IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. JOHN DOES 1-2, CONTROLLING A COMPUTER NETWORK AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS, Defendants.	Civil Action No: 1:19-cv-00716-ABJ

MICROSOFT'S STATUS REPORT

Plaintiff Microsoft Corporation ("Microsoft"), by counsel, hereby submits a status report pursuant to this Court's Order. *See* 8/11/2019 Minute Order (granting Microsoft's motion to extend time to conduct discovery necessary to identify and serve defendants and ordering Microsoft to file status report by August 30, 2019).

I. ***Microsoft Has Exhausted Discovery Efforts to Further Identify Defendants.***

To date, Defendants have been and are identified by the publicly-available domain registration information associated with the domain names that they have registered to carry out the activities forming the basis of Microsoft's complaint and motions for injunctive relief. *See e.g.* Dkt. Nos. 14 (Appendix A), 21 (Appendix A) (identifying defendants by the information listed in domain registration records). Microsoft has now exhausted efforts to use discovery upon third-party companies, such as Internet service providers ("ISPs"), domain registrars, hosting companies, and payment providers to try to more specifically identity defendants. Over the last several months, Microsoft has served subpoenas to U.S. service providers and carried out

follow up discovery, both through additional subpoenas and through informal engagement with parties located in countries that do not afford reciprocal civil discovery with the U.S. and with parties who have been determined to be victims of the defendants. Based on the information received in response to Microsoft's subpoenas and other discovery efforts, Microsoft has been met with the following circumstances:

Registration And Payment Information: Additional domain registration and payment information associated with Defendants' infrastructure and obtained from the relevant ISPs, domain registrars, and hosting companies is fraudulent, stolen, or otherwise unable to be specifically associated with Defendants.

- In particular, additional information regarding names, addresses and telephone numbers associated with Defendants' infrastructure, from these third-party companies' internal records, has almost uniformly been either entirely fake information or information stolen from individual victims being impersonated by defendants. For example, Defendants paid for domain registration using credit card information or forms of digital payment that were stolen from various individual victims. In these situations, the internal records reflect either individual victim information being used fraudulently, or reflect such information in combination with other fake information to create a false persona associated with a working credit card or other form of digital payment. Counsel has directly engaged with such victims to determine whether they may possess relevant information, but these individuals do not have any further information regarding defendants.

- In some cases, the information in the third-party companies' internal records reflects fake "reseller" operations (*i.e.,* fake companies or individuals purporting to operate as resellers of domains, hosting, and other infrastructure elsewhere in the world). This is apparently

to create an additional layer of separation between the defendants' infrastructure and information associated with defendants. In a number of instances, information associated with the fake "reseller" operations appears to have been put into effect just long enough to register domains, then it was abandoned. For example, email addresses associated with the fake resellers are no longer operative and the domains upon which the emails were operating are no longer registered. Further, all information put forward by Defendants associated with these fake reseller operations was artificial. For example, Defendants used addresses or phone numbers that simply do not exist or, in some cases, fraudulently listed the addresses of well-known U.S. technology companies. Similarly, Defendants often listed incoherent words as personal names associated with the purported "resellers." Further, many of these fake "resellers" purported to be in jurisdictions that do not afford reciprocal civil discovery with the U.S.—particularly Oman, the United Arab Emirates, Burundi, Uzbekistan, and Russia.

Login And Access IP Addresses: Defendants have accessed all resources investigated to date through means that either make their true source IP addresses anonymous or are otherwise not discoverable. Uniformly, nearly all of the login and access IP addresses used by Defendants to access their domain, hosting, or email accounts were either anonymous VPN services or IP addresses of hacked devices. In the first case, IP addresses of anonymous VPN services are used by many different individuals and such services do not maintain logs, such that IP addresses cannot be associated with any particular user's use at a given point in time. In the latter case, infrastructure was accessed from non-public IP addresses associated with devices such as hacked routers or similar devices that were compromised by Defendants and used to obfuscate the evidentiary trail that would otherwise exist. A given non-public IP address may, for example, be shared by many millions of devices that are not intended to connect to the public

internet, and thus cannot be used to identify a particular user at a particular time. These steps demonstrate the technical and operational sophistication of defendants. In a handful of instances, across the entirety of defendants' infrastructure, access was seen from IP addresses associated with several telecommunications companies in Iran. These IP addresses were not clearly associated with anonymization services. It is more likely that these IP addresses are actually associated with defendants. However, there is no means by which to pursue additional detail about these IP addresses, given the jurisdiction in which these companies operate.

Accordingly, even with the benefit of discovery, Defendants remain identified by the names by which they identified themselves in connection with the domain infrastructure at issue in this case. *See e.g.*, Dkt. Nos. 14, 21. Defendants have been and may be contacted at the email addresses used to register and maintain these domains, as well as several other email addresses maintained outside of the U.S., and identified during the course of discovery. In these ways, defendants may be sufficiently identified, served, and placed on notice of actions in this case, including any final judgment and injunction in this matter.

II. *Microsoft Intends to Request Entry of Default, Default Judgment, and Permanent Injunction Against Defendants.*

Microsoft intends to request entry of default, default judgment, and permanent injunction against Defendants. Other courts have repeatedly granted similar requests where, as here, "[d]espite extensive investigation, Plaintiffs have been unable to discover the Doe Defendants' true identities." *Microsoft Corp. v. John Does 1-8,* No. 1:14-CV-811, 2015 WL 4937441, at *1 (E.D. Va. Aug. 17, 2015) (O'Grady, J.) (adopting Report & Recommendation entering default judgment, issuing permanent injunction against John Does 1-8 and "their representatives and persons who are in active concert or participation with them," and prohibiting them from sending malware code and content to specified internet domains); *Microsoft Corp. v. John Does 1-82,*

No. 3:13-CV-00319-GCM, 2013 WL 6119242, at *4 (W.D.N.C. Nov. 21, 2013) (Mullen, J.) (same; restricting access and sending malicious software to Microsoft's licensed operating system and software and protected computers of Microsoft customers); *Consumer Source Holding, Inc. v. Does 1-24,* No. 1:13-CV-1512 AJT/JFA, 2014 WL 2967942, at *1 (E.D. Va. July 1, 2014) (same; restraining use of trademarks in connection with Internet websites).

In so doing, courts have reasoned that Defendants "can likely be contacted directly or through third-parties." *Microsoft Corp. v. Does 1-2*, No. 1:16CV993, 2017 WL 5163363, at *3 (E.D. Va. Aug. 1, 2017), *report and recommendation adopted,* No. 116CV00993GBLTCB, 2017 WL 3605317 (E.D. Va. Aug. 22, 2017) (Lee, J.) (granting default judgment and permanent injunction and transferring control to Microsoft over domains and appointing Court Monitor to oversee defendants' compliance with permanent injunction); *see also* Order, *Microsoft v. John Does, 1-11*, No. 11CV00222 (W.D. Wash. Sept. 13, 2011), Dkt. No. 68 (Robart, J.) (granting default judgment and permanent injunction against Doe Defendants and directing Microsoft to serve a copy of order "upon Defendants, the data centers and hosting providers and domain registries"); *Microsoft Corp. v. Does*, No. 12-CV-1335 SJ RLM, 2012 WL 5497946, at *3 (E.D.N.Y. Nov. 13, 2012) (Johnson, J.) (granting motion for default judgment against Doe Defendants 1-21, 25-35, and 37-39 after finding Microsoft's "email and internet-based service of process upon Defendants was designed to provide Defendants with notice of the action existing against them, Defendants' anonymity and unknown whereabouts notwithstanding"); *see also Core Distribution, Inc. v. Doe 1,* No. 16-CV-04059 (SRN/HB), 2018 WL 6178720, at *10 (D. Minn. Nov. 27, 2018) (restraining Doe Defendants identified by usernames and seller IDs from patent infringement, false advertising, and deceptive trade practices). Accordingly, this Court will have sufficient grounds to permit entry of a default judgment and permanent injunction

against Defendants in this case.

III. *Microsoft Expects Defendants to Continue Illegal Conduct and Requests An Expedited Process for Addressing Ongoing Threats*.

Microsoft is aware that Defendants continue to put in place new infrastructure and has brought to this Court's attention through numerous motions for supplemental preliminary injunctions including its most recent request, which is currently pending, that identifies additional domains. *See* Dkt. Nos. 19, 24. Microsoft expects Defendants to continue to put in place new infrastructure in the future, which, like the previously addressed infrastructure, will have to be disabled to prevent harmful actions carried out by Defendants.

Therefore, Microsoft respectfully proposes that this Court consider an efficient, expedited process to enforce the permanent injunction in the future and would welcome this Court's input on whether to do so through the current process of appealing to this Court for supplemental preliminary injunctions, through a Court-appointed adjunct, or some other expedited process. Given the speed and persistence with which Defendants are able to put in place new harmful infrastructure, Microsoft has proposed that this Court appoint a monitor or Special Master to oversee the enforcement of any permanent injunction that might issue in order to ensure continuing remediation of injury flowing from Defendants' numerous violations of the Court's injunctions to date. *See* Dkt. No. 24. This approach is based off one adopted by another federal court in a nearly identical case where the Court appointed a monitor – former federal Judge Faith S. Hochberg from U.S. District Court for the District of New Jersey – to oversee enforcement of a permanent injunction through a less formal and expedited process, and to submit reports to the Court identifying additional illegal activities by Defendants, noting additional domains that needed to be removed from Defendants' control, and itemizing fees and expenses relating to work to enforce the injunction. *See, e.g., Microsoft Corp. v. Does 1-2,* No. 16-CV-00993

(GBL/TCB), 2017 WL 3605317, at *1 (E.D. Va.), Dkt. Nos. 52, 65, 68-69, 72-73 (notice of filing of court monitor reports). Microsoft believes that this is one possible solution that would afford an expedited process necessary to meet the pace of Defendants' actions and would ease any burden on this Court from serial, conventional proceedings, while ensuring this Court's continued involvement through regular reports on efforts to take down additional domains and curtail continued harmful actions carried out by Defendants in violation of court orders.

Microsoft invites a status conference to discuss the course of the action, if the Court would find such a conference to be of assistance in determining the appropriate path forward.

Dated: August 23, 2019

Respectfully submitted,

/s/ *Gabriel M. Ramsey*

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

Julia R. Milewski (D.C. Bar No. 1008678)
Justin D. Kingsolver (D.C. Bar. No. 1033806)
Matthew B. Welling (*pro hac vice*)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
jmilewski@crowell.com
jkingsolver@crowell.com
mwelling@crowell.com

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

Attorneys for Plaintiff Microsoft Corp.