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

MICROSOFT CORPORATION, a Washington corporation, and FS-ISAC, INC., a Delaware corporation,

Plaintiffs,

v.

JOHN DOES 1-8, CONTROLLING A COMPUTER BOTNET THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS,

Defendants.

Civil Action No: 1:14 CV 811
LOG/TCB

FILED UNDER SEAL

APPLICATION OF MICROSOFT CORPORATION AND FS-ISAC, INC. FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER, SEIZURE ORDER, AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiffs Microsoft Corp. and Financial Services—Information Sharing and Analysis Center, Inc. (FS-ISAC, Inc.) (collectively "Plaintiffs"), by counsel, pursuant to Federal Rule of Civil Procedure 65(b) and (c), the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1116, & 1125) and the common law, and the All Writs Act, (28 U.S.C. § 1651), 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 and Internet Protocol (IP) addresses and seizing the command and control servers and software by which Defendants control a harmful "botnet" known as the "Shylock botnet." Botnets are computer networks made up of tens of thousands

The damage caused by the Shylock botnets is staggering, as Defendants have infected tens of thousands of user computers and have caused millions of dollars in losses to computers and financial institutions. The Shylock botnets cause further substantial harm by misusing the trademarks of Microsoft and FS-ISAC's member institutions. Defendants misuse Microsoft's trademarks to lull owners of infected computers into believing that their Windows operating system and Internet Explorer are functioning normally when, in fact, Defendants have converted them into instruments of crime aimed at the computer owners' financial accounts. Defendants, moreover, misuse FS-ISAC member organizations' trademarks to generate fake financial institution websites, deceiving computer users into providing their account login credentials.

The Shylock botnets are a particularly sophisticated and destructive botnet enterprise. At the core are Defendants John Does 1 through 8, who created the Shylock malware that they then deployed at least as early as September 2011. Since then, John Does 1 through 8 have improved upon the Shylock malware, deployed additional Shylock botnets, and have developed a central Shylock command and control infrastructure comprised of Internet domains, domain name servers, and Internet Protocol (IP) addresses all Shylock botnets share. Defendants' criminal enterprise is responsible for deploying eight Shylock botnets, infecting tens of thousands of user computers globally.

The requested TRO directs the disablement of the Shylock command and control infrastructure. These are specialized computers and software located at specific Internet domains, domain name servers and IP addresses that Defendants use to send instructions to infected user computers, to control said computers, to steal users' online credentials, and to steal funds from users and financial institutions. The command and control software operating from and through the Shylock command and control infrastructure instructs infected user computers how to perform the Shylock botnets' day-to-day illegal activities. Disabling the Shylock command and control infrastructure will cut communications between Defendants and the infected user computers, thereby halting the criminal activity and harm to Plaintiffs, their customers and member organization, and the public. The requested TRO, moreover, directs further steps to then neutralize the Shylock malware running on users' computers.

Ex parte relief is essential. Notice to Defendants would provide them an opportunity to destroy, move, conceal, or otherwise make inaccessible the instrumentalities they use to direct the Shylock botnets and the evidence of their unlawful activity. Defendants can easily redirect infected user computers away from the Shylock command and control infrastructure if they learn of the impending action. Giving Defendants that opportunity would render further prosecution of this lawsuit entirely fruitless. Equally important, the Shylock command and control infrastructure must be disabled simultaneously to prevent one or more Defendants from directing already-infected end-user computers to communicate with alternate command and control infrastructure.

The requested *ex parte* relief is not uncommon when disabling criminal botnet schemes. Courts in eight cases involving Microsoft and other plaintiffs have granted such extraordinary relief to disable botnets. For example, in the February 2010 case concerning the "Waledac" botnet, the District Court for the Eastern District of Virginia (Judge Brinkema) adopted an approach where:

1. the Court issued a tailored *ex parte* TRO, including provisions sufficient to effectively disable the harmful botnet infrastructure, preserve all evidence of its operations and stop the irreparable harm being inflicted on Microsoft and its customers;
2. immediately after implementing the TRO, Microsoft undertook a comprehensive effort to provide notice of the preliminary injunction hearing and to effect service of process on the defendants, including Court-authorized alternate service by email, electronic messaging services, mail, facsimile, publication, and treaty-based means; and
3. after notice, the Court held a preliminary injunction hearing and granted the preliminary injunction while the case proceeded in order to ensure that the harm the botnet cause would not continue during the action.

See Microsoft v. John Does 1-27, Case No. 1:10-cv-00156 (E.D. Va. 2010) (Brinkema, J.) (Declaration of Jacob Heath In Support Of Plaintiffs' Motion For TRO ("Heath Decl."), Exs. 17 and 18). Subsequently, in eight other cases involving dangerous botnets, Federal Courts have followed this approach. *See Microsoft v. John Does*, 1-11, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.) (at Heath Decl., Exs. 19 and 20; involving the "Rustock" botnet); *Microsoft v. Piatti, et al.,* Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (Heath Decl., Exs. 21 and 22; 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.) (Heath Decl. Exs. 23 and 24; involving the "Zeus" botnets); *Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (Heath Decl., Ex. 25; 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.) (Heath Decl. Exs. 26 and 27; 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.) (Heath Decl. Exs. 28 and 29; 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.) (at Heath Decl., Ex. 30; involving the "ZeroAccess" botnets.)

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 papers in this action on Defendants, using known contact information and contact information maintained by third-party hosting companies and domain registrars that host Defendants' command and control infrastructure.

I. STATEMENT OF FACTS

Plaintiffs seek to stop Defendants' illegal conduct, including the infiltration and hijacking of Microsoft's Windows operating system and other software on user computers, theft of users' financial credentials, and use of the stolen information to pilfer users' bank accounts. (Declaration of Vishant Patel in Support of Plaintiffs' Motion for TRO ("Patel Decl.") ¶¶ 8-10 and 56-68; Declaration of Edgardo Diaz, Jr. in Support of Plaintiffs' Motion for TRO ("Diaz Decl.") ¶¶ 7, 8, and 34-43. Defendants conduct this activity through what are commonly referred to as the "Shylock botnets" or more simply "Shylock." Patel Decl. ¶¶ 5-10; Declaration of Eric Guerrino ("Guerrino Decl.") ¶¶ 12-14. Shylock has caused millions in losses. *See* Guerrino Decl. ¶¶ 10, 16-19.

A. Shylock—A Criminal Botnet Enterprise

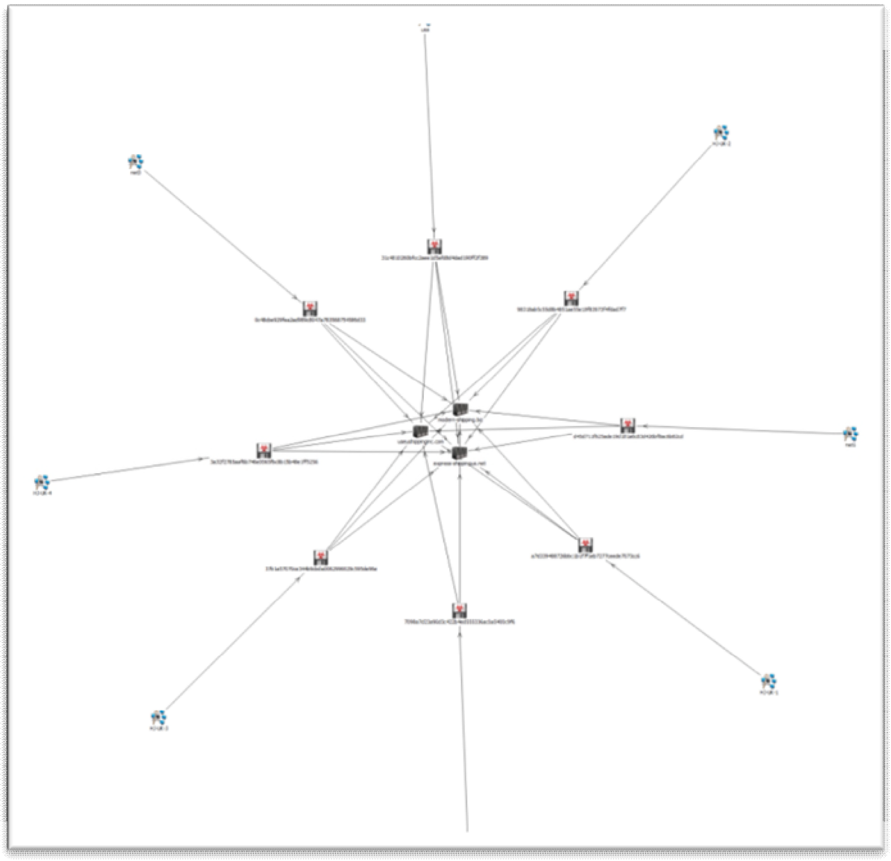
A "botnet" is a collection of user computers infected with malware. Patel Decl. ¶ 4. This malware places the infected computers under the control of the individuals or an organization who operates the botnet. *Id.* Defendants communicate with infected computers over the Internet and use them to conduct their illegal acts. *Id.* Shylock is a highly-sophisticated botnet designed to intrude upon Microsoft's Windows operating system to steal money from financial accounts of owners of Shylock-infected computers. *Id.* ¶¶ 5-6. Shylock inflicts extensive damage on infected computers. *Id.* ¶ 71-77. After infecting user computers with Shylock, Defendants can survey constantly the online banking activities of the unknowing victims. *Id.*¶ 9. Defendants' goals are to steal victims' financial account login IDs, passwords, and other personal identifying information in order to steal their money and their identities. Patel Decl. ¶ 8; Guerrino Decl. ¶¶ 14-16.

