsoft, its consumers and the public, is to take the steps described in the [Proposed] Ex Parte Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("Proposed TRO"). *Id*. ¶ 80. This relief will significantly hinder the ZLoader botnet's monetization and capability and operational control, and stop the harmful activities of the Defendants. *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). In order to obtain a preliminary injunction, a plaintiff must demonstrate: (1) a substantial likelihood of success on the merits; (2) that irreparable injury will be suffered if the relief is not granted; (3) that the threatened injury outweighs the harm the relief would inflict on the nonmovant; and (4) that granting the relief would not be adverse to the public interest. *Kumi v. United Asset Mgmt., LLC*, No. 1:21-CV-4949-MHC, 2021 WL 6536663 (N.D. Ga. Dec. 7, 2021).

III. PLAINTIFFS' REQUESTED RELIEF IS WARRANTED

This matter presents a quintessential case for injunctive relief. Defendants' conduct causes irreparable harm. Every day that passes gives Defendants an opportunity to steal victims' financial information and money, and to expand their illegal operations. Unless enjoined, Defendants will continue to cause irreparable harm to Plaintiffs, their customers and member organizations, and the public.

A. Plaintiffs are Likely to Succeed on the Merits of Their Claims

The record demonstrates that Plaintiffs will likely succeed in their claims based on the substantial empirical evidence and forensic documentation. In short, there is no legitimate dispute about what the ZLoader operation is, what the associated actions of Defendants are and the function of the delivered ZLoader malware. Given the strength of Plaintiffs' evidence, the likelihood of success on the merits weighs heavily in favor of granting injunctive relief.

The numerous claims set forth in the Complaint include: (1) Computer Fraud and Abuse Act ("CFAA") (18 U.S.C. § 1030); (2) Electronic Communications Privacy Act, 18 U.S.C. § 2701; (3) Trademark Infringement, False Designation, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 et seq.); (4) Georgia Computer Systems Protection Act (O.C.G.A. § 16-9-93); (5) Uniform Deceptive Trade Practices Act (O.C.G.A. § 10-1-372); (6) Common Law Trespass to Chattels and Conversion (O.C.G.A. § 51-10-1 et seq.); and (7) Unjust Enrichment.

1. Defendants' Conduct Violates the CFAA

Congress enacted the CFAA specifically to address computer crime. *See, e.g.*, *Van Buren v. United States*, 141 S. Ct. 1648, 1652 (2021). "[A]ny computer with Internet access [is] subject [to] the statute's protection." *Id*. To prevail on the CFAA claim, Plaintiffs must establish that Defendants (1) accessed a protected computer; (2) without authorization; (3) for obtaining information or defrauding others; and (4) resulting in loss or damage more than $5,000. Here, Defendants' conduct satisfies each of these elements. 18 U.S.C. § 1030(a).

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).

The Declarations of Christopher Coy and Rodel Finones establish that Defendants' conduct satisfies each of these elements. First, each of the computers accessed by the ZLoader Defendants is, by definition, a protected computer, because

only computers that connect to the Internet can possibly be infected. 18 U.S.C. § 1030(e)(2)(B) (defining "protected computer" as a computer "used in interstate or foreign commerce or communication"). This includes the computers of Microsoft and its customers, and computers of the financial institution members of FS-ISAC and the health care institution members of H-ISAC. Second, each computer into which Defendants have intruded into user accounts and each computer which is infected with the ZLoader malware has been accessed without authorization. Defendants gained access to and surreptitiously installed malware onto the infected machines of Plaintiffs' customers and member organizations without their knowledge or consent. *See supra*. Third, intrusion into Microsoft customer accounts and installation of the ZLoader malware is carried out for the purpose of obtaining user credentials and defrauding users and banks. *See supra.* Defendants, moreover, damage the infected computer's operating system—*inter alia*—by impairing the integrity of the Windows registry. *See supra*. Finally, the amount of harm caused by the ZLoader Defendants exceeds $5,000. *Id*.

Defendants' conduct is precisely the type of activity that the CFAA is designed to prevent. *See, e.g., Davies v. Afilias Ltd*., 293 F. Supp. 2d 1265, 1273 (M.D. Fla. 2003) (citing 18 U.S.C. § 1030(g)) ("[A] civil cause of action was added [to the CFAA] to redress damage and loss as a result of serious computer abuses, such as

transmission of viruses or destructive worms and use of fraud to access non-public information."); *Facebook, Inc. v. Fisher*, 2009 WL 5095269, at *2-3 (N.D. Cal. Dec. 21, 2009) (granting a TRO under CFAA where defendants allegedly engaged in a phishing and spamming scheme that compromised the accounts of Facebook users); *Physicians Interactive v. Lathian Sys.*, 2003 U.S. Dist. LEXIS 22868, at *30-31 (E.D. Va. Dec. 5, 2003) (granting TRO and preliminary injunction under CFAA where defendant hacked into a computer and stole confidential information). Thus, Plaintiff are likely to succeed on the merits of their CFAA claim.

2. Defendants' Conduct Violates the ECPA

The Electronic Communications Privacy Act prohibits "intentionally access[ing] without authorization a facility through which electronic communications are provided" or doing so in excess of authorization, and, in so doing, obtaining, altering, or preventing authorized access to an electronic communication while it is in electronic storage. 18 U.S.C. § 2701(a). Defendants' conduct in operating the ZLoader operations violates ECPA because Defendants break into computing devices and computer networks with the direct intention of acquiring the contents of sensitive communications, including particularly account credentials. Defendants use software, installed without authorization on compromised computers to do so. Obtaining stored electronic information in this

way, without authorization, is a violation of the Electronic Communications Privacy Act. *See Dish Network, L.L.C. v. Irving*, 2014 WL 6470231, at *2 (M.D. Fla. Nov. 16, 2014) (access of data on a computer without authorization actionable under ECPA); *Global Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631, 635-637 (E.D.V.A. 2009) (unauthorized access to emails was actionable under ECPA).

In addition, Defendants' conduct in operating the ZLoader botnet violates ECPA because the ZLoader malware uses the "hook browser process" to support its "man-in-the-browser" functionality. Allowing ZLoader to intercept victim data, evade detection mechanisms, and maintain persistence over victim machines flies against the premise of ECPA. Coy Decl. ¶ 51. Once installed in the victim's machines, ZLoader can capture the title of the active window, record the keyboard state, and make a screenshot of a user's performed activities. *Id*. Thus, Plaintiffs are likely to succeed on the merits of their ECPA claim.

3. Defendants' Conduct Violates the Lanham Act

As discussed, ZLoader botnet's deceptive phishing emails, command and control Internet domains, and malware installation are the primary means through which Defendants use counterfeit trademarks of Microsoft. Through these deceptive means Defendants (1) infiltrate and corrupt Windows, converting it into an instrument of fraud while leaving the branding intact; and (2) cause the ZLoader

malware to make repeated copies of Microsoft's trademarks onto computing devices in the form of file names, target names and/or registry paths. *See supra.* These uses of Microsoft's trademarks are designed to cause the intrusion into the user's computing device and to confuse the user into believing that the software installed is a legitimate part of the Windows operating system or that users are logging into legitimate financial websites, when that is not the case. *See supra*. Defendants similarly reproduce the financial account websites of FS-ISAC's financial institution members, reproducing their trademarks, names and logos, to confuse victims. This all constitutes trademark infringement, false designation of origin, and dilution under Sections 1114, 1125(a), and 1125(c) of the Lanham Act.

In addition, 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. Defendants reproduction and display of Microsoft's and FS-ISAC's financial institution members' registered, famous and distinctive trademarks in spam emails and through adulteration of the Windows operating system and deceptive websites, deceive victims, causing them confusion and causing them to mistakenly associate Microsoft and FS-ISAC's members with this activity.

The Defendants make such use of trademarks to mislead Internet users into providing their credentials. Defendants steal those credentials and use them to raid Internet users' financial accounts. 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 Plaintiffs are likely to succeed on the merits. *Illinois Tool Works Inc. v. Hybrid Conversions, Inc.*, 817 F. Supp. 2d 1351, 1355 (N.D. Ga. 2011) (granting injunction against creating and distributing counterfeit products bearing holder's marks); *Garden* & *Gun, LLC v. Twodalgals, LLC,* 2008 U.S. Dist. LEXIS 79982 (W.D.N.C. 2008) (granting preliminary injunction against misleading use of trademarks under Section 1125(a)); *IHOP Corp.* v. *Langley*, 2008 U.S. Dist. LEXIS 112056 at *1-3 (E.D.N.C. Apr. 11, 2008) (granting TRO where defendant created a counterfeit version of IHOP); *Am. Online* v. *IMS*, 24 F. Supp. 2d 548, 551-52 (E.D. Va. 1998) (misuse of trademark in e-mail headers violated § 1125(a), and also constituted trademark "dilution" under § 1125(c)); *Hotmail Corp.* v. *Van$ Money Pie, Inc.*, 1998 U.S. Dist. LEXIS 10729, *12-13 (N.D. Cal. 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)).

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). The ZLoader Defendants' misleading and false use of Microsoft's trademarks - including Microsoft, Windows, Excel and Word - causes confusion and mistake as to their affiliation with Defendants' malicious conduct. Thus, Plaintiffs are likely to success on its Lanham Act claims.

4. Defendants' Conduct Violates the Georgia Computer Systems Protection Act

This Act addresses the problem of "computer related crime" O.C.G.A. § 16-9-91. including computer theft, computer trespass, and computer invasion of privacy. *Id*. at § 16-9-93; *SCQuARE Int'l, Ltd. v. BBDO Atlanta, Inc.*, 455 F. Supp. 2d 1347, 1368 (N.D. Ga. 2006).

Computer Theft. A person commits "computer theft" if he "uses a computer or computer network with knowledge that such use is without authority and with the intention of: (1) Taking or appropriating any property of another ... [or] (2) Obtaining property by any deceitful means or artful practice." O.C.G.A. § 16-9-93(a)(l)-(2). The term "property" includes "computers, computer networks,

computer programs, data, financial instruments, and services." O.C.G.A. § 16-9-92(13).

Defendants know their use of Microsoft's operating system and its customers' computers, and the computers and networks of FS-ISAC's and H-ISAC's members is without authority. The ZLoader malware takes control of infected computers and uses them for illicit purposes without the victims' knowledge or permission. Coy Decl. ¶ 35; Finones Decl. ¶ 27. Defendants surreptitiously take data from infected computers, including keystrokes, mouse actions, and credentials submitted online. *Id*.

Computer Trespass. A person commits "computer trespass" if he "uses computer or computer network with knowledge that such use is without authority and with the intention of: (1) Deleting or in any way removing . . . any computer program or data from a computer . . . (2) Obstructing, interrupting or in any way interfering with the use of a computer program or data; or (3) Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program." Ga. Code § 16-9-93(b)(1)-(3).

Defendants' use of infected Microsoft operating systems and victim computers is without authority. Coy Decl. ¶ 58. Defendants use the ZLoader malware with the intention of installing plugins and/or additional malware, as well

as stealing data from infected computers. *Id*. ¶ 61. Defendants utilize ZLoader to alter the functionality of Microsoft products on victims' computers, and to interfere with the normal operation of computers and networks of FS-ISAC's and H-ISAC's members, thus interfering with victims' use of those products. *Id*. ¶¶ 58, 68, 71; Tishuk Decl. ¶¶ 21-24; Weiss Decl. ¶¶ 8-10.

Computer Invasion of Privacy. A person commits computer invasion of privacy if he "uses a computer ... with the intention of examining ... financial or personal data relating to any other person with knowledge that such examination is without authority." O.C.G.A. § 16-9-93(c). Defendants use the ZLoader malware to access data on infected computers running Microsoft products, including can use the victim's computer to steal the victim's online banking credentials and funds from their online financial accounts, constantly monitor their online activities, send commands and instructions to the infected computing device to control it surreptitiously and deliver malware that, among other things, enables Defendants to take control of the victim's computer and extort money from them. Coy Decl. ¶ 35. As explained, Defendants know such examination is without authority.

5. Defendants' Conduct is Tortious

Defendants' conduct is tortious under the common law doctrine of conversion. The tort of conversion is the wrongful exercise of dominion or control over property

to the detriment of the rights of one entitled to possession. *United States v. Bailey*, 288 F. Supp. 2d 1261, 1269 (M.D. Fla. 2003), *aff'd*, 419 F.3d 1208 (11th Cir. 2005). Here, Defendants exercised dominion and authority over Microsoft's proprietary Windows operating system by intruding into end user computers and servers on which Windows and online account infrastructure is running. The Defendants similarly intrude into the computers and networks of FS-ISAC's and H-ISAC's members. Defendants carried out this tortious conduct by injecting code into Microsoft's software that fundamentally changed important functions of the software and by wrongfully logging into targeted accounts. They also engaged in this conduct by manipulating fake webpages that provide an interface to FS-ISAC's members' online account services and by compromising and holding for ransom computers and information of members of H-ISAC. These acts deprived Plaintiffs and their customers and members of their right to control the content, functionality, and nature of their software and services. Thus, Plaintiffs are likely to succeed on the merits of the common law claims.

6. Unjust Enrichment

Unjust enrichment occurs when (1) the plaintiff has conferred a benefit on the defendant and (2) equity requires these defendants to compensate for that benefit. *Schutz Container Sys., Inc. v. Mauser Corp.*, No. 1 :09-CV-3609-RWS, 2012 U.S.

Dist. LEXIS 44012, 110--11 (N.D. Ga. Mar. 28, 2012). Here, Defendants alter Microsoft products, including the Windows operating system, and obtain access to and alter the computers and networks of FS-ISAC's and H-ISAC's members for financial gain. Defendants exploit the widespread distribution and use of Microsoft's software and services, and the Internet-facing infrastructure of FS-ISAC's and H-ISAC's members to propagate the botnets operated using ZLoader malware, steal victims' information, and engage in other malicious activity. Moreover, Microsoft investigators find that a central group of botnet developers chose to commercialize ZLoader by offering other criminals the use of ZLoader as a "malware-as-a-service" basis. Coy Decl ¶¶ 10, 51; Finones Decl. ¶ 4. It is inequitable for Defendants to retain these benefits; equity requires that they desist in these activities and that appropriate relief to that end be granted.

B. Defendants' Conduct Causes Irreparable Harm

It is well-settled that consumer confusion and injury to business goodwill constitute irreparable harm. *See Ferrellgas Partners, L.P. v. Barrow*, 143 F. App'x 180, 191 (11th Cir. 2005) (citing *McDonald's Corp. v. Robertson*, 147 F.3d 1301, 1310 (11th Cir. 1998)) (a sufficiently strong showing of likelihood of confusion [caused by trademark infringement] may by itself constitute a showing of ... [a] substantial threat of irreparable harm.); *see also Tally–Ho, Inc. v. Coast Community*

College Dist., 889 F.2d 1018, 1029 (11th Cir. 1989) (holding that a substantial likelihood of confusion is a substantial threat of irreparable injury). Many other circuits agree. *See*, *e.g.*, *Societe Des Produits Nestle, S.A. v. Casa Helvetia, Inc.*, 982 F.2d 633, 640 (1st Cir. 1992) ("irreparable harm flows from an unlawful trademark infringement as a matter of law"); *Opticians Ass'n of Am.*, 920 F.2d at 196 ("Potential damage to reputation constitutes irreparable injury for the purpose of granting a preliminary injunction in a trademark case."); *Int'l Kennel Club, Inc.*, 846 F.2d at 1092 (holding that damages caused by "trademark infringement are by their very nature irreparable"); *General Mills, Inc. v. Kellogg Co.*, 824 F.2d 622, 625 (8th Cir. 1987) ("Since a trademark represents intangible assets such as reputation and good-will, a showing of irreparable injury can be satisfied if it appears that [plaintiff] can demonstrate a likelihood of consumer confusion."); *Rodeo Collection, Ltd. v. West Seventh*, 812 F.2d 1215, 1220 (9th Cir. 1987) ("Once the plaintiff in an infringement action has established a likelihood of confusion, it is ordinarily presumed that the plaintiff will suffer irreparable harm if injunctive relief does not issue."); *Standard & Poor's Corp. v. Commodity Exchange, Inc.*, 683 F.2d 704, 708 (2d Cir. 1982) ("In the preliminary injunction context, a showing of likelihood of confusion as to source or sponsorship establishes the requisite likelihood of success on the merits as well as risk of irreparable harm.").

Here, the ZLoader Defendants tarnish Microsoft's and FS-ISAC's members' valuable trademarks, and cause disruption to H-ISAC's members critical health care operations, all injuring Plaintiffs' goodwill, creating confusion as to the source of Defendants' malware and false messages, and damaging the reputation of and confidence in the services of Plaintiffs and their members. *See supra*. 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 Plaintiffs are unlikely to be able to enforce judgments against. *See Hoxworth v. Blinder, Robinson & Co.*, 903 F.2d 186, 206 (3d Cir. 1990) ("[T]he unsatisfiability of a money judgment can constitute irreparable injury"); *Hughes Network Sys., Inc. v. InterDigital Commc'ns Corp.*, 17 F.3d 691, 694 (4th Cir. 1994) ("[I]rreparable harm may still exist where ... damages may be unobtainable from the defendant because he may become insolvent before a final judgment can be entered and collected." (quotation omitted)); *Specialty Healthcare Mgmt., Inc. v. St. Mary Par. Hosp.*, 220 F.3d 650, 658 (5th Cir. 2000) ("There is some authority...for the proposition that an inability to actually collect on a money judgment may suffice to make an injury irreparable.").

C. The Balance of Equities Tips in Microsoft's Favor

Defendants are engaged in an illegal scheme to defraud consumers and injure Plaintiffs, their customers and their members. Given these actions, the balance of equities clearly tips in favor of granting an injunction. *See* e.g., *United States v. Dinh*, 2021 WL 5867441, at *7 (M.D. Fla. Dec. 10, 2021) (balance of hardships weighs in favor of granting a permanent injunction—Defendants suffer no relevant hardship from an injunction prohibiting illegal activity harming residents of the United States). On one side of the scales of equity rests the harm caused by the ZLoader Defendants to Plaintiffs and their customers and members. On the other side, Defendants can claim no legally cognizable harm because an injunction would only require Defendants to cease illegal activities. As such, the balance of equities leans in favor of Plaintiffs.

D. <u>The Public Interest Favors an Injunction</u>

It is clear that an injunction would serve the public interest. For each passing day, Defendants intrude into more victim accounts, infect more computers, deceive more members of the public, and steal more information from the accounts and computers of their innocent victims. Moreover, the public interest is clearly served by enforcing statutes designed to protect the public, such as the Lanham Act, CFAA, and ECPA. *DISH Network L.L.C. v. Torres*, No. 620CV878ORL41LRH, 2020 WL 10318560, at *5 (M.D. Fla. Nov. 30, 2020) (the public interest would be

served by enforcing the ECPA); *Express Franchise Servs., L.P. v. Impact Outsourcing Sols., Inc*., 244 F. Supp. 3d 1368, 1384 (N.D. Ga. 2017) (as is often the case in cases involving Lanham Act violations, the public interest weighs in favor of enforcing Express's intellectual property rights and preventing consumer confusion). Notably, this court and numerous courts that have confronted requests for injunctive relief targeted at disabling malicious computer botnets have granted such relief. *See Microsoft v. John Does 1-51*, Case No. 1:17-cv-4566 (N.D. Ga. 2017) (Cohen, J.) (*Ex Parte* TRO and preliminary injunction to dismantle botnet command and control servers), *Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (same); *Microsoft v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (same); *Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va. 2010) (Brinkema, J.) (same); *Microsoft v. John Does 1-11*, Case No. 2:11-cv-00222 (W.D. Wash. 2011) (Robart, J.) (same); *Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) (same); *FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal. 2009) (Whyte, J.) (*Ex Parte* TRO and preliminary injunction disconnecting service to botnet hosting company). Plaintiffs respectfully submit 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

Plaintiffs' Proposed Order directs that the third-parties whose infrastructure Defendants rely on to operate the ZLoader infrastructure reasonably cooperate to effectuate the order. Critically, these third parties are the only entities within the United States that can effectively disable command and control 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) (citations omitted) (order to telephone company to assist in implementation of a pen register warrant was authorized under the All Writs Act); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398 at *30 (invoking All Writs act and granting relief similar to that requested herein); *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'"); *In re Baldwin-United Corp.*, 770 F.2d 328, 338-39 (2d Cir. 1985) ("An 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"; "[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[3] and (4) requires Plaintiffs 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, Plaintiffs 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

Due to the extraordinary factual circumstance in this instant matter, an *ex parte* TRO is necessary to be effective against the ZLoader botnet. Defendants'

[3] Microsoft will work with the providers identified in Appendix A to deploy technology designed to ensure no third-party is deprived of any property interest.

technical sophistication and ability to move their malicious infrastructure if given advance notice of Plaintiffs' request for injunctive relief, necessitates this request. *See supra*. 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 is likely that Defendants will be able to quickly mount an alternate command and control structure, in order to continue targeting victims and in order to direct the vast majority of infected computers to begin to communicate through that alternate structure before the TRO can have any remedial effects. To create the command and control computers, Defendants set up accounts with web-hosting provides that provide facilities were computers can be connected through high-capacity connections to the Internet and locate their servers in those facilities. Coy Decl. ¶ 25. By contacting a command and control server, the ZLoader malware can receive updated commands and modules from and communicate with the Defendants. *Id*. As easily as Defendants engage hosting providers to host the domains and name servers in the network, Defendants

can easily establish a new infrastructure should they be made initially aware of proceedings designed to cease their efforts at proliferating ransomware. Thus, providing notice of the requested TRO will undoubtedly facilitate efforts by Defendants to defend their operations. 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., Commodity Futures Trading Comm'n v. Highrise Advantage, LLC,* No. 620CV1657ORL41GJK, 2020 WL 6380876, at *6 (M.D. Fla. Sept. 16, 2020) (Normally ex parte relief is justified when notice to the other party would result in making the restraining order ineffective—for example when there is evidence that funds will be dissipated or documents will be destroyed when notice is given); *Crosby v. Petromed, Inc*., No. CV-09-5055-EFS, 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 Plaintiff...."); *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).

In this case, there is specific evidence that Defendants will attempt to move the infrastructure if notice is given, as Defendants have persistently changed infrastructure once it becomes known to the security community, in order to stay ahead of cybersecurity counter-measures. Coy Decl. ¶ 79. Where there is evidence that operators of cybercrime infrastructure will attempt to evade enforcement attempts where they have notice, by moving the command and control servers, *ex parte* relief is appropriate. Particularly instructive here are cases such as *Microsoft Corp. v. John Does 1-51, Microsoft Corp. v. John Does 1-27, Microsoft Corp. v. Peng Yong,* and *Microsoft Corp. v. Piatti,* all cases in which the district court issued *ex parte* TROs to disable cybercrime infrastructure, recognizing the risk that Defendants would move the infrastructure and destroy evidence if prior notice were given.

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, Plaintiffs will undertake extraordinary efforts to effect formal and informal notice of the preliminary injunction hearing to Defendants and to serve the complaint. Plaintiffs will provide notice of preliminary injunction hearing and a copy of the summons, complaint, TRO motion and supporting documents to the Defendants by the following means, to the fullest extent possible:

Plaintiffs 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. Declaration of Gabriel M. Ramsey in Support of Plaintiffs' Application for an Ex Parte Temporary Restraining Order and Order to Show Cause re Preliminary Injunction ("Ramsey Decl.") ¶¶ 10.

Plaintiffs 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 or otherwise carry out their activities. 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* ¶¶ 15-33.

Plaintiffs Will Provide Notice To Defendants By Publication: Plaintiffs 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.

Plaintiffs Will Provide Notice To Defendants By Personal Delivery: Plaintiffs have 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*. ¶¶ 10-14.

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, to the extent such are applicable and in force. *Id.* ¶¶ 13-14.

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. Plaintiffs hereby formally request that the Court approve and order the alternative means of service discussed above.

Legal notice and service by e-mail, facsimile, mail and/or 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 Plaintiffs have been approved in other cases involving international defendants attempting to evade judicial process or other 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 to all email addresses associated with the Bamital botnet command and control domains and published 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. This rationale has been similarly followed in cases within the 11th Circuit involving internet-based misconduct. *See Black & Decker, Inc. v. King Grp. Can.*, 2009 U.S. Dist. LEXIS 136277, at *8 (N.D. Ga. May 20, 2009); *Abercrombie & Fitch Trading Co. v. 2cheapbuy.com*, 2014 U.S. Dist. LEXIS 188877, at *5 (S.D. Fla. Mar. 5, 2014).

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.[4]

For all of the foregoing reasons, Plaintiffs respectfully request 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, Plaintiffs respectfully request that this Court grant their motion for a TRO and order to show cause regarding a preliminary injunction. Plaintiffs further respectfully request that the Court permit notice of the preliminary injunction hearing and service of the Complaint by alternative means.

Dated: April 4, 2022

Respectfully submitted,

/s/ Joshua D. Curry
Joshua D. Curry

[4] 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."). And in the case of Mr. Malikov, Crimea is not party to the Hague Convention.

Joshua D. Curry (Georgia Bar No. 117378)
Jonathan D. Goins (Georgia Bar No. 738593
LEWIS BRISBOIS BISGAARD & SMITH LLP
600 Peachtree Street NE, Suite 4700
Atlanta, GA 30308
Tel: 404.348.8585
Fax: 404.467.8845
josh.curry@lewisbrisbois.com
jonathan.goins@lewisbrisbois.com

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

Emily Alban (*pro hac vice*)
Garylene Javier (*pro hac vice*)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Tel: (202) 624-2500
Fax: (202) 628-5116
ealban@crowell.com
gjavier@crowell.com

Richard Domingues Boscovich
(*pro hac vice*)
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399

Tel: (425) 704-0867
Fax: (425) 936-7329
rbosco@microsoft.com

Attorneys for Plaintiff Microsoft Corporation

CERTIFICATE OF COMPLIANCE

Pursuant to L.R. 7.1(D), N.D. Ga., counsel for Plaintiff hereby certifies that this Motion has been prepared with one of the font and point selections approved by the Court in L.R. 5.1, N.D. Ga.

Dated: April 4, 2022

Respectfully submitted,

/s/ Joshua D. Curry
Joshua D. Curry

Joshua D. Curry (Georgia Bar No. 117378)
Jonathan D. Goins (Georgia Bar No. 738593
LEWIS BRISBOIS BISGAARD & SMITH LLP
600 Peachtree Street NE, Suite 4700
Atlanta, GA 30308
Tel: 404.348.8585
Fax: 404.467.8845
josh.curry@lewisbrisbois.com
jonathan.goins@lewisbrisbois.com

Gabriel M. Ramsey (*pro hac vice*)
Kayvan Ghaffari (*pro hac vice*)
Anna Z. Saber (*pro hac vice*)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111

Tel: (415) 986-2800
Fax: (415) 986-2827
gramsey@crowell.com
kghaffari@crowell.com
asaber@crowell.com

Emily Alban (*pro hac vice*)
Garylene Javier (*pro hac vice*)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Tel: (202) 624-2500
Fax: (202) 628-5116
ealban@crowell.com
gjavier@crowell.com

Richard Domingues Boscovich
(*pro hac vice*)
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399
Tel: (425) 704-0867
Fax: (425) 936-7329
rbosco@microsoft.com

Attorneys for Plaintiff Microsoft Corporation