Exhibit 1

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 1-2, CONTROLLING COMPUTER BOTNETS AND THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS, Defendants.	Civil Action No: 1:20-cv-1171 (AJT/IDD)

[PROPOSED] PRELIMINARY INJUNCTION ORDER

Plaintiffs Microsoft Corp. ("Microsoft") and Financial Services – Information Sharing And Analysis Center, Inc. ("FS-ISAC") (collectively "Plaintiffs") have filed a complaint for injunctive and other relief pursuant to: (1) the Copyright Act (17 U.S.C. § 101, *et seq*.); (2) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (3) the Electronic Communications Privacy Act (18 U.S.C. § 2701); (4) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (5) the common law of trespass, unjust enrichment and conversion. Plaintiffs have moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act). Plaintiffs have moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules

of Civil Procedure, 17 U.S.C. § 502(a) (the Copyright Act), (15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651 (the All-Writs Act). On October 6, 2020, the Court issued a temporary restraining order and order to show cause why an injunction should not issue. On October 14, 2020, the Court issued a supplemental temporary restraining. Defendants have not responded to the Court's order to show cause.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum, and all other pleadings and papers relevant to Plaintiff's request for a Preliminary Injunction, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants John Does 1-2 ("Defendants") under the Copyright Act (17 U.S.C. §§ 106 and 501 *et seq*.), the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and the common law of trespass to chattels, unjust enrichment and conversion.

2. Defendants have not responded to the Court's October 6, 2020 Order to Show Cause.

3. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Copyright Act (17 U.S.C. §§ 106 and 501 *et seq*.), the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and constitute trespass to chattels, unjust enrichment and conversion, and that Plaintiffs are, therefore, likely to prevail on the

merits of this action;

4. Microsoft owns the registered copyrights in the Windows 8 Software Development Kit ("SDK"), Reg. No. TX 8-888-365 ("Copyrighted Work"). Microsoft's Copyrighted Work is an original, creative work and copyrightable subject matter under the laws of the United States. *See* 17 U.S.C. § 102(a); *see also Oracle America, Inc. v. Google Inc.*, 750 F.3d 1339 (Fed. Cir. 2014) (holding the structure, sequence, and organization of declaring computer code qualifies as an original work under the Copyright Act).

5. Microsoft owns the registered trademarks "Microsoft" and "Windows" used in connection with its services, software and products. FS-ISAC's member organizations have invested in developing their brands, trademarks, and trade names in association with the financial services they offer.

6. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations. The evidence set forth in Plaintiffs' Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"), and the accompanying declarations and exhibits, demonstrates that Plaintiffs are likely to prevail on their claim that Defendants have engaged in violations of the foregoing law by:

a. directly, contributorily and through inducement, infringing Microsoft's Copyrighted Work by reproducing, distributing, and creating derivative works in their malicious software, which includes code that is literally copied from, substantially similar to and derived from the Copyrighted Work, in violation of Microsoft's exclusive rights at least under 17 U.S.C. § 101 *et seq*. without any authorization or other permission from Microsoft;

b. transmitting malicious code containing the Copyrighted Work through Internet Protocol addresses ("IP Addresses") to configure, deploy and operate a botnet;

c. intentionally accessing and sending malicious software, code, and instructions to the protected computers and operating systems of the customers or associated member organizations of Microsoft and FS-ISAC, without

authorization and exceeding authorization, in order to

i. install on those computers and computer networks malicious code and thereby gain control over those computers and computer networks in order to make them part of the computer botnet known as the "Trickbot" botnet (the "botnet");

ii. attack and compromise the security of those computers and computer networks by conducting remote reconnaissance, stealing and harvesting authentication credentials, monitoring the activities of users, and using other instrumentalities of theft;

iii. steal and exfiltrate information from those computers and computer networks;

d. corrupting Microsoft's operating system and applications on victims' computers and networks, thereby using them to carry out the foregoing activities

e. creating false websites that falsely indicate that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations;

f. stealing personal and financial account information from computer users; and

g. using stolen information to steal money from the financial accounts of those users.

7. There is good cause to believe that if such conduct continues, irreparable harm will occur to Plaintiffs, Plaintiffs' customers and member organizations, and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

8. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of botnet command and control software that is hosted at and otherwise operates through the Internet Protocol (IP) addresses listed in **Appendix A** and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available at those locations if Defendants receive advance notice of this action. Based on the evidence cited in Plaintiffs' TRO Application and accompanying declarations and exhibits, Plaintiffs are likely to be able to prove that:

a. Defendants are engaged in activities that directly violate United States law and harm Plaintiffs and the public, including Plaintiffs' customers and member-organizations;
b. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;
c. Defendants are likely to delete or to relocate the botnet command and control software at issue in Plaintiffs' TRO Application and the harmful and malicious software, infringing Microsoft's Copyrighted Work and trademarks, disseminated through the IP Addresses listed in **Appendix A** to this Order, thereby permitting them to continue their illegal acts; and
d. Defendants are likely to warn their associates engaged in such activities if informed of Plaintiffs' action.

9. Plaintiffs' request for this preliminary injunction is not the result of any lack of diligence on Plaintiffs' part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 17 U.S.C. § 502(a), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and accordingly, Plaintiffs are relieved of the duty to provide Defendants with prior notice of Plaintiffs' motion.

10. There is good cause to believe that Defendants have specifically directed their activities to computers of Plaintiffs' customers and member organizations located in the Eastern District of Virginia, have engaged in illegal activity using the IP Addresses identified in **Appendix A** to this Order that are registered to command and control servers located at data centers and/or Internet hosting companies ("Hosting Providers") set forth in **Appendix A**, to direct malicious botnet code and content through the Internet to said computers of Plaintiffs' customers and member organizations to further perpetrate their fraud on Plaintiffs' customers and member organizations.

11. There is good cause to believe that Defendants have engaged in illegal activity using the Hosting Providers identified in **Appendix A** to host command and control software and the malicious botnet code and content used to maintain and operate the botnet at computers, servers, electronic data storage devices, or media at the IP Addresses listed in **Appendix A**.

12. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants' IP Addresses identified in **Appendix A** must be immediately disabled; Defendants' computer resources related to such IP Addresses must be disconnected from the Internet; Defendants must be prohibited from accessing Defendants' computer resources related to such IP Addresses; and to prevent the destruction of data and evidence located on those computing resources.

13. There is good cause to believe that in order to halt the injury caused by Defendants and to ensure the future prosecution of this case it not rendered fruitless by attempts to delete, hide, conceal, or otherwise render inaccessible the software components that create, distribute, and are involved in the creation, perpetuation, and maintenance of the botnet and prevent the unauthorized copying, reproduction, distribution, public display, and creation of derivative works in Microsoft's Copyrighted Work and prevent the creation and distribution of unauthorized copies of the registered trademarks of Microsoft and FS-ISAC's member organizations and carry out other harmful conduct, with respect to the Defendants' most current, active command and control servers hosted at the IP Addresses, the following actions should be taken. The Hosting Providers set forth in **Appendix A**, should take reasonable steps to block incoming and/or outgoing traffic on their respective networks that originates or has been sent from and/or to the IP Addresses identified in **Appendix A**, such that said traffic will not reach victim end-user computers on the Hosting Providers' respective networks and/or the computers at the IP Addresses in **Appendix A**, and should take other reasonable steps to block such traffic to and/or from any other IP addresses to which Defendants may move the botnet infrastructure, identified by Plaintiffs, to ensure that Defendants cannot use such infrastructure to control the botnet.

14. There is good cause to believe that Defendants may change infrastructure or third party infrastructure providers in order to conduct further illegal activities, and that it may be necessary for Plaintiffs to identify and update infrastructure and/or third party infrastructure providers as may be reasonably necessary to account for additional infrastructure used by Defendants for the purposes set forth herein.

15. There is good cause to permit notice of the instant Order and service of all other pleadings by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' Hosting Providers and as agreed to by Defendants in Defendants' Hosting Providers' agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

PRELIMINARY INJUNCTION

IT IS THEREFORE ORDERED that, Defendants, their representatives and persons who are in active concert or participation with them are restrained and enjoined from: (1) intentionally accessing and sending malicious software or code to Plaintiffs and the protected computers and operating systems of Plaintiffs' customers and associated member organizations, without authorization, in order to infect those computers and make them part of any botnet, (2)

sending malicious code to configure, deploy and operate a botnet, (3) attacking and compromising the security of the computers and networks of Plaintiffs, their customers, and any associated member organizations, (4) stealing and exfiltrating information from computers and computer networks, (5) creating false websites that falsely indicated that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations; (6) configuring, deploying, operating, or otherwise participating in or facilitating the botnet described in the TRO Application, including but not limited to the command and control software hosted at and any infrastructure, including IP addresses, domain names, servers or other computers, and through any other component or element of the botnet in any location; (7) delivering malicious software designed to steal financial account credentials, (8) monitoring the activities of Plaintiffs, Plaintiffs' customers or member associations and stealing information from them, (9) attacking computers and networks, monitoring activities of users, and theft of information, (10) corrupting Microsoft's operating system and applications on victims' computers and networks, thereby using them to carry out the foregoing activities, (11) misappropriating that which rightfully belongs to Plaintiffs, Plaintiffs' customers or member associations or in which Plaintiffs have a proprietary interests, and (12) undertaking any similar activity that inflicts harm on Plaintiffs, Plaintiffs' customers or member associations, or the public.

IT IS FURTHER ORDERED that, Defendants, their representatives and persons who are in active concert or participation with them are restrained and enjoined from: (1) reproducing, distributing, creating derivative works, and/or otherwise infringing Microsoft's Copyrighted Work, bearing registration number TX 8-888-365; (2) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks "Microsoft," "Windows," "Outlook" and "Word" logo bearing registration numbers 2872708, 5449084,

2463526, 4255129 and 77886830; and/or the trademarks of financial institution members of FS-ISAC; (2) using in connection with Defendants' activities, products or services any false or deceptive designation, representation or description of Defendants or of their activities, whether by symbols, words, designs or statements, which would damage or injure Plaintiffs or their member organizations or give Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products or services as Plaintiffs' or their member organizations.

IT IS FURTHER ORDERED that, with respect to any of the IP Addresses set forth in **Appendix A** to this Order, the Hosting Providers identified in **Appendix A**to this Order, shall take reasonable best efforts to implement the following actions:

A. Take reasonable steps to identify incoming and/or outgoing Internet traffic on their respective networks that originates and/or is being sent from and/or to the IP Addresses identified in **Appendix A**;

B. Take reasonable steps to block incoming and/or outgoing Internet traffic on their respective networks that originate and/or are being sent from and/or to the IP Addresses identified in **Appendix A**, by Defendants or Defendants' representatives or resellers, except as explicitly provided for in this Order;

C. Completely disable the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the IP Addresses set forth in **Appendix A,** or any additional IP Address Defendants may use after execution of this Order and not specifically identified in **Appendix A,** and make them inaccessible from any other computer

on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives and all other persons, except as otherwise ordered herein;

D. Completely, and until further order of this Court, suspend all services to Defendants or Defendants' representatives or resellers associated with the IP Addresses set forth in **Appendix A**;

E. Transfer any content and software hosted at the IP Addresses listed in **Appendix A** that are not associated with Defendants, if any, to new IP Addresses not listed in **Appendix A**; notify any non-party owners of such action and the new IP addresses, and direct them to contact Plaintiffs' counsel, Gabriel M. Ramsey, Crowell & Moring LLP, 3 Embarcadero Ctr., 26th Floor, San Francisco, CA 94111, gramsey@crowell.com, (Tel: 415-365-7207), to facilitate any follow-on action;

F. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with Hosting Providers, data centers, the Plaintiffs or other ISPs to execute this order;

G. Not enable, and shall take all reasonable steps to prevent, any circumvention of this order by Defendants or Defendants' representatives associated with the IP Addresses, including without limited to enabling, facilitating, and/or allowing Defendants or Defendants' representatives or resellers to rent, lease, purchase, or otherwise obtain another IP Address associated with your services;

H. Preserve, retain and produce to Plaintiffs all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the IP Addresses set forth in **Appendix A**, including any and all individual or entity names, mailing

addresses, e-mail addresses, facsimile numbers and telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage, access and contact records and all records, documents and logs, including without limitation data flow analyses, server logs, traffic logs, and any other similar information, associated with Defendants' or Defendants' Representatives' use of or access to the IP Addresses;

I. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order; and

J. Completely preserve the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the IP Addresses set forth in **Appendix A**, and preserve all evidence of any kind related to the content, data, software or accounts associated with such IP addresses and such computer hardware, such that such evidence of Defendants' unlawful activities is preserved.

IT IS FURTHER ORDERED that, with respect to any new or additional infrastructure put in place by Defendants for the purposes prohibited by this Order, including IP addresses, domain names, servers or other computers that Defendants may use and which are adjudged to be subject to this Order by the Court Monitor or this Court, such infrastructure shall be disabled pursuant to the terms of further Orders of the Court Monitor or the Court, as may be issued under the process set forth below.

IT IS FURTHER ORDERED that, pursuant to Federal Rule of Civil Procedure 53(a)(1)(C) and the court's inherent equitable powers, **Hon. S. James Otero (Ret.)** is appointed to serve as Court Monitor in order to make determinations and orders regarding whether particular infrastructure, including IP addresses and/or domain names, constitute command and control infrastructure for the Trickbot botnet, and to monitor Defendants' compliance with the

Preliminary Injunction. The Court Monitor has filed an affidavit "disclosing whether there is any ground for disqualification under 28 U.S.C. § 455." Fed. R. Civ. P. 53(b)(3); *see also* Fed. R. Civ. P. 53(a)(2) (discussing grounds for disqualification), and the record shows no grounds for disqualification. The following sets forth the terms of the appointment of the Court Monitor:

1. **Duties:** The duties of the Court Monitor shall include the following:

A. Carrying out all responsibilities and tasks specifically assigned to the Court Monitor in this Order;

B. Resolving objections submitted by third party infrastructure providers, Defendants or other third parties, to Plaintiffs' determinations that infrastructure constitutes Trickbot command and control infrastructure and, with respect to motions submitted by Plaintiffs that particular infrastructure constitutes Trickbot command and control infrastructure, making determinations whether such infrastructure constitutes Trickbot infrastructure;

C. Otherwise facilitating the Parties' or third parties' resolution of disputes concerning compliance with obligations under this Order or any orders issued by the Court Monitor, and recommending appropriate action by the court in the event an issue cannot be resolved by the Parties or third parties with the Court Monitor's assistance;

D. Investigating matters related to the Court Monitor's duties, and enforcing orders related to the matters set forth in this Order.

E. Monitoring and reporting on Defendants' compliance with their obligations under the Permanent Injunction;

F. The Court Monitor shall have all authority provided under Federal Rule of Civil Procedure 53(c).

2. **Orders Regarding Trickbot Infrastructure:** The Court Monitor shall resolve

objections and shall make determinations and issue orders whether infrastructure is Trickbot infrastructure, pursuant to the terms set forth in this Preliminary Injunction and pursuant to the following process:

A. Upon receipt of a written objection from any third party infrastructure provider, Defendants or any other third parties contesting any determinations by Plaintiffs that particular infrastructure constitutes Trickbot command and control infrastructure, or upon receipt of a written motion from Plaintiffs for a finding that particular infrastructure constitutes Trickbot infrastructure, the Court Monitor shall take and hear evidence whether infrastructure is Trickbot infrastructure, pursuant to the standards set forth in Rule 65 of the Federal Rules of Civil Procedure. Any party opposing such objection or motion shall submit to the Court Monitor and serve on all parties an opposition or other response within twenty four (24) hours of receipt of service of the objection or motion. The Court Monitor shall issue a written ruling on the objection or motion no later than two (2) days after receipt of the opposition or other response. Any party may seek and the Court Monitor may order provisional relief, including disablement of IP addresses, transfer of control or redirection of domain names or other temporary disposition of technical infrastructure, while any objection or motion is pending.

B. It is the express purpose of this order to afford prompt and efficient relief and disposition of Trickbot infrastructure. Accordingly, in furtherance of this purpose, all objections, motions and responses shall be embodied and communicated between the Court Monitor, parties and third parties in electronic form, by electronic mail or such other means as may be reasonably specified by the Court Monitor. Also in furtherance of this purpose, hearings shall be telephonic or in another expedited form as may be reasonably specified by the Court Monitor.

C. The Court Monitor's determinations regarding any objection or any motion shall be embodied in a written order, which shall be served on all Parties and relevant third parties (including hosting companies, hosting reseller, data centers, ISPs, domain registries and/or domain registrars, or other similar entities).

D. The Court Monitor is authorized to order the Parties and third parties to comply with such orders (pursuant to 28 U.S.C. § 1651(a)), subject to the Parties' and third parties' right to judicial review, as set forth herein.

E. If no Party or third party objects to the Court Monitor's orders and determinations pursuant to the judicial review provisions herein, then the Court Monitor's orders and determinations need not be filed on the docket. However, at the time the Court Monitor submits periodic reports to the court, as set forth below, the Monitor shall separately list in summary form uncontested orders and determinations.

3. **Judicial Review:** Judicial review of the Court Monitor's orders, reports or recommendations, shall be carried out as follows:

A. If any Party or third party desires to object to any order or decision made by the Court Monitor, the Party shall notify the Court Monitor within one business day of receipt of service of the order or decision, and thereupon the Court Monitor shall promptly file on the court's docket the written order setting forth the Monitor's decision or conditions pursuant to Federal Rule of Civil Procedure 53(d). The Party or third party shall then object to the Court Monitor's order in the manner prescribed in this Order.

B. The Parties and third parties may file objections to, or a motion to adopt or modify, the Court Monitor's order, report, or recommendations no later than 10 calendar days after the order is filed on the docket. The court will review these objections under the standards

set forth in Federal Rule of Civil Procedure 53(f).

C. Any party may seek and the Court may order provisional relief, including disablement of IP addresses, transfer of control or redirection of domain names or other temporary disposition of technical infrastructure, while any objection or motion is pending.

D. The orders, reports and recommendations of the Court Monitor may be introduced as evidence in accordance with the Federal Rules of Evidence.

E. Before a Party or third party seeks relief from the court for alleged noncompliance with any court order that is based upon the Court Monitor's report or recommendations, the Party or third party shall: (i) promptly notