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 MICROSOFT AND ITS CUSTOMERS,

Defendants.

Civil Action No: 1:14CV811
LOG/TCB

FILED UNDER SEAL

COMPLAINT

Plaintiffs MICROSOFT CORP. ("Microsoft") and FS-ISAC, INC., ("FS-ISAC") hereby complain and allege that JOHN DOES 1-8 (collectively "Defendants") are controlling a global network of interconnected illegal computer networks, collectively known as the "Shylock botnets," comprised of user computers connected to the Internet that Defendants have infected with malicious software. Defendants have used the Shylock botnets to infect computers on the Internet that Defendants then use to steal millions of dollars. Defendants control the Shylock botnets through a sophisticated command and control infrastructure hosted at and operated through Internet domains ("domains") and domain name servers set forth at Appendix A to this Complaint (the "Shylock domains"), Internet Protocol addresses set forth at Appendix B to this Complaint (the "Shylock IP addresses") (collectively the "Shylock command and control infrastructure"). Plaintiffs allege as follows:

NATURE OF ACTION

1. This is an action based upon: (1) The Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Electronic Communications Privacy Act, 18 U.S.C. § 2701; (3) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 et seq. (4) False Designation of Origin

under The Lanham Act, 15 U.S.C. § 1125(a); (5) Trademark Dilution under The Lanham Act, 15 U.S.C. § 1125(c); (6) the Racketeer Influence and Corrupt Organizations Act (18 U.S.C. § 1962(c)); (7) Common Law Trespass to Chattels; (8) Unjust Enrichment; and (9) Conversion. Plaintiffs seek injunctive and other equitable relief and damages against Defendants who operate controlled networks of computers—*i.e.*, the "Shylock" botnets—through the Shylock Command and Control Infrastructure. Defendants, using the Shylock botnets, have caused and continue to cause irreparable injury to Plaintiffs, their member organizations and customers, and the public.

PARTIES

2. Plaintiff Microsoft is a corporation duly organized and existing under the laws of the State of Washington, having its headquarters and principal place of business in Redmond, Washington.

3. Plaintiff FS-ISAC, Inc. is a non-profit corporation duly organized and existing under the laws of Delaware, having its headquarters and principal place of business in Reston, Virginia. FS-ISAC is a membership organization comprised of 4,400 organizations including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, payment processors, and over 20 trade associations representing the majority of the U.S. financial services sector. FS-ISAC represents the interests of its financial services industry members in combating and defending against cyber threats that pose risk and loss to the industry.

4. On information and belief, **John Doe 1** controls the Shylock botnet identified as the "USA" botnet in furtherance of conduct designed to cause harm to Plaintiffs, their customers, and the public. Plaintiffs are informed and believe and thereupon allege that John Doe 1 can likely be contacted directly or through third-parties using the information set forth in Appendices A and B.

5. On information and belief, **John Doe 2** controls the Shylock botnet identified as the "HJ-UK-1" botnet in furtherance of conduct designed to cause harm to Plaintiffs, their customers, and the public. Plaintiffs are informed and believe and thereupon allege that John Doe 2 can likely be contacted directly or through third-parties using the information set forth in Appendices A and B.

6. On information and belief, **John Doe 3** controls the Shylock botnet identified as the “HJ-UK-2” botnet in furtherance of conduct designed to cause harm to Plaintiffs, their customers, and the public. Plaintiffs are informed and believe and thereupon allege that John Doe 3 can likely be contacted directly or through third-parties using the information set forth in Appendices A and B.

7. On information and belief, **John Doe 4** controls the Shylock botnet identified as the “HJ-UK-3” botnet in furtherance of conduct designed to cause harm to Plaintiffs, their customers, and the public. Plaintiffs are informed and believe and thereupon allege that John Doe 4 can likely be contacted directly or through third-parties using the information set forth in Appendices A and B.

8. On information and belief, **John Doe 5** controls the Shylock botnet identified as the “HJ-UK-4” botnet in furtherance of conduct designed to cause harm to Plaintiffs, their customers, and the public. Plaintiffs are informed and believe and thereupon allege that John Doe 5 can likely be contacted directly or through third-parties using the information set forth in Appendices A and B.

9. On information and belief, **John Doe 6** controls the Shylock botnet identified as the “Net1” botnet in furtherance of conduct designed to cause harm to Plaintiffs, their customers, and the public. Plaintiffs are informed and believe and thereupon allege that John Doe 6 can likely be contacted directly or through third-parties using the information set forth in Appendices A and B.

10. On information and belief, **John Doe 7** controls the Shylock botnet identified as the “Net2” botnet in furtherance of conduct designed to cause harm to Plaintiffs, their customers, and the public. Plaintiffs are informed and believe and thereupon allege that John Doe 7 can likely be contacted directly or through third-parties using the information set forth in Appendices A and B.

11. On information and belief, **John Doe 8** controls the Shylock botnet identified as the “Net3” botnet in furtherance of conduct designed to cause harm to Plaintiffs, their customers, and the public. Plaintiffs are informed and believe and thereupon allege that John Doe 8 can

likely be contacted directly or through third-parties using the information set forth in Appendices A and B.

12. Third parties VeriSign Naming Services and VeriSign Global Registry Services (collectively, "VeriSign") are the domain name registries that oversee the registration of all domain names ending in ".net," ".cc," and ".com." VeriSign Name Services is located at 21345 Ridgetop Circle, 4th Floor, Dulles, Virginia 20166. VeriSign Global Registry Services is located at 12061 Bluemont Way, Reston, Virginia 20190.

13. Set forth in Appendices A and B are the identities of and contact information for third party domain registries that control the domains used by the Defendants and third party hosting companies that control servers used by the Defendants.

14. On information and belief, John Does 1-8 jointly own, control, maintain, and do business under the names of the Shylock botnets and Shylock Command and Control Infrastructure. Plaintiffs will amend this complaint to allege the Doe Defendants' true names and capacities when ascertained. Plaintiffs will exercise due diligence to determine Doe Defendants' true names, capacities, and contact information, and to effect service upon those Doe Defendants.

15. Plaintiffs are informed and believe and thereupon allege that each of the fictitiously named Doe Defendants is responsible in some manner for the occurrences herein alleged, and that Plaintiffs' injuries as herein alleged were proximately caused by such Defendants.

16. On information and belief, the actions and omissions alleged herein to have been undertaken by John Does 1-8 were actions that Defendants, and each of them, authorized, controlled, directed, or had the ability to authorize, control or direct, and/or were actions and omissions each Defendant assisted, participated in, or otherwise encouraged, and are actions for which each Defendant is liable. Each Defendant aided and abetted the actions of Defendants set forth below, in that each Defendant had knowledge of those actions and omissions, provided assistance and benefited from those actions and omissions, in whole or in part. Each Defendant was the agent of each of the remaining Defendants, and in doing the things hereinafter alleged,

was acting within the course and scope of such agency and with the permission and consent of other Defendants.

JURISDICTION AND VENUE

17. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises out of Defendants' violation of the Federal Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Racketeer Influence and Corrupt Organizations Act (18 U.S.C. § 1962(c)); and the Lanham Act (15 U.S.C. §§ 1114, 1125). The Court, also has subject matter jurisdiction over Plaintiffs' claims for trespass to chattels, unjust enrichment, and conversion pursuant to 28 U.S.C. § 1367.

18. On information and belief, venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Plaintiffs' claims has occurred in this judicial district, and because a substantial part of the property that is the subject of Plaintiffs' claims is situated in this judicial district. Defendants maintain computers and Internet websites and engage in other conduct availing themselves of the privilege of conducting business in Virginia and have utilized instrumentalities located in Virginia and the Eastern District of Virginia to carry out the acts of which Plaintiffs complain.

19. Defendants have affirmatively directed actions at Virginia and the Eastern District of Virginia by directing malicious computer code at the computers of individual users located in Virginia and the Eastern District of Virginia, attempting to infect those user computers with the malicious code and to make the user computers part of the "botnet," which is used to injure Plaintiffs, their customers, and the public. The following figures depict the geographical location of user computers in Virginia (**Figure 1**) and the Eastern District of Virginia (**Figure 2**) against which Defendants are known to have directed malicious code, attempting to infect those computers and enlist them into the botnet:

Fig. 1

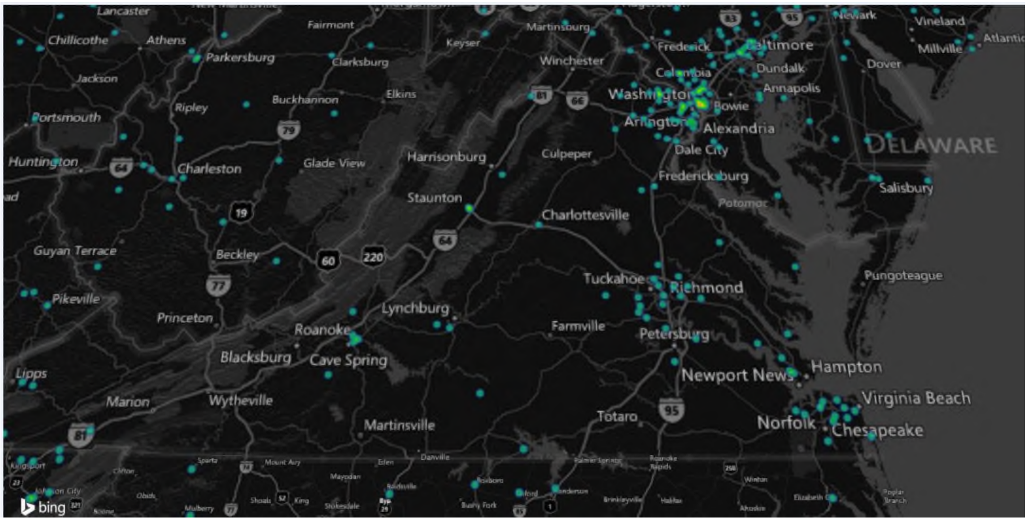
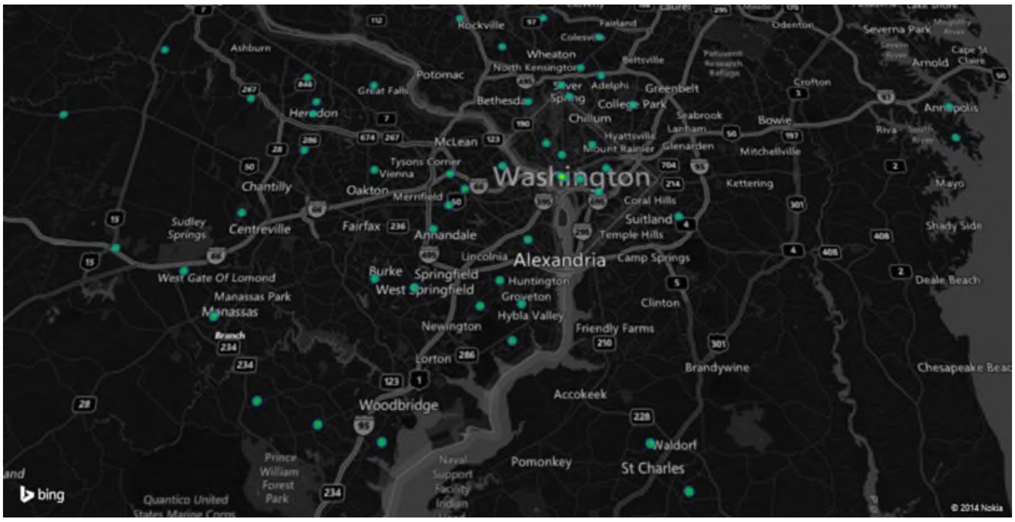


Fig. 2



20. Defendants maintain certain of the Shylock Domains registered through VeriSign and Public Interest Registry, which reside in the Eastern District of Virginia. Defendants use these domains to control the communications of the Shylock botnets that Defendants own, operate, and maintain in this judicial district. Defendants have undertaken the acts alleged herein with knowledge that such acts would cause harm through domains located in the Eastern District of Virginia, through the Shylock domains maintained through facilities in the Eastern District of Virginia, and through user computers located in the Eastern District of Virginia, thereby injuring

Plaintiffs, the customers and member organizations of Plaintiffs, and others in the Eastern District of Virginia and elsewhere in the United States. Therefore, this Court has personal jurisdiction over Defendants.

21. Pursuant to 28. U.S.C. § 1391(b), venue is proper in this judicial district. A substantial part of the events or omissions giving rise to Plaintiffs' claims, together with a substantial part of the property that is the subject of Plaintiffs' claims, are situated in this judicial district. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because Defendants are subject to personal jurisdiction in this judicial district.

FACTUAL BACKGROUND

Plaintiffs' Services And Reputation

22. Microsoft® is a provider of the Windows® operating system and the Internet Explorer® web browser, and a variety of other software and services. Microsoft has invested substantial resources in developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, establishing a strong brand and developing 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. Microsoft has registered trademarks representing the quality of its products and services and its brand, including Microsoft®, Windows®, and Internet Explorer®. Copies of the trademark registrations for the Microsoft, Windows, and Internet Explorer trademarks are attached as Appendix C to this Complaint.

23. Plaintiff FS-ISAC is a trade organization comprised of 4,400 organizations including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, payment processors, and over 20 trade associations representing the majority of the U.S. financial services sector. It was established by the financial services sector in response to the 1998 Presidential Directive 63, later updated by the 2003 Homeland Security Presidential Directive 7, which requires that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the United States' critical

infrastructure. (See www.fsisac.com/about/). Its purpose is "to enhance the ability of the financial services sector to prepare for and respond to cyber and physical threats, vulnerabilities and interests...." FS-ISAC's activities include actively coordinating and promoting financial industry detection, analysis, and response to cyber security threats. FS-ISAC works closely with various government agencies including the U.S. Department of Treasury, Department of Homeland Security (DHS), Federal Reserve, Federal Financial Institutions Examination Council regulatory agencies, United States Secret Service, Federal Bureau of Investigation, National Security Agency, Central Intelligence Agency, and state and local governments. Financial institutions that are members of FS-ISAC have generated substantial goodwill with their customers, establishing a strong brand and developing their respective names and the names of their products and services into strong and famous world-wide symbols that are well-recognized within their channels of trade.

Computer "Botnets"

24. A "botnet" is a collection of individual computers infected with malicious software ("malware") that allows communication among those computers and centralized or decentralized communication with other computers providing control instructions. A botnet network may be comprised of multiple, sometimes millions, of infected user computers. The individual computers in a botnet often belong to users who have unknowingly downloaded or been infected by malware. A user's computer, for example, may become part of a botnet when the user inadvertently interacts with a malicious website advertisement, clicks on a malicious email attachment, or downloads malware. In each instance, malware is downloaded or executed on the user's computer, causing that computer to become part of the botnet. Once part of a botnet, the user's computer is capable of sending and receiving communications, code, and instructions to or from other botnet computers.

25. Some botnets' computers are wholly within the control of the botnet creators. These may have specialized functions, such as sending control instructions to infected user computers. These are generally referred to as "command and control" computers.

26. Criminal organizations and individual cybercriminals often create, control,

maintain, and propagate botnets in order to carry out misconduct that harms others' rights. They use botnets because of botnets' ability to support a wide range of illegal conduct, their resilience against attempts to disable them, and their ability to conceal the identities of the malefactors controlling them. The controllers of a botnet will use an infected user computer for a variety of illicit purposes, unknown to the end user. A computer in a botnet, for example, may be used to:

a. carry out theft of credentials and information, fraud, computer intrusions, or other misconduct;

b. anonymously send unsolicited bulk email without the knowledge or consent of the individual user who owns the compromised computer;

c. deliver further malware to infect other computers; or

d. "proxy" or relay Internet communications originating from other computers, in order to obscure and conceal the true source of those communications.

27. Botnets provide a very efficient means of controlling a large number of computers and means of targeting any action internally against the contents of those computers or externally against any computer on the Internet.

Overview Of The Shylock Botnets

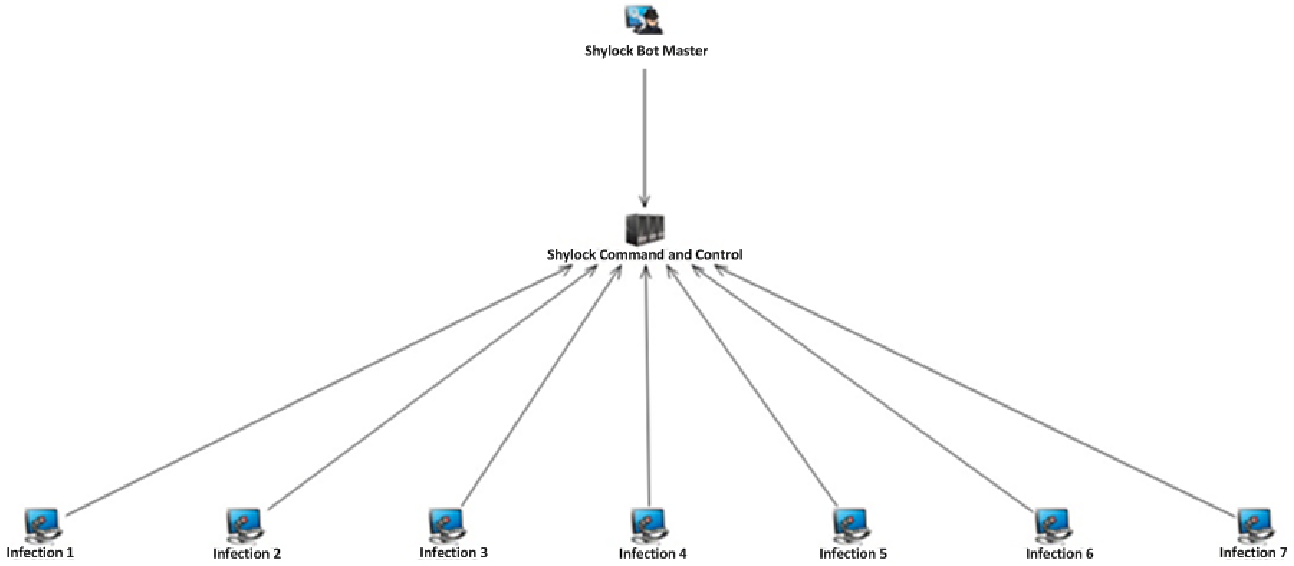
28. Plaintiffs bring this action to stop Defendants from harming Plaintiffs, the customers and member organizations of Plaintiffs, and the public, through the Shylock command and control infrastructure central to the Shylock botnets.

29. Defendants use the Shylock botnets primarily to gain access to account credentials for online banking websites to steal—among other things—funds from computer users and financial institutions. When a user of a Shylock-infected computer attempts to log onto a financial institutions website, Shylock (a) secretly hijacks the user's web browser, (b) captures the user's online financial login credentials and other personal identifying information, and (c) sends that information to Defendants. The user is unaware of Shylock's activity as Defendants have designed Shylock to hide itself and its unlawful activity on infected computers. After Shylock captures the user's login credentials and personal identifying information,

Defendants use that information, for example, to access the user's bank account. The user perceives only a normal login and is unaware of Defendants' surveillance and control of her computer and theft of her identity and of funds from her account.

The Shylock Botnets' Infrastructure

30. The Shylock botnets have a multi-tiered architecture that is represented below:



31. The lowest "**Infection Tier**" in this architecture is estimated to be comprised of Shylock-infected user computers. These computers may be home desktop computers, laptop computers, or computers in public libraries. These infected user computers are essentially the workers of the Shylock botnets, performing the day-to-day illegal activity, including the theft of user's credentials and the infection of other user computers.

32. Defendants use deceptive methods to infect user computers. Upon information and belief, Defendants controlling the Shylock botnets are part of a criminal enterprise that have infected legitimate websites and/or created websites designed specifically to infect user computers. When an unsuspecting user browses one or more of these websites, the user's computer is taken to another website where an "exploit pack" is downloaded and silently probes the user's computer for vulnerabilities, looking for an opportunity to execute code or place the

malware onto the system.

33. Once installed, the exploit pack downloads and installs the Shylock malware onto the user's computer. Defendants are known to infect advertisements on YouTube's advertising network to redirect users to compromised websites. Defendants have also targeted instant messenger applications, using them to send fake messages to other users of instant messaging services in an attempt to redirect users to exploit websites. Defendants, moreover, have given Shylock a Remote Access Tool ("RAT") that allows Defendants to access uninfected user computers on a Shylock-infected computer's local area network ("LAN"). This feature essentially gives Defendants a backdoor access into uninfected user computers that are not a part of the Shylock botnets.

34. Once infected, Defendants direct the Shylock-infected computers to engage in unlawful conduct, including (a) stealing users' online login credentials for financial institutions and other online accounts; (b) stealing users' personal identifying information; (c) stealing funds from users and financial institutions; (d) hijacking users' web browsers; (e) surveying users' computers for other sensitive information; as well as other illegal activity. Most if not all owners of Shylock-infected computers are unaware that their machines are infected and operating as part of the Shylock botnets.

35. At the highest tier in the architecture, the "**Command and Control Tier**" consists of domains, domain name servers, and IP addresses that Defendants use and control as command and control servers to continuously control the Shylock-infected computers. Command and control servers refer to either physical server computers or software running on computers that support the Shylock botnets. The number and location of the Shylock command and control servers may change over time.

The Shylock Command And Control Infrastructure

36. The Shylock command and control infrastructure is comprised of two groups of resources. First are the Shylock domains, consisting of domains and name servers Defendants use to communicate with and to expand the botnet. The "Hardcoded" Shylock domains host instructions to Shylock-infected computers, including the Shylock executables that install the

Shylock malware on user computers. The Hardcoded Shylock domains may also serve as fallback domains should a Shylock-infected computer lose contact with the Shylock command and control Infrastructure. The "Configuration File" domains host the Shylock configuration files that Shylock-infected computers will download. The Shylock configuration files are encrypted text files that Defendants use to control infected computers. The configuration files include—among other things—commands that allow Defendants to engage in their unlawful conduct. Defendants have designed Shylock to be adaptable through plug-ins, allowing Defendants to complement Shylock's main framework with additional functions, even after Shylock has been deployed. These plug-ins include the mechanism Defendants use to infect users' instant messenger applications and the RAT mechanism for accessing and attacking uninfected user computers. Defendants also maintain "Money Mule" domains that they use to recruit money mules to collect and transfer the stolen funds into Defendants' accounts. Defendants use the domain name servers to host the domains controlling the Shylock botnets. **Appendix A** to this Complaint lists the Shylock domains.

37. Second are the Shylock IP addresses that Defendants use to host the configuration files and instructions necessary to grow and to maintain the Shylock botnets. **Appendix B** to this Complaint lists the Shylock IP addresses.

Defendants Use The Shylock Botnets To Steal Money

38. The Shylock botnets' primary goal is to steal financial account credentials of owners of Shylock-infected computers to access owners' financial accounts and siphon funds to Defendants. Defendants, through the Shylock botnets, use multiple techniques to conduct those attacks.

39. A Shylock attack begins when Shylock detects the user's attempt to connect to a financial institution's website. When this occurs, Shylock can proceed in several ways. Shylock can, for example, log the keystrokes the user enters while logging into his or her account. Shylock can use the keystrokes to access the user's financial accounts, record the user's information displayed by the website, and even take a screenshot or video of the user's account pages. Shylock will upload this information later to the Shylock command and control

infrastructure. Defendants can use this information to attempt to steal additional information from the user's account or conduct other illegal acts with the stolen information.

40. In a more sophisticated variation on that basic attack, the Shylock botnets' malware running on the infected computers can engage in a "web-inject" attack to extract more sensitive information from the user. In a web-inject attack, Shylock alters the appearance of the financial institutions' webpage as it is being displayed in the user's web browser. Shylock essentially takes control of the user's browser. Instead of allowing the browser to provide an accurate rendering of the financial website, Shylock causes the browser to change what the user sees. It does this by "injecting" additional code into the website code that the browser is rendering in a displayable format for the user. For example, if the real website asks only for a login ID and password, Shylock can extend it through a web-inject and ask for additional information such as social security number, birth date, mother's maiden name, and other such information typically used to answer security questions. Again, Shylock will record this information and upload it later to Defendants, who can use it to steal from the user. Shylock is capable of exploiting various browsers in this manner including Microsoft Internet Explorer and Mozilla Firefox.

41. In still more sophisticated versions of this attack, Shylock can simply display a completely fake website for the financial institution the user is attempting to contact. To do this, it first hijacks the user's browser to keep it from connecting to the real website of the financial institution. It then contacts the Shylock command and control infrastructure and downloads a template for the website of the financial institution and displays that to the user. The user, believing he is connected to the real website of the financial institution, proceeds as normal. However, while the user types her real account access information, such as login ID and password into the fake website, Defendants can access her accounts on the real website. 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. 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 to be sent.

42. In some instances, Defendants will replace only portions of the financial institutions website. For example, Defendants have used web-injects to inject the Shylock Telephone Numbers into the financial institution's website. Plaintiffs are informed and believe and thereupon allege that Defendants change these numbers to prevent situations where a user becomes suspicious of or begins to notice fraudulent activity and attempts to contact the bank.

43. Defendants repeatedly misuse the trademarks of financial institutions on these fake online banking websites in order to confuse and mislead victims. Critically, the web-injects contain FS-ISAC member institutions' trademarks. Defendants design the web-injects to use those trademarks in such a manner to mimic the real website of a financial institution. This confuses owners of Shylock-infected computers and allows Defendants to carry out the web-inject attacks. This also makes it nearly impossible for users to detect the attacks.

44. More sophisticated still, Shylock provides a built-in Virtual Network Console (VNC) server with the ability to connect out to a remote server. This feature allows Defendants to directly access the infected computer over the Internet, bypassing network address translation and firewall restrictions on inbound connections. From this point, the botnet operator 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.

45. Additionally, Shylock can take a "video" of the user's browsing session. This feature could be used to steal sensitive information such as account balances, or to acquire authentication information. The ability to capture video allows a malicious actor to monitor portions of a victim's entire browsing session at a target of interest. This knowledge could be valuable to a malicious actor to better understand how an online banking application works. The video capture plug-in is typically downloaded from the Shylock command and control infrastructure.

46. Shylock is specifically designed to allow Defendants to conduct this malicious activity without revealing any evidence of the fraud to the user, Microsoft, the financial institutions or other victim websites until it is too late for the user or owners of these websites to regain control over funds or stolen information. For example, to avoid alerting the user to the

activity being conducted remotely via their own computer, Shylock has a command to turn off any sounds (*e.g.*, beeps or clicks) that the user's computer might otherwise make while being operated remotely. Many aspects of the information gathering and the attacks can be automated by the botnet operator so that the bot code running on each user computer can advance the theft autonomously.

Defendants Use Infected Computers To Attack Other Computers On The Internet

47. Defendants have developed plug-ins allowing Defendants to attack other computers on the Internet. The "MessengerSpread" plug-in, for example, allows Defendants to infect other computers on the Internet running instant messenger programs. Defendants' RAT plug-in, moreover, allows Defendants to attack other computers on an infected computer's LAN. Defendants serve these plug-ins to infected user computers using the "Plug-in" Shylock domains identified in Appendix A.

Injuries The Shylock Botnets Cause

48. The Shylock malware infection itself harms Microsoft and Microsoft's customers by damaging the customers' computers and the software installed on their computers licensed from Microsoft. During the infection of a user's computer, the Shylock malware makes changes at the deepest and most sensitive levels of the computer's operating system. Additionally, it makes fundamental changes at the level of the Windows Registry. Microsoft's customers whose computers are infected with the malicious software are damaged by these changes to Windows, which alter the normal and approved settings and functions of the user's operating system, destabilize it, and forcibly draft the customers' computers into the botnet.

49. Once a computer is infected, the Windows operating system and Internet Explorer browser applications on that computer cease to operate normally and are transformed into tools of deception and theft. But Windows and Internet Explorer still bear Microsoft's trademarks. Customers who experience degraded performance of Microsoft's products may attribute such poor performance to Microsoft, causing extreme damage to Microsoft's brands and trademarks and the goodwill associated therewith.   Even customers who eventually come to learn their computers are infected with malware may incorrectly attribute the infection to vulnerabilities in

Microsoft's products, because many customers are unaware that they have fallen prey to Defendants' attacks.

50. Moreover, as a provider of the Windows and Internet Explorer products, Microsoft devotes significant computing and human resources to combating infections by the Shylock Botnet, helping customers determine whether or not their computers are infected, and cleaning infected computers. These efforts by Microsoft cost substantial sums of money, and thus the Shylock Botnet and malware exact a tangible economic toll on Microsoft.

51. The Shylock Botnets and malware cause injury to numerous consumers, as well as the financial institutions whose interests are represented by FS-ISAC and FS-ISAC itself. Like Microsoft, FS-ISAC has devoted substantial resources to investigating and remediating the harm caused by the Shylock botnets. In addition, FS-ISAC 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. FS-ISAC institutions, moreover, suffer direct financial harm as a result of Defendants' unlawful conduct. Defendants and the Shylock botnets have cost FS-ISAC member institutions millions.

Defendants Work Together In A Common Operation To Create, Control, Maintain, And Operate The Shylock Botnets

52. The Shylock botnets comprise a family of inter-related botnets—commonly known as the Shylock malware. The Shylock malware first emerged in September 2011. The Shylock malware evolved over time, becoming more sophisticated and including additional features designed to counter attempts to analyze and disable the botnets.

53. Plaintiffs are informed and believe and thereupon allege that the common code and characteristics of the Shylock botnets, and evidence regarding specific activities of Defendants, demonstrate that Defendants—acting in concert with each other—control the Shylock botnets. Upon information and belief, the Shylock malware that Defendants install on users' computers all share common code and characteristics, and have evolved over time to more closely resemble one another. The Shylock botnets use similar configuration files, configuration files from the Zeus family of botnets. The Shylock configuration files, moreover, share similar

structures and use similar commands to command and to control Shylock-infected user computers. Defendants, moreover, rely on the same domains, name servers, IP addresses, and phone numbers that comprise the Shylock Command and Control Infrastructure.

54. Each of the Defendants have participated in the Shylock enterprise by: (1) generating Shylock executable files, configuration files, and plug-ins to control user computers; (2) deploying the Shylock botnets under one botnet name; (3) creating and maintaining the Shylock Command and Control Infrastructure consisting of server computers connected to the Internet through which to communicate with the infected user computers; (4) using one or more means to cause user computers to become infected with Shylock; (5) using the Shylock-infected computers around the world to steal security identification and financial account information; (6) using the Shylock bots to steal money directly from financial accounts of unsuspecting users around the world; (7) damaging Microsoft-owned and licensed software, including Windows and Internet Explorer, by corrupting these programs' behavior and converting them to instruments of criminality; (8) exploiting Microsoft's famous brands and trademarks to mislead Microsoft's customers, and consequently causing severe harm to Microsoft's brand, trademarks, reputation, and goodwill; (9) using Shylock-infected computers to send fake instant messages; and (10) using Shylock-infected computers to launch distributed denial of service attacks on financial and other institutions.

The Shylock Racketeering Enterprise

55. Plaintiffs are informed and believe and thereupon allege that Defendants cooperate to develop, to improve, and to support the Shylock botnets and the Shylock Command and Control Infrastructure. Upon information and belief, Defendants constitute a group of persons associated together for a common purpose of engaging in a course of conduct, as part of an ongoing organization, with the various associates functioning as a continuing unit. The Defendants' enterprise has a purpose, with relationships among those associated with the enterprise, and longevity sufficient to permit those associates to pursue the enterprise's purpose. Upon information and belief, Defendants John Does 1 through 8 conspired to, and did, form an associated in fact enterprise (herein after the "Shylock Racketeering Enterprise") with a common

purpose of developing and operating a global credential-stealing botnet operation as set forth in detail herein.

56. The Shylock Racketeering Enterprise has existed since at least September 2011 when Defendants created a single, consolidated global credential-stealing botnet in public. Other Defendants joined and began participating in the Shylock Racketeering Enterprise.

57. The Shylock Racketeering Enterprise has continuously and effectively carried out its purpose of developing and operating a global credential-stealing botnet operation since that time, and will continue to do so absent the judicial relief that Plaintiffs request.

58. Both the purpose of the Shylock Racketeering Enterprise and the relationship between Defendants is established by: (1) the emergence of the Shylock botnets; (2) the subsequent development and operation of the Shylock botnets; and (3) Defendants' respective and interrelated roles in the operation of, maintenance of, and profit from the Shylock botnets in furtherance of Defendants' common financial interests.

59. Upon information and belief, Defendants have conspired to, and have, conducted and participated in the operation of the Shylock Racketeering Enterprise through a continuous pattern of racketeering activity as set forth herein. Each predicate act is related to and in furtherance of the common unlawful purpose shared by the members of the Shylock Racketeering Enterprise. These acts are continuing and will continue unless and until this Court grants Plaintiffs' request for a temporary restraining order and other injunctive relief.

60. Upon information and belief, Defendants have conspired to, and have, knowingly and with intent to defraud trafficked in thousands of unauthorized access devices in the form of stolen passwords, bank account numbers and other account login credentials through the Shylock botnets created and operated by Defendants.

61. As set forth in detail herein, Defendants have used the Shylock botnets to steal, intercept and obtain this access device information from tens of thousands of individuals using falsified web pages, and have then used these fraudulently obtained unauthorized access devices to steal millions of dollars from individuals' accounts.

62. Upon information and belief, Defendants have also conspired to, and have, knowingly and with intent to defraud, possessed, and do possess, thousands of such unauthorized access devices fraudulently obtained as described herein.

63. Upon information and belief, Defendants have conspired to, and have, knowingly and with intent to defraud, effected transactions with the stolen unauthorized access devices to receive millions of dollars in payment from individuals' bank accounts.

64. Upon information and belief, Defendants have conspired to, and have, executed a scheme to defraud scores of financial institutions by enabling members of the Shylock Racketeering Enterprise to fraudulently represent themselves as specific bank customers, thereby enabling them to access and steal funds from those customer accounts.

65. Each of the foregoing illegal acts were conducted using interstate ACH and/or interstate and/or foreign wires as described herein, and therefore affected interstate and/or foreign commerce.

FIRST CLAIM FOR RELIEF

Violation of the Computer Fraud & Abuse Act, 18 U.S.C. § 1030

66. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 65 above.

67. Defendants knowingly and intentionally accessed protected computers without authorization and knowingly caused the transmission of a program, information, code and commands, resulting in damage to the protected computers, the software residing thereon, and Microsoft.

68. Defendants' conduct involved interstate and/or foreign communications.

69. Defendants' conduct has caused a loss to each Plaintiff during a one-year period aggregating at least $5,000.

70. Plaintiffs seek injunctive relief and compensatory and punitive damages under 18 U.S.C. §1030(g) in an amount to be proven at trial.

71. As a direct result of Defendants' actions, Plaintiffs have suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue

unless Defendants' actions are enjoined.

SECOND CLAIM FOR RELIEF

Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2701

72. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 65 above.

73. Microsoft's Windows operating system and Internet Explorer software, and Microsoft's customers' computers running such software, are facilities through which electronic communication service is provided to Microsoft's users and customers.

74. Defendants knowingly and intentionally accessed the Windows operating system and Internet Explorer software and computers upon which it runs without authorization or in excess of any authorization granted by Microsoft or any other party.

75. Through this unauthorized access, Defendants intercepted, had access to, obtained and altered, and/or prevented legitimate, authorized access to, wire electronic communications transmitted via Microsoft's Windows operating system and Internet Explorer software and the computers running such software.

76. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

77. As a direct result of Defendants' actions, Plaintiffs have suffered and continue to suffer irreparable harm for which no adequate remedy at law exists, and which will continue unless Defendants' actions are enjoined.

THIRD CLAIM FOR RELIEF

Trademark Infringement Under the Lanham Act – 15 U.S.C. § 1114 *et seq.*

78. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 65 above.

79. Defendants have used Microsoft's and FS-ISAC institutions' trademarks in interstate commerce.

80. The Shylock botnets generate and use unauthorized copies of Microsoft's trademarks in fake and unauthorized versions of the Windows operating system and Internet

Explorer software, including through the software operating from and through the Shylock Command and Control Infrastructure. The Shylock botnets also generate and use unauthorized copies of FS-ISAC institutions' trademarks. By doing so, Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake and unauthorized versions of the Windows operating system and Internet Explorer software.

81. As a result of their wrongful conduct, Defendants are liable to Plaintiffs for violation of the Lanham Act.

82. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

83. As a direct result of Defendants' actions, Plaintiffs have suffered and continue to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

84. Defendants' wrongful and unauthorized use of Microsoft's and FS-ISAC institutions' trademarks to promote, market, or sell products and services constitutes trademark infringement pursuant to 15 U.S.C. § 1114 et seq..

FOURTH CLAIM FOR RELIEF

False Designation of Origin Under The Lanham Act – 15 U.S.C. § 1125(a)

85. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 65 above.

86. Microsoft's and FS-ISAC member institutions' trademarks are distinctive marks that are associated with Microsoft and FS-ISAC member institutions and exclusively identify their businesses, products, and services.

87. Defendants make unauthorized use of Microsoft's and FS-ISAC member institutions' trademarks. By doing so, Defendants create false designations of origin as to tainted Microsoft products and FS-ISAC member institution services that are likely to cause confusion, mistake, or deception.

88. As a result of their wrongful conduct, Defendants are liable to Plaintiffs for violation of the Lanham Act, 15 U.S.C. § 1125(a).

89. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

90. As a direct result of Defendants' actions, Plaintiffs have suffered and continue to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

FIFTH CLAIM FOR RELIEF

Trademark Dilution Under The Lanham Act – 15 U.S.C. § 1125(c)

91. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 65 above.

92. Microsoft's and FS-ISAC member institutions' trademarks are famous marks that are associated with Microsoft and FS-ISAC member institutions and exclusively identify their businesses, products, and services.

93. Defendants make unauthorized use of Microsoft's and FS-ISAC member institutions' trademarks. By doing so, Defendants are likely to cause dilution by tarnishment of Plaintiffs' trademarks.

94. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

95. As a direct result of Defendants' actions, Plaintiffs have suffered and continue to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SIXTH CLAIM FOR RELIEF

Violations of the Racketeer Influenced and
Corrupt Organizations Act (RICO) – 18 U.S.C. § 1962(c)
(Microsoft)

96. Microsoft realleges and incorporates by reference the allegations contained in paragraphs 1 through 65 above.

97. Beginning, during, or before September of 2011 and continuing up through the filing of this Complaint, Defendants John Does 1 through 8 were and are associated in fact with the Shylock Racketeering Enterprise and have conducted its affairs through a pattern of

racketeering activity, with such conduct and activities affecting interstate and foreign commerce. At various dates after September 2011 and continuing through the filing of this Complaint, Defendants John Does 2 through 8 became associated in fact with the Shylock Racketeering Enterprise and have also conducted and participated in its affairs through a pattern of racketeering activity that affects interstate and foreign commerce. Defendants have engaged in an unlawful pattern of racketeering activity involving thousands of predicate acts of fraud and related activity in connection with access devices, 18 U.S.C. § 1029, wire fraud, 18 U.S.C. § 1343, and bank fraud, 18 U.S.C. § 1344.

98. The members of the Shylock Racketeering Enterprise share the common purpose of developing and operating a global credential-stealing botnet operation as set forth above.

99. Defendants have knowingly and with intent to defraud trafficked in thousands of unauthorized access devices in the form of stolen passwords, bank account numbers and other account login credentials through the Shylock botnets that Defendants created and operated. As set forth in detail above, Defendants have used the Shylock botnets to steal, intercept and obtain this access device information from thousands of individuals using falsified web pages, and have then used these fraudulently obtained unauthorized access devices to steal millions of dollars from these individuals' accounts, all in violation of 18 U.S.C. § 1029(a)(2).

100. Defendants have also knowingly and with intent to defraud, possessed, and do possess, thousands of unauthorized access devices fraudulently obtained as described above, in violation of 18 U.S.C. § 1029(a)(3).

101. Defendants have also knowingly and with intent to defraud effected transactions with stolen unauthorized access devices to receive millions of dollars in payment from individuals' bank accounts, in violation of 18 U.S.C. § 1029(a)(7).

102. Also as set forth in detail above, Defendants have executed a scheme to defraud scores of financial institutions by enabling members of the Shylock Racketeering Enterprise to fraudulently represent themselves as bank customers, thereby enabling them to access and steal funds from those customer accounts, all in violation of 18 U.S.C. § 1344.

103. Each of the violations of 18 U.S.C. §1029(a) and 18 U.S.C. § 1344 described

above were conducted using internet communications “transmitted by means of wire … in interstate or foreign commerce,” in violation of 18 U.S.C. § 1343.

104. Microsoft has been and continues to be directly injured by Defendants’ conduct. But-for the alleged pattern of racketeering activity, Microsoft would not have incurred damages.

105. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

SEVENTH CLAIM FOR RELIEF

Common Law Trespass to Chattels

106. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 65 above.

107. Defendants have used a computer and/or computer network, without authority, with the intent to cause physical injury to the property of another.

108. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to trespass on the computers and computer networks of FS-ISAC member institutions.

109. Defendants’ actions in operating the Shylock Botnet result in unauthorized access to Microsoft’s Windows operating system and Internet Explorer software and the computers on which such programs run, and result in unauthorized intrusion into those computers and theft of information, account credentials, and funds.

110. Defendants intentionally caused this conduct and this conduct was unlawful and unauthorized.

111. Defendants’ actions have caused injury to Microsoft, FS-ISAC, and FS-ISAC member institutions, and have interfered with the possessory interests of Microsoft over its software and with the FS-ISAC member institutions’ possessory interests in their respective computers and computer networks.

112. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

113. As a direct result of Defendants’ actions, Plaintiffs and FS-ISAC member

institutions have suffered and continue to suffer irreparable harm for which no adequate remedy at law exists, and which will continue unless Defendants' actions are enjoined.

EIGHTH CLAIM FOR RELIEF

Unjust Enrichment

114. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 65 above.

115. The acts of Defendants complained of herein constitute unjust enrichment of the Defendants at the expense of Microsoft and FS-ISAC member institutions in violation of the common law. Defendants used, without authorization or license, software belonging to Microsoft to facilitate unlawful conduct inuring to the benefit of Defendants.

116. Defendants profited unjustly from their unauthorized and unlicensed use of Microsoft's intellectual property.

117. Upon information and belief, Defendants had an appreciation and knowledge of the benefit they derived from their unauthorized and unlicensed use of Microsoft's intellectual property.

118. Retention by the Defendants of the profits they derived from their malfeasance would be inequitable.

119. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including without limitation disgorgement of Defendants' ill-gotten profits.

120. As a direct result of Defendants' actions, Plaintiffs and FS-ISAC member institutions suffered and continue to suffer irreparable harm for which no adequate remedy at law exists, and which will continue unless Defendants' actions are enjoined.

NINTH CLAIM FOR RELIEF

Conversion

121. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 65 above.

122. Microsoft owns all right, title, and interest in its Windows and Internet Explorer

software. Microsoft licenses its software to end-users. Defendants have interfered with, unlawfully and without authorization, and dispossessed Microsoft of control over its Windows and Internet Explorer software.

123. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to remove, halt, or otherwise disable computer data, computer programs, and computer software from a computer or computer network.

124. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to cause a computer to malfunction.

125. Defendants have converted funds from FS-ISAC member institutions through unauthorized withdrawals of funds from customer accounts using stolen online banking credentials.

126. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including without limitation the return of Defendants' ill-gotten profits.

127. As a direct result of Defendants' actions, Plaintiffs and FS-ISAC member institutions suffered and continue to suffer irreparable harm for which no adequate remedy at law exists, and which will continue unless Defendants' actions are enjoined.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs prays that the Court:

1. Enter judgment in favor of Plaintiffs and against the Defendants.

2. Declare that Defendants' conduct has been willful and that Defendants have acted with fraud, malice and oppression.

3. Enter a preliminary and permanent injunction enjoining Defendants and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein.

4. Enter a preliminary and permanent injunction giving Microsoft control over the domains, IP addresses, and phone numbers used by Defendants to cause injury and enjoining Defendants from using such instrumentalities.

5. Enter judgment awarding Plaintiffs actual damages from Defendants adequate to compensate Plaintiffs for Defendants' activity complained of herein and for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial.

6. Enter judgment disgorging Defendants' profits.

7. Enter judgment awarding enhanced, exemplary and special damages, in an amount to be proved at trial.

8. Enter judgment awarding attorneys' fees and costs, and

9. Order such other relief that the Court deems just and reasonable.

Dated: June 27, 2014 Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE
LLP

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*)
JACOB M. HEATH (*pro hac vice*)
ROBERT L. URIARTE (*pro hac vice*)
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

DEMAND FOR JURY TRIAL

Plaintiffs respectfully request a trial by jury on all issues so triable in accordance with Fed. R. Civ. P. 38.

Dated: June 27, 2014 Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

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 L. 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