Shylock also inflicts extreme damage on Microsoft. Specifically, Shylock victimizes Microsoft's customers using Microsoft's and financial institutions' trademarks as part of the fraudulent scheme. Patel Decl. ¶ 8; Guerrino Decl. ¶ 16. Shylock creates and deploys malware that targets Microsoft's Windows® operating system and Internet Explorer® software. Patel Decl. ¶ 78; Diaz Decl. ¶¶ 10-21. In so doing, Shylock damages Microsoft's brand, trademarks, reputation, and customer goodwill as Microsoft's customers attribute the attack to perceived flaws in Microsoft's products such as Windows and Internet Explorer. Patel Decl. ¶ 78. Microsoft, moreover, must deploy significant resources to help its customers defend themselves against Shylock. *Id.* Microsoft has spent more than $1.2 million in detecting malware attacks to its systems and customers, analyzing said malware, and remediating the harm botnets cause—including the Shylock botnets. *Id.*

Similarly, Shylock inflicts damage on FS-ISAC member organizations. FS-ISAC represents 4,400 financial institutions. Shylock targets those financial institutions' customers using their trademarks as part of the fraudulent scheme. *See* Patel Decl. ¶¶ 35-36, 56-68; Guerrino Decl. ¶ 16. Defendants use financial trademarks to create fake websites to deceive users to provide their online login credentials and to steal money from users' accounts. Patel Decl. ¶ 56-68; Diaz Decl. ¶¶ 34-43; Guerrino Decl. ¶ 16. In so doing, Shylock damages the financial institutions' trademarks, reputations, and customers' goodwill. *See* Guerrino Decl. ¶ 16. FS-ISAC member organizations, moreover, attribute millions in losses to botnets—including the Shylock botnets. *Id.*

Defendants, whose true identities are unknown, created and deployed the Shylock botnet. Patel Decl. ¶ 7. Defendants' activities suggest they most likely operate from and reside in Ukraine or Russia or elsewhere in Eastern Europe. *Id.* Since the creation and deployment of the first Shylock botnet at least as early as September 2011, Defendants have developed additional Shylock botnets to improve on the original, have developed a command and control infrastructure to support the Shylock botnets, and have used this infrastructure to commit financial crimes over the Internet. *Id.* That shared infrastructure is represented in the **Figure 1** below (*id.*):

Fig. 1

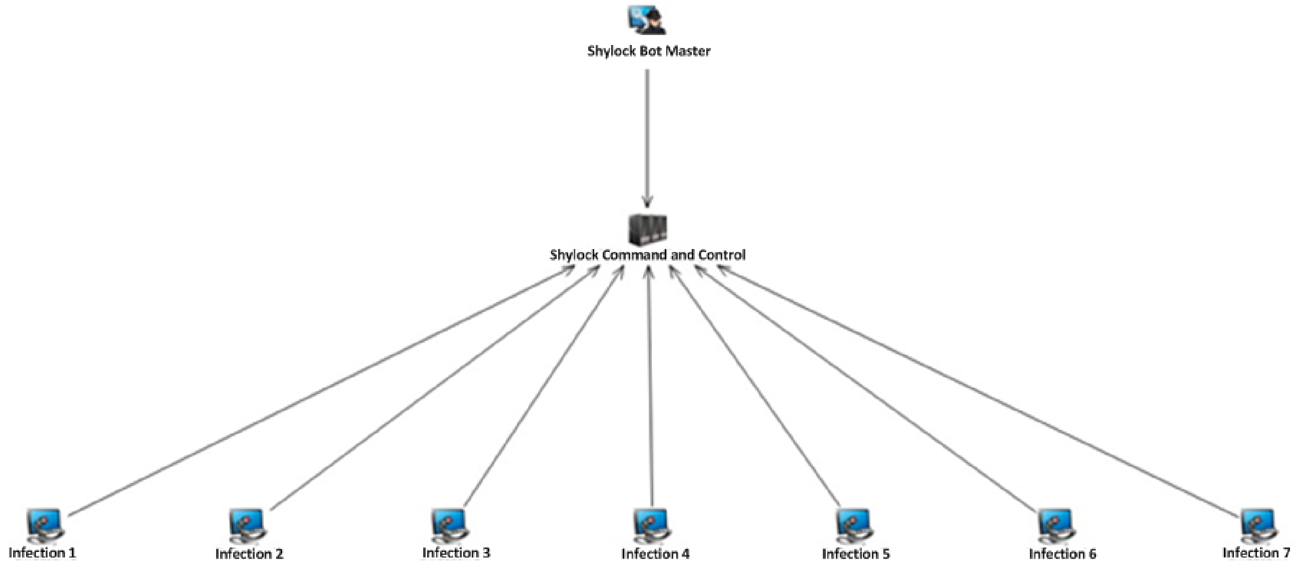


At the center of the infrastructure are the Shylock command and control servers—represented by three Internet domains Defendants use to host the Shylock malware, including the executable files used to infect user computers and the configuration files used to control user computers. *Id.* In short, the evidence shows that Shylock operates as an enterprise.

B. The Organization, Structure And Function Of The Shylock Botnets

Shylock botnets have a two-tiered architecture. Patel Decl. ¶¶ 16-17. The lowest tier—referred to as the "Infection Tier"—consists of user computers infected with Shylock. *Id.* ¶ 17. The second tier—referred to as the "Command and Control Tier"—consists of specialized computers that Defendants use to communicate with the infected user computers in the Infection Tier. The tiered architecture of Shylock botnets is shown in **Figure 2** below (*id.*):

Fig. 2



1. <u>The Shylock Infection Tier</u>

The Infection Tier consists of tens of thousands of infected user computers that are under the control of the Shylock botnets unbeknownst to their owners. *Id.* ¶¶ 18-19. These user computers are of the type commonly found in businesses, living rooms, schools, libraries, and Internet cafes around the world. *Id.* ¶ 18. They are commonly referred to Shylock "bots" or simply, infected computers. Defendants target the owners of such computers and steal financial account credentials and other personal information. *Id.* ¶ 20. Defendants have intentionally infected user computers throughout the United States, including the Eastern District of Virginia. *Id.* ¶¶ 20-21.

2. <u>The Shylock Command And Control Tier</u>

The Command and Control Tier consists of specialized computers connected to the Internet running specialized software. *Id.* ¶ 24. Defendants have purchased and/or lease these servers and use them to send commands to control and to receive information from the infected computers in the Infection Tier. *Id.* The Shylock malware running on infected computers instructs them to connect to the Command and Control Tier over the Internet every 20 to 30 minutes to provide detailed information about the processes running on the infected computer and to obtain—if available—an updated configuration with new instructions. *Id.* ¶¶ 33, 37, 48; Diaz Decl. ¶¶ 26-31. Defendants, by updating the instructions on the command and control servers, are able to communicate with and control the infected user computers. Diaz Decl. ¶¶ 22-25. Servers in the command and control tier include the domain names and name servers at Exhibit 3 and the IP addresses at Exhibit 4 to the Patel Declaration.

C. The Propagation And Operation Of The Shylock Botnets

1. Creation Of The Shylock Malware

Plaintiffs' investigation revealed that Defendants operating the Shylock botnet use the same configuration files as the "Zeus" family of botnets. Patel Decl. ¶ 14. Zeus is a family of financial fraud botnet malware that spies on users of computers and steals their financial account information, including account numbers, account balances, and passwords for online banking. *Id.* The criminals behind Zeus then use that stolen information to surreptitiously employ the victims' bank accounts. *Id.* In December 2012, Microsoft, FS-ISAC, and other plaintiffs from the financial industry obtained a default judgment against the operators of Zeus in *Microsoft et al. v. John Does 1-39*, Civil Action No. 1:12-cv-01335-SJ-RLM (E.D. N.Y.) (Johnson, J.), taking down a significant part of that botnet. *Id.*

Critical to the Shylock botnets are the executable files that allow Shylock to install itself onto user computers running Windows operating system. Diaz Decl. ¶¶ 10-12. To install itself on a user's computer, Shylock will make fundamental changes to the Windows operating system in order to obtain unfettered access to the computer's processes, to lower security settings, and to hide its activity from the user. *Id.* ¶¶ 10-21. Equally important are the Shylock configuration files that contain commands that control the infected computers' day-to-day work. *See id.* ¶¶ 22-33; *see also* Patel Decl. ¶¶ 34-38. The Shylock configuration files, for example, contain the domains to which the infected computers will connect to obtain additional files and instructions. Patel Decl. ¶ 34.

2. <u>The Shylock Command And Control Infrastructure</u>

To operate the Shylock botnets, Defendants have developed a command and control infrastructure on the Internet. Patel Decl. ¶ 7. Defendants set up accounts with web-hosting providers—*i.e.*, companies, usually legitimate, that provide facilities where computers can be connected through high-capacity connections to the Internet. *Id.* Defendants use Internet domains, domain name servers, and IP addresses as their command and control infrastructure for the Shylock botnets. *Id.* The most vulnerable points in the Shylock botnet architecture are these domains, name servers, and IP addresses of the command and control servers, as they can be identified and located, and if they are disconnected from the Internet, the botnets' communications with the infected user computers will be severed (*i.e.*, communications between computers in the Infection Tier and Command and Control Tier will be broken) and the activity of the botnet disabled. *Id.* ¶¶ 84-89; Diaz Decl. ¶ 46.

3. <u>Propagation And Control Of Shylock Botnets</u>

Defendants use several techniques to infect user computers to assimilate them into the Shylock botnets. Patel Decl. ¶ 27. Shylock infections typically result from "drive-by-downloads." *Id.* In a drive-by-download infection, a cybercriminal creates a website and stages on that website specialized software—known as an "exploit pack"—designed to infect a user's computer. *Id.*¶ 28. When a user connects to a website hosting an exploit pack, the exploit pack silently probes the user computer looking for an unpatched vulnerability in the operating system or in third-party applications that would provide an opportunity to execute code or hook malware into the operating system. *Id.*

Defendants then typically use lures to cause users to browse the Internet to visit one of these websites. *Id.* ¶ 29. Defendants, for example, have used YouTube advertisements to lure users onto exploit websites. *Id.* Defendants will load infected advertisements onto YouTube that redirect visitors to compromised websites hosting the Shylock exploit kit. *Id.* The content in the advertisement misleads users to click on the links, redirecting the user to an exploit website. *Id.* Defendants also use instant messenger applications to send users of instant messengers fake messages containing links to exploit websites. *Id.* Once a user connects to the exploit website, the exploit pack will download Shylock onto the user's computer. *Id.* From that point forward, the user's computer and Microsoft's Windows operating system running on the computer are secretly controlled by Defendants as part of the Shylock botnets. *Id.* ¶ 30. Defendants, in fact, convert the infected user computer into instrumentalities of crime, aimed at the user's bank account. *Id*.

Once installed, Shylock instructs the infected computer to contact the Shylock command and control Infrastructure over the Internet. *Id.* ¶¶ 34-35. The Shylock malware contains several hardcoded domains that correspond to command and control servers. *Id.* ¶ 32; Diaz Decl. ¶ 25. These domains are labeled "Hardcoded" in Exhibit 3 to the Patel Declaration. Patel Decl. ¶ 32. The newly-infected computer will attempt to first contact one of these hardcoded domains to download an encrypted configuration file, containing further information and instructions. *Id.*; Diaz Decl. ¶ 22. The domains labeled "Configuration File" in Exhibit 3 to the Patel Declaration host the Shylock configuration files. Patel Decl. ¶ 34.

Shylock configuration files contain various types of information that control the operation of the infected computer. Diaz Decl. ¶¶ 22-33; Patel Decl. ¶¶ 34-38. The Shylock configuration files, for example, contain parameters (commands) that instruct the infected computer to contact the command and control infrastructure every 20 to 30 minutes in order to (1) "ping" the command and control infrastructure; (2) collect and send to the command and control infrastructure detailed information about the systems and processes running on the infected computer; (3) check for new Shylock executable files; and (4) check for new Shylock configuration files. Diaz Decl. ¶¶ 22-31. Requiring infected user computers to frequently provide detailed information and check for new executable and configuration files solidifies Defendants control over the infected computers.

The configuration files also contain a list of hardcoded "fallback" domains. Diaz Decl. ¶¶ 25. If the infected user computer loses contact with the Shylock command and control infrastructure, it will attempt to contact one of the hardcoded fallback domains to attempt to reestablish communication with the command and control infrastructure. Patel Decl. ¶ 38; Diaz Decl. ¶ 25.

The configuration files also contain information used in the day-to-day work of stealing users' money. Patel Decl. ¶¶ 34-48; Diaz Decl. ¶ 8. Most significant is code that calls a "web-inject" file Defendants use to carry out a web-inject attack (discussed below). Patel Decl. ¶¶ 36, 60-66. These web-inject files contain a list of targeted financial institutions. *Id.*¶¶ 35-36, 60-66; Diaz Decl. ¶¶ 34-36. The Shylock malware running on an infected computer will monitor all Internet connections attempted by the user's computer, waiting for the user to attempt to connect to one of the targeted financial institutions. Patel Decl. ¶ 57; Diaz Decl. ¶ 34. At that point, the botnet can begin its attack on the user's account using a variety of techniques discussed below. *See* Patel Decl. ¶¶ 56-68; Diaz Decl. ¶ 34. Plaintiffs—by analyzing the Shylock configuration files—have developed a list of the financial institutions attacked by the Shylock botnets. Patel Decl. ¶ 35; Diaz Decl. ¶ 35. **Chart 1** below shows the targeted financial institutions:

Chart 1

Targeted Financial Institutions		
Abbey	Citi	NatWest
Bank of America	Citizen	navyfederal.org
Bank of Scotland	Comercia	NewEgg
Bank of West	Co-Operative Bank	nwolb.co
BankCard	co-operativebank.co.uk	parthershipcard.co.uk
Barclays	credem.it	partnershipcard.co.uk
bbt.com	crveneto.it	PNC
bmedonline.it	cv-library.co.uk	pofssavecredit.co.uk
btbonline.it	E-Trade	poste.it
cahoot.com	Evanquis	RBS
CapitalOne	Fidelity	Regions
CaptialOne	FirstCitizens	Santandar
cariciv.it	FirstDirect	Santander
carifvg.it	firstdirect.co	sovereignbank.com
caript.it	fisglobal.com	Suntrust
cariri.it	harrisbank.com	tdbank.com
cariromagna.it	HSBC	theaa.com
carisap.it	iblogin.com	tiscali.it
carisbo.it	ING	unicredit.it
carive.it	intesasanpaolo.com	unicreditcorporate.it

Targeted Financial Institutions		
carivit.it	intesasanpaoloprivatebanking.it	usaa.com
cassedellumbria.it	Lloyds	usbank.com
cbonline.co.uk	monteparma.it	virginmoney.com
cedacri.it	mybusinessbank.co.uk	WellsFargo
Chase	NationWide	ybonline.co.uk

4. **Defensive Mechanism Of The Shylock Botnets**

Relevant to Plaintiffs' requested relief, Shylock botnets have certain defensive mechanisms to better withstand technical counter-measures. Patel Decl. ¶¶ 46-55. First is the Shylock botnets' ability to move to new command and control infrastructures. *Id.* ¶ 48. Infected computers check in with the Shylock command and control infrastructure every 20 to 30 minutes for new executable and configuration files. Patel Decl. ¶¶ 33, 48. Defendants can deploy new configuration files around the world almost instantaneously. *Id.* ¶ 48. Together these tools allow Defendants to move infected computers over to a new command and control infrastructure if they detect an attack on their existing command and control infrastructure. *Id.*

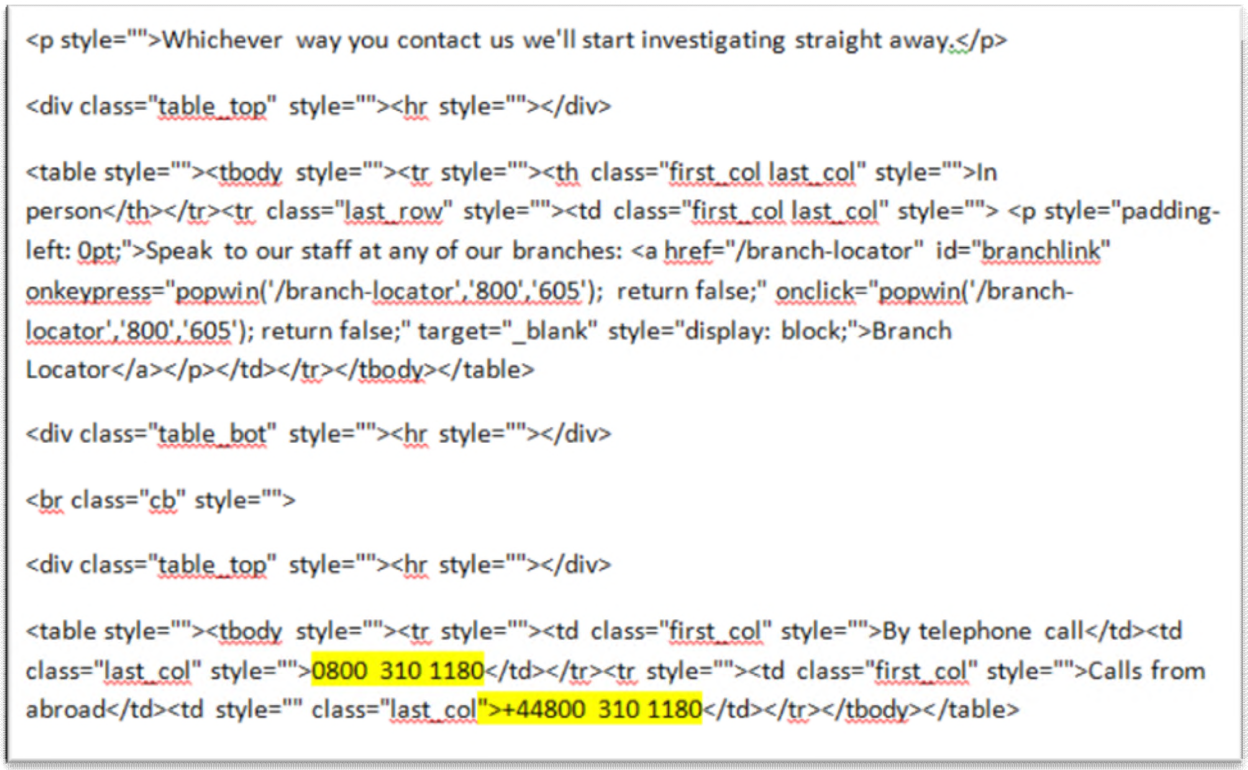
Another defense mechanism the Shylock botnets have used is their ability to keep infected computers from connecting to websites that offer antivirus software. *Id.* ¶ 51. If a user attempts to connect to a website that offers antivirus software, Shylock will block it. *Id.* When the Shylock botnets detect an attempt to connect to an antivirus website, the botnets will hijack and redirect the user's browsers. *Id.* This keeps any antivirus software on the user's computer form receiving updates, and prevents victims from being able to visit antivirus or other security websites to download removal tools and mitigation advice. *Id.*

D. **Defendants Use Shylock To Steal Money**

After infecting a user computer, Defendants move to the next phase—stealing money from the financial accounts of owners of the infected computers. A Shylock attack begins when the malware on the infected computer detects the user attempting to connect to a financial institution's website. Patel Decl. ¶ 58. Once Shylock detects this, it can instruct the infected computer to proceed in several ways. First, it can log keystrokes the user enters while he or she accesses financial accounts, it can record information displayed by the web browser, and it can even take video of what the user's account pages look like. *Id.* The Shylock botnets will later upload all this information to the Shylock command and control infrastructure, where Defendants can retrieve it and use it to steal from the user's accounts, or to conduct other illegal acts with the stolen information. *Id.*

In a variation on this attack, Shylock can use a technique called a "web-inject" to extract more sensitive information from the user. *Id.* ¶ 59. In a web-inject attack, Shylock alters the appearance of the financial institution's web page as it displays in the user's browser. *Id.* Shylock essentially takes control of the user's web browser and instead of allowing the browser to provide an accurate rendering of the financial websites to which the user has connected, it causes the browser to change what the user sees. *Id.* It does this by "injecting" additional code into the website code that the browser is rendering in a displayable format for the user. *Id.*; Diaz Decl. ¶¶ 34. Shylock, for example, will replace the contact telephone numbers for customer complaints provided on a financial institution's website. Patel Decl. ¶¶ 60-61; Diaz Decl. ¶¶ 41-42. **Figure 2** below shows a Shylock web-inject attack where Defendants have changed a bank's phone number for submitting complaints:

Fig. 2.



```
<p style="">Whichever way you contact us we'll start investigating straight away.</p>

<div class="table_top" style=""><hr style=""></div>

<table style=""><tbody style=""><tr style=""><th class="first_col last_col" style="">In
person</th></tr><tr class="last_row" style=""><td class="first_col last_col" style=""> <p style="padding-
left: 0pt;">Speak to our staff at any of our branches: <a href="/branch-locator" id="branchlink"
onkeypress="popwin('/branch-locator','800','605'); return false;" onclick="popwin('/branch-
locator','800','605'); return false;" target="_blank" style="display: block;">Branch
Locator</a></p></td></tr></tbody></table>

<div class="table_bot" style=""><hr style=""></div>

<br class="cb" style="">

<div class="table_top" style=""><hr style=""></div>

<table style=""><tbody style=""><tr style=""><td class="first_col" style="">By telephone call</td><td
class="last_col" style="">0800 310 1180</td></tr><tr style=""><td class="first_col" style="">Calls from
abroad</td><td style="" class="last_col">+44800 310 1180</td></tr></tbody></table>
```

Defendants appear to change these numbers to prevent situations where a customer—perhaps suspicious of or noticing fraudulent activity—attempts to contact the financial institution. Patel Decl. ¶ 61.

In another version of this attack, Shylock can display a completely fake website for the financial institution that the user is attempting to contact. Patel Decl. ¶ 63. To do this, Shylock first hijack's the user's browser to keep it from connecting to the real website of the financial institution. *Id.* It then contacts the Shylock command and control infrastructure to download a template for the website of the financial institution to display to the user. *Id.* The user believes they are connected to the real website of the financial institution and proceeds as normal. *Id.* However, while the user enters her real account access information, such as login ID and password, into the fake website, Defendants can access the user's accounts on the real website. *Id.* Altered account information from the real website can be reflected back to the user looking at the false website so as to maintain the ruse until the theft is complete. *Id.* To complete the theft, Defendants can alter the transactions performed on the real website by, for example, changing withdrawal amounts and changing information related to where the money is sent. *Id.*

In a variant of this attack, instead of downloading a template for the website of the financial institution, Shylock can connect the user to a completely fake website Defendants control that appears to be the website of the financial institution. *Id* . ¶ 64. More sophisticated still, Shylock can provide a built-in Virtual Network Console (VNC) server with the ability to connect out to a remote server. *Id.* ¶ 66. This feature allows Defendants to access the infected computers over the Internet, bypassing network address translation and firewall restrictions on inbound connections. *Id.* From this point, Defendants can connect the user's computer to the user's bank, and use the login information previously stolen from the user to empty the user's bank accounts. *Id.*

Defendants use the victims' account credentials to access their stolen online financial accounts or other accounts to steal money and information. *Id.* ¶¶ 42-43. Defendants often hire "money mules"—individuals who travel to the different countries, including the United States, to set up bank accounts to receive transfers of stolen funds from victims' accounts. *Id.* ¶ 43. They then withdraw funds from the accounts they have set up, keeping a percentage for their own payment, and transmit the remainder to Defendants. *Id.* To recruit money mules, Defendants use domains that comprise the Shylock command and control infrastructure. *Id.* These domains are labeled "Money Mule" in Exhibit 3 to the Patel Declaration.

E. <u>Defendants Use Microsoft's Customers' Computers In Criminal Activity</u>

Once infected with malicious software, the user's computer is under Defendants' control. *Id.* ¶ 70. Defendants have tools to turn the infected computer into a tool for criminal activity. Specifically, Shylock's configuration files utilize "plug-ins"—modules that Defendants can add to the configuration file to modify Shylock's functionality. *Id.* ¶ 39. Defendants, by making Shylock adaptable, can add new functions to Shylock even after they have deployed it. Patel Decl. ¶ 39.

Defendants serve plug-ins to Shylock-infected computers through domains comprising the Shylock command and control infrastructure. Patel Decl. ¶ 39. These domains are labeled "Plug-in" in Exhibit 3 to the Patel Declaration. *Id.* One such Plug-in is the "MessengerSpread" plug-in that allows Defendants to target users' instant messaging applications to spread Shylock to other users of instant messaging applications. *Id.* ¶ 40. Another is the "BackSock" plug-in that gives Defendants access to any uninfected computers on a local area network ("LAN") with a Shylock-infected computer. *Id.* ¶ 41. In this way, Defendants can use already infected computers to connect to other computers and engage in additional unlawful activity. *Id.* ¶ 70.

F. Damage To Computers And Microsoft

Aside from the harms listed above, the Shylock infection harms Microsoft and Microsoft's customers by damaging the customers' computers and the Microsoft-licensed software installed on their computers. *Id.* ¶¶ 71-72. During the infection of a user's computer, Shylock makes changes at the deepest and most sensitive levels of the computer's operating system. *Id.* ¶¶ 72-75; Diaz Decl. ¶¶ 10-19. When the Shylock executable infects a target computer, it disables the Windows firewall, removes antivirus software, and adds new users or escalates privileges of the current user. *Id.* ¶ 74.

In effect, once infected, altered and controlled by Shylock, the Windows operating system, Internet Explorer, and Firefox cease to operate normally and are now tools of deception and theft. *Id.* ¶ 75. Yet they still bear the Microsoft Windows and Internet Explorer trademarks. *Id*. This is obviously meant to confuse and mislead Microsoft's customers, and it causes extreme damage to Microsoft's brands and trademarks. *Id.* Customers are usually unaware of the fact that their computers are infected and have become part of a Shylock botnet. *Id.* ¶ 76. Even if aware of the infection, they often lack the technical resources or skills to resolve the problem, allowing their computers to be misused indefinitely. *Id.* ¶¶ 76-77. Even with professional assistance, cleaning an infected end-user computer can be exceedingly difficult, time-consuming, and frustrating. *Id.* ¶ 77.

1. Shylock Causes Severe Injury To Microsoft

Microsoft, as a provider of the Windows® operating system and Internet Explorer® web browser, must incorporate security features in an attempt to stop account credential theft by the Shylock botnets from occurring to customers using Microsoft's software. *Id.* ¶¶ 78-79. Additionally, Microsoft devotes significant computing and human resources to combating infections by Shylock and helping customers determine whether or not their computers are infected, and if so, cleaning them. *Id.* ¶ 82. Customers' frustration with having to deal with botnet infections on their computers, discussed above, unfairly diminishes their regard for Windows and Microsoft, and tarnishes Microsoft's reputation and goodwill. *Id.* ¶¶ 81-82.

2. Shylock Causes Severe Injury To Third Parties And The Public

Shylock causes injury to numerous financial institutions, whose interests are represented by the trade group FS-ISAC, Microsoft, and its individual customers whose information and funds are stolen. *Id.* ¶ 83; Guerrino Decl. ¶17. Like Microsoft, FS-ISAC and its member organizations have devoted substantial resources to investigate and remediate the harm the Shylock botnets cause. Guerrino Decl. ¶ 10. In addition, FS-ISAC member institutions have their trademarks, brand names, and trade names misused to deceive owners of Shylock-infected computers to provide Defendants their login credentials and other personal identifying information. *Id.* ¶ 16. FS-ISAC member institutions, moreover, suffer direct financial harm as a result of Defendants' unlawful conduct. Defendants and the Shylock botnets have cost FSI-ISAC member institutions millions is losses. *Id.* ¶ 10.

I. LEGAL STANDARD

The purpose of a preliminary injunction is to protect the status quo and to prevent irreparable harm during the pendency of a lawsuit and to preserve the court's ability to render a meaningful judgment on the merits. *United States v. South Carolina*, 720 F.3d 518, 524 (4th Cir. 2013) (citations omitted). "Parties seeking a preliminary injunction must demonstrate that (1) they are likely to succeed on the merits, (2) they are likely to suffer irreparable harm, (3) the balance of hardships tips in their favor, and (4) the injunction is in the public interest. *Metro.*

Reg'l Info. Sys. v. Am. Home Realty Network, Inc., 722 F.3d 591, 595 (4th Cir. 2013) (citing *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008)).

II. PLAINTIFFS' REQUESTED RELIEF IS WARRANTED

This matter presents a quintessential case for injunctive relief. Defendants' conduct causes irreparable harm to Plaintiffs, their customers and member institutions, and the general public. Every day that passes gives Defendants an opportunity to steal online banking credentials, steal victims' money, and expand their botnet enterprise. Unless enjoined, Defendants will continue to cause irreparable harm to Plaintiffs and their customers.

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

Even at this early stage in the proceedings, the record demonstrates that Plaintiffs will be able to establish the elements of each of their claims. The evidence in support of Plaintiffs' TRO application is based on the diligent work of experienced investigators and is supported by substantial empirical evidence and forensic documentation. In short, there is no legitimate dispute about what the Shylock botnets and Shylock malware do. Given the strength of Plaintiffs' evidence, the likelihood of success on the merits weighs heavily in favor of granting injunctive relief.

1. Defendants' Conduct Violates the CFAA

Congress enacted the CFAA specifically to address computer crime. *See, e.g., Big Rock Sports, LLC v. AcuSport Corp.*, 2011 U.S. Dist. LEXIS 110995, 3 (E.D.N.C. Sept. 26, 2011). "Any computer with Internet access [is] subject [to] the statute's protection." *Id. Inter alia*, the CFAA penalizes a party that: (1) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage, 18 U.S.C. § 1030(a)(5)(C); or (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer, 18 U.S.C. § 1030(a)(2)(C); or (3) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage to a protected computer, 18 U.S.C. § 1030(a)(5)(A).

A "protected computer" is a computer "used in interstate or foreign commerce or communication." *E.g., SecureInfo Corp. v. Telos Corp*., 387 F. Supp. 2d 593, 608 (E.D. Va. 2005). The phrase "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to obtain or alter." *Id.* (citing 18 U.S.C. § 1030(e)(6)). In order to prosecute a civil claim under the CFAA, a plaintiff must demonstrate loss or damage in excess of $5,000.[1] The CFAA defines loss as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Sprint Nextel Corp. v. Simple Cell, Inc*., 2013 U.S. Dist. LEXIS 99580, 21 (D. Md. July 17, 2013) (citing 18 U.S.C. § 1030(e)(8)). "Damage. . . means any impairment to the integrity or availability of data, a program, a system, or information." *Id*. (citing 18 U.S.C. § 1030(e)(11)). "The Fourth Circuit has recognized that this 'broadly worded provision plainly contemplates consequential damages' such as 'costs incurred as part of the response to a CFAA violation, including the investigation of an offense.'" *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009). The CFAA permits plaintiffs to aggregate multiple intrusions or violations for the purposes of meeting the $5,000 statutory threshold. *See Sprint Nextel Corp.,* 2013 U.S. Dist. LEXIS 99580, 21 (citations omitted).

[1] Trade associations such as FS-ISAC have standing to assert claims arising from injuries to trade association members where the test for associational standing is met. *See, e.g., American Booksellers Ass'n v. Virginia*, 802 F.2d 691, 694 n.5 (4th Cir. 1986). FS-ISAC's claims and requested relief meet the associational standing test here, because (a) its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organization's purpose; and (c) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit. *Hunt v. Wash. State Apple Adver. Comm'n*, 432 U.S. 333, 343 (1977) *partially superseded as to claims under the WARN Act as stated in United Food & Commer. Workers Union Local 751 v. Brown Group,* 517 U.S. 544, 546 (1996).

In sum, in order to prevail on their CFAA claim, Plaintiffs must establish that Defendants (1) accessed a protected computer; (2) without authorization; (3) for the purpose of obtaining information or defrauding others; (4) resulting in loss or damage in excess of $5,000. The Patel, Diaz, and Guerrino Declarations establish that Defendants' conduct satisfies each of these elements. First, each of the computers comprising the Shylock botnets is, by definition, a protected computer, because only computers that connect to the Internet can possibly be infected. *See* Section A, *supra*; 18 U.S.C. § 1030(e)(2)(B) (defining "protected computer" as a computer "used in interstate or foreign commerce or communication"). Second, each computer infected with the Shylock malware has been accessed without authorization—Defendants surreptitiously installed the malware onto the infected machines without their owner's knowledge or consent. *See* Section C.3, *supra*. Third, installation of the Shylock malware is carried out for the purpose of obtaining user credentials and defrauding users and banks. *See* Section D, *supra.* Defendants, moreover, damage the infected computer's operating system—*inter alia*—by impairing the integrity of the Windows registry and master boot log. *See* Section F.1, *supra.* Finally, the amount of harm caused by the Shylock botnets exceeds $5,000. *See* Sections A, D, and E, *supra.*

Defendants' conduct is precisely the type of activity that the Computer Fraud and Abuse Act is designed to prevent. *See, e.g.*, *Physicians Interactive v. Lathian Sys., Inc.*, 1:03-cv-01193, 2003 U.S. Dist. LEXIS 22868, at *26 (E.D. Va. Dec. 5, 2003) (granting TRO and preliminary injunction under CFAA where defendant hacked into a computer and stole confidential information) *partially abrogated on other grounds as stated in ForceX, Inc. v. Tech. Fusion, LLC*, 2011 U.S. Dist. LEXIS 69454, at * 12 (E.D. Va. June 27, 2011); *Global Policy Partners, LLC v. Yessin*, 1:09-cv-00859, 2009 U.S. Dist. LEXIS 112472, *9-13 (E.D. Va. Nov. 24, 2009) (accessing computer using credentials that did not belong to defendant actionable under the CFAA); *see also United States v. Phillips,* 477 F.3d 215, 219 (5th Cir. 2007) (noting that CFAA is concerned with "outside hackers who break into a computer") (citations to legislative history omitted).

2. Defendants' Conduct Violates the ECPA

"The ECPA, in pertinent part, prohibits intentionally intercepting any electronic communication." *Global Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631, 637 (E.D. Va. 2009) (citing 18 U.S.C. § 2511(1)(a)); *see also Brown v. Waddell*, 50 F.3d 285, 289 (4th Cir. 1995) (discussing prohibition on unauthorized interception of electronic communications). "Intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Global Policy Partners,* 686 F. Supp. 2d at 637. The ECPA also prohibits use of information obtained in violation of section 2511. 18 U.S.C. § 2511(1)(d). Persons injured by violations of the ECPA may bring a civil suit to obtain injunctive relief and damages. *E.g., DIRECTV, Inc. v. Benson*, 333 F. Supp. 2d 440, 449 (M.D.N.C. 2004).

Defendants' conduct in operating the Shylock botnets violates the ECPA because the Shylock malware intercepts Internet communications between a user and her bank. *See* Section D, *supra*. For example, when Shylock conducts a web-inject attack, the malware intercepts a user's communication of login information to banking institutions and redirects such communications to computers controlled by Defendants. *See* Patel Decl. ¶¶ 58-68. Defendants then knowingly use these intercepted communications to access user bank accounts to facilitate theft. *Id*. Hacking into a computer and intercepting Internet communications clearly violates the ECPA. *See, e.g., Sharma v. Howard County*, 2013 U.S. Dist. LEXIS 18890, 19 (D. Md. Feb. 12, 2013).

3. Defendants' Conduct Violates the Lanham Act

Section 1114(1) of the Lanham Act prohibits use of a reproduction, counterfeit, copy or "colorable imitation" of a registered mark in connection with the distribution of goods and services where such use is likely to cause confusion or mistake or to deceive. E*.g., George & Co., LLC, v. Imagination Entm't Ltd.*, 575 F.3d 383, 393 (4th Cir. 2009) (citing 15 U.S.C. § 1114(1)(a)). Defendants distribute copies of Microsoft's registered, famous and distinctive trademarks in fraudulent versions of Defendants' Windows operating system and Internet

Explorer browser, which deceive victims, causing them confusion and causing them to mistakenly associate Microsoft with this activity. Defendants make use of counterfeit reproductions of Plaintiffs' marks, *inter alia*, by causing consumers to use adulterated products that bear the Microsoft and Windows trademarks. Defendants similarly misuse the trademarks of FS-ISAC's third-party financial institutions as well. *See* Section F, *supra*.

The Shylock botnets also make such use of trademarks in website templates and spam templates that Defendants then use 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. Indeed, "courts have almost unanimously presumed a likelihood of confusion upon a showing that the defendant intentionally copied the plaintiff's trademark or trade dress." *Larsen v. Terk Techs. Corp.*, 151 F.3d 140, 149 (4th Cir. 1998).

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

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

15 U.S.C. § 1125(a)(1)(A). The Shylock botnets' misleading and false use of Microsoft's trademarks—including "Microsoft," "Windows," and "Internet Explorer"—and also the trademarks of FS-ISAC member institutions, causes confusion and mistakes as to their affiliation with Defendants' malicious conduct. *See* Sections F, *supra*. This activity is a clear violation of Lanham Act § 1125(a) and Plaintiffs are likely to succeed on the merits. *See 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.*, 2008 U.S.

Dist. LEXIS 112056 at *1-3 (same; granting TRO); *Am. Online v. IMS*, 24 F. Supp. 2d 548, 551-552 (E.D. Va. 1998) (misuse of trademark in e-mail headers violated §1125(a); also constituted trademark "dilution" under §1125(c)); *Brookfield Commc'ns.*, 174 F. 3d at 1066-67 (entering preliminary injunction under Lanham Act §1125(a) for infringement of trademark in software and website code); *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)).

4. Defendants' Conduct is Tortious

Defendants' conduct is tortious under the common law doctrines of trespass to chattels, conversion, and unjust enrichment. Under Virginia law, the tort of conversion "encompasses any wrongful exercise or assumption of authority . . . over another's goods, depriving him of their possession; and any act of dominion wrongfully exerted over property in denial of the owner's right, or inconsistent with it." *United Leasing Corp. v. Thrift Ins. Corp*., 247 Va. 299, 305 (Va. 1994) (quotation omitted). The related tort of trespass to chattels—sometimes referred to as "the little brother of conversion"—applies where "personal property of another is used without authorization, but the conversion is not complete." *Dpr Inc. v. Dinsmore*, 82 Va. Cir. 451, 458 (Va. Cir. Ct. 2011) (citations omitted). Here, Defendants exercised dominion and authority over Microsoft's proprietary Windows and Internet Explorer by injecting code into Microsoft's software that fundamentally changed important functions of the software. This act deprived Microsoft of its right to control the content, functionality, and nature of its software. *See, e.g., Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 698 (D. Md. 2011) (holding defendant liable for conversion where defendant replaced current version of plaintiffs' website with former version, because such action effectively "dispossessed [plaintiff] of the chattel;" i.e., its website). District courts in the Fourth Circuit have recognized that computer hacking can amount to tortious conduct under the doctrines of conversion and trespass to chattels. *See*

Microsoft Corp. v. Doe, 2014 U.S. Dist. LEXIS 48398, 24-25 (E.D. Va. Jan. 6, 2014) ("The unauthorized intrusion into an individual's computer system through hacking, malware, or even unwanted communications supports actions under these claims"); *see also Microsoft Corp. v. Does*, 2013 U.S. Dist. LEXIS 168237, 3 (W.D.N.C. Nov. 21, 2013) (similar). Moreover, the object of Defendants' conduct is to ultimately convert monies belonging to FS-ISAC member institutions.

B. Defendants' Conduct Causes Irreparable Harm

It is well settled that consumer confusion and injury to business goodwill constitute irreparable harm. *See, e.g., Int'l Labor Mgmt. Corp. v. Perez,* 2014 U.S. Dist. LEXIS 57803, 35 (M.D.N.C. Apr. 25, 2014) (damage to "reputation and loss of goodwill constitutes irreparable harm for purposes of injunctive relief") (citing *In Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.*, 22 F.3d 546 (4th Cir. 1994)); *MicroAire Surgical Instruments, LLC v. Arthrex, Inc.*, 726 F. Supp. 2d 604, 635 (W.D. Va. 2010) ("The loss of goodwill is a well-recognized basis for finding irreparable harm"). A finding of irreparable harm usually follows a finding of unlawful use of a trademark and a likelihood of confusion. *Ledo Pizza Sys. v. Singh*, 2013 U.S. Dist. LEXIS 146938, 9 (D. Md. Oct. 10, 2013); *Nabisco Brands, Inc. v. Conusa Corp.*, 722 F. Supp. 1287, 1290 (M.D.N.C. 1989) ("In the context of a trademark infringement dispute, several courts have held that where likelihood of confusion is established likelihood of success on the merits as well as risk of irreparable harm follow.").

Here, the Shylock botnets tarnish Plaintiffs' valuable trademarks, 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 Microsoft and FS-ISAC member institutions. 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. "[C]ircumstances[] such as insolvency or unsatisfiability of a money judgment, can show irreparable harm." *Khepera-Bey v. Santander Consumer USA, Inc*., 2013 U.S. Dist. LEXIS 87641, 13-14 (D. Md. June 21, 2013); *accord Burns v. Dennis-Lambert Invs., Ltd. P'ship,* 2012 Bankr. LEXIS 1107, 9 (Bankr. M.D.N.C. Mar. 15, 2012) ("a preliminary injunction may be appropriate where 'damages may be unobtainable from the defendant because he may become insolvent before final judgment can be entered.'"); *Rudolph v. Beacon Indep. Living LLC,* 2012 U.S. Dist. LEXIS 7075, 5 (W.D.N.C. Jan. 23, 2012) ("Irreparable harm exists here because of Defendant Beacon's continued occupancy of the Facility without paying any rents, particularly in light of the threat of insolvency by one or more Defendants.").

C. The Balance of Equities Strongly Favor Injunctive Relief

Because Defendants are engaged in an illegal scheme to defraud consumers and injure Plaintiffs, the balance of equities clearly tips in favor granting an injunction. *See, e.g., US Airways, Inc. v. US Airline Pilots Ass'n,* 813 F. Supp. 2d 710, 736 (W.D.N.C. 2011); *Pesch v. First City Bank of Dallas,* 637 F. Supp. 1539, 1543 (N.D. Tex. 1986) (balance of hardships clearly favors injunction where enjoined activity is illegal). On one side of the scales of equity rests the harm to Plaintiffs and their customers caused by the Shylock botnets, while on the other side rests no legally cognizable harm to Defendants because an injunction would only require them to cease illegal activities. *US Airways,* 13 F. Supp. 2d at 736.

D. The Public Interest Favors an Injunction

It is clear that an injunction would serve the public interest here. Every day that passes presents the opportunity for new computers to be infected, for more members of the public to be deceived, and for more money to be stolen from innocent persons' bank accounts. Moreover, the public interest is clearly served by enforcing statutes designed to protect the public, such as the Lanham Act, CFAA, and ECPA. *See, e.g., BSN Med., Inc. v. Art Witkowski*, 2008 U.S. Dist. LEXIS 95338, 10 (W.D.N.C. Nov. 21, 2008) ("In a trademark case, the public interest is 'most often a synonym for the right of the public not to be deceived or confused.' . . .the infringer's use damages the public interest.") (citation omitted); *accord Meineke Car Care Ctrs., Inc. v. Bica,* 2011 U.S. Dist. LEXIS 118171, 10 (W.D.N.C. Oct. 12, 2011) (similar); *Dish Network LLC v. Parsons,* 2012 U.S. Dist. LEXIS 75386, 8-9 (W.D.N.C. May 30, 2012) (public interest weighed in favor of injunction to enforce ECPA); *Microsoft Corp. v. Doe,* 2014 U.S. Dist. LEXIS 48398, 32 (E.D. Va. Jan. 6, 2014) (public interest weighed in favor of injunction to enforce CFAA).

Notably, most courts that have confronted requests for injunctive relief targeted at disabling malicious computer botnets have granted such relief. Heath Decl. Ex. 25 (*Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (Ex Parte TRO to dismantle botnet command and control servers); Exs. 21 and 22 (*Microsoft v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (Ex Parte TRO and preliminary injunction to dismantle botnet command and control servers); Exs. 17 and 18 (*Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va., Brinkema J.) (same); Exs. 19 and 20 (*Microsoft v. John Does 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.) (same); Exs. 23 and 24 (*Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) (same); Exs. 13 & 14 (*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-party registries, hosting companies, and ISPs whose infrastructure Defendants rely on to operate the Shylock botnets 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 located abroad, and thus their cooperation is necessary.[2]

[2] The Proposed Order also includes a non-binding request for voluntary cooperation from hosting companies through which Defendants procured the IP addresses and domains used to control the Shylock botnets.

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. at 174 (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, 30 (E.D. Va. Jan. 6, 2014) (invoking All Writs act and granting relief similar to that requested herein); *United States v. X,* 601 F. Supp. 1039, 1042 (D. Md. 1984) (All Writs Act permits the district court to order a third party to provide "nonburdensome technical assistance" in aid of valid warrant); *Moore v. Tangipahoa Parish Sch. Bd*., 507 Fed. App'x. 389, 396 (5th Cir. 2013) (unpublished) ("The All Writs Act provides 'power to a federal court to issue such commands . . . as may be necessary or appropriate to effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained.'") (citing *New York Tel. Co*., 434 U.S. at 172); *see also In re Application of United States 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*., "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.'" 434 U.S. at 172); *In re Baldwin-United Corp*., 770 F.2d 328, 338-339 (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"; "We do 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.*, 2007 U.S. Dist. LEXIS 98676, at

*16 (All Writs Act applied in conjunction with trademark seizure under Rule 65 and Lanham Act).

Requiring these third parties to reasonably assist in the execution of this order will not offend due process as the Proposed Order (1) requires only minimal assistance from the third parties in executing the order (acts that they would take in the ordinary course of their operations), (2) requires that it be implemented with the least degree of interference with the normal operation of third parties, (3) does not deprive the third parties of any tangible or significant property interests and (4) requires 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. **<u>An *Ex Parte* TRO and Preliminary Injunction Is the Only Effective Means of Relief, and Alternative Service Is Warranted Under the Circumstances</u>**

The TRO Plaintiffs request must issue *ex parte* for the relief to be effective at all because of the extraordinary factual circumstances here—namely, Defendants' technical sophistication and ability to move their malicious infrastructure if given advance notice of Plaintiffs' request for injunctive relief. Rule 65 of the Federal Rules of Civil Procedure permits an *ex parte* TRO where the moving party sets forth facts that show an immediate and irreparable injury and why notice should not be required. Fed. R. Civ. P. 65(b)(1); *see Granny Goose Foods, Inc. v. Brotherhood of Teamsters & Auto Truck Drivers, Lcal No. 70*, 415 U.S. 423, 438-39 (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 distribute updated configuration files throughout the Shylock botnets and/or direct the command and control domains to new IP addresses before the TRO can have any remedial effects. Thus, providing notice of the requested TRO will undoubtedly facilitate efforts of the parties controlling the botnet. It is well established that *ex parte* relief is appropriate under circumstances such as the instant case, where notice would render the requested relief ineffective. *See, e.g., AllscriptsMisys, LLC v. Am. Digital Networks, LLC*, 1:10-cv-00111, 2010 U.S. Dist. LEXIS 4450, at *2 (D. Md. Jan. 20, 2010) (granting an *ex parte* TRO where "Defendant may dissipate the funds and/or take action to render it difficult to recover funds …."); *Crosby v. Petromed, Inc*., 2:09-cv-05055, 2009 U.S. Dist. LEXIS 73419, at *5 (E.D. Wash. Aug. 6, 2009) (granting *ex parte* TRO as "notice to Defendants of this TRO request could result in further injury or damage to Plaintiffs...."); *AT&T Broadband v. Tech Commc'ns, Inc*. 381 F.3d 1309, 1319-1320 (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 Center v. Exxon Co.*, U.S.A., 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"); *Kelly v. Thompson*, 2010 U.S. Dist. LEXIS 31800, *3 (W.D. Tex. Mar. 31, 2010) (granting *ex parte* TRO without notice where irreparable harm would result if notice were 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 already shift the location of their infrastructure periodically in order to stay ahead of counter-measures from the security industry. Where there is evidence that operators of botnets 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 1-27, Microsoft Corp. v. Peng Yong*, and *Microsoft Corp. v. Piatti*, all cases in which the district court issued *ex parte* TROs to disable botnets, recognizing the risk that Defendants would move the botnet infrastructure and destroy evidence if prior notice were given. (*See* Heath Decl., Exs. 21, 22, 25, 17, and 18.)

Similarly, in *FTC v. Pricewert LLC*, the district court issued an *ex parte* TRO suspending Internet connectivity of a company enabling botnet activity and other illegal computer-related conduct on the basis that "Defendant is likely to relocate the harmful and malicious code it hosts and/or warn its criminal clientele of this action if informed of the [plaintiff's] action." *See* Heath Decl., Ex. 10 (*FTC v. Pricewert LLC et al.,* Case No. 09-2407) (N.D. Cal., Whyte J.) at pg. 3. Moreover, the court in *Dell, Inc. v. Belgiumdomains, LLC*, 1:07-cv-22674, 2007 U.S. Dist. Lexis 98676, at *4-5 (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 *4. 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.* at *5-6.

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

Plaintiffs Will Provide Notice To Defendants By Personal Delivery: Plaintiffs have identified IP addresses, domains, and name servers from which the Shylock command and control software operates, and, pursuant to the TRO, will obtain from the hosting companies and domain registrars/registries any and all physical addresses of the Defendants. Pursuant to Rules 4(e)(2)(A) and 4(f)(3), Plaintiffs plan to effect formal notice of the preliminary injunction hearing and service of the complaint by hand delivery of the summons, Plaintiffs' Complaint, the instant motion and supporting documents, and any Order issued by this Court to such addresses in the U.S**.** Heath Decl. ¶ 13.

Plaintiffs Will Provide Notice By E-mail, Facsimile And Mail: Plaintiffs have identified 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. *Id.* ¶ 10. Plaintiffs will provide notice of the preliminary injunction hearing and will effect service of the Complaint by immediately sending the same pleadings described above to the e-mail addresses, facsimile numbers and mailing addresses that Defendants provided to the hosting companies, registrars, and registries. *Id.* ¶ 10. When Defendants registered for domain names and IP addresses, 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.* ¶¶ 33-34.

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, publically accessible source on the Internet for a period of 6 months. *Id.* ¶ 11.

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

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

First, legal notice and service by e-mail, facsimile, mail and publication satisfies Due Process as these means are reasonably calculated, in light of the circumstances, to apprise the interested parties of the TRO, the preliminary injunction hearing and the lawsuit. *See Mullane v. Central Hanover Bank & Trust Co.*, 339 U.S. 306, 314 (1950). Such methods are also authorized under Federal Rule of Civil Procedure 4(f)(3), which allows a party to serve defendants by means not prohibited by international agreement. The methods of notice and service proposed by Microsoft have been approved in other cases involving international defendants attempting to evade authorities. *See e.g.*, *Rio Properties, Inc. v. Rio Int'l. Interlink,* 284 F.3d 1007, 1014-1015 (9th Cir. 2002) (authorizing service by e-mail upon an international defendant); Heath Decl., Ex. 16 (*Microsoft Corp. v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va. 2010, Brinkema J.)); *Smith v. Islamic Emirate of Afghanistan*, 2001 U.S. Dist. LEXIS 21712 (S.D.N.Y. 2001) (authorizing service by publication upon Osama bin Laden and the al-Qaeda organization); *FMAC Loan Receivables v. Dagra,* 228 F.R.D. 531, 535036 (E.D. Va. 2005) (acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means); *BP Products North Am., Inc. v Dagra,* 236 F.R.D. 270, 271-73 (E.D. Va. 2006) (approving notice by publication); *AllscriptsMisys, LLC v. Am. Digital Networks, LLC,* 2010 U.S. Dist. LEXIS 4450, *3 (D. Md. 2010) (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.").

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 recently 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 1014-1015. Notably, *Rio Properties* has been followed in the Fourth Circuit. *See FMAC Loan Receivables*, 228 F.R.D. at 534 (E.D. Va. 2005) (following *Rio*); *BP Prods. N. Am, Inc.*, 232 F.R.D. at 264 (E.D. Va. 2005) (same); *Williams v. Adver. Sex L.L.C.*, 231 F.R.D. 483, 486 (N.D. W. Va. 2005) ("The Fourth Circuit Court of Appeals has not addressed this issue. Therefore, in the absence of any controlling authority in this circuit, the Court adopts the reasoning of the Ninth Circuit in *Rio Properties, Inc. ....*").

In this case, the e-mail addresses provided by Defendants to the hosting companies and domain registrars, in the course of obtaining services that support the botnet, 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 their botnet by those means, as Defendants agreed to such in their agreements. *See Nat'l Equip. Rental, Ltd. v. Szukhent*, 375 U.S. 311 (1964) ("And it is settled … that parties to a contract may agree in advance to submit to the jurisdiction of a given court, to permit notice to be served by the opposing party, or even to waive notice altogether."). For these reasons, notice and service by e-mail and publication are warranted and necessary here.[3]

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

[3] Additionally, if the physical addressees provided by Defendants to hosting companies turns 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 Products North Am., Inc.*, 236 F.R.D. at 271 ("The Hague Convention does not apply in cases where the address of the foreign party to be served is unknown.")

III. 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: June 27, 2014

Respectfully submitted,

LAUREN J. PARKER
Va. State Bar No. 77018
Attorneys for Plaintiffs Microsoft Corp. and FS-ISAC, Inc.
ORRICK, HERRINGTON & SUTCLIFFE LLP
Columbia Center
1152 15th Street, N.W.
Washington, D.C. 20005-1706
Telephone: (202) 339-8400
Facsimile: (202) 339-8500
lparker@orrick.com

Of counsel:

GABRIEL M. RAMSEY (*pro hac vice* application pending)
JACOB M. HEATH (*pro hac vice* application pending)
ROBERT URIARTE (*pro hac vice* application pending)
Attorneys for Plaintiffs Microsoft Corp. and FS-ISAC, Inc.
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401
gramsey@orrick.com
jheath@orrick.com
ruriarte@orrick.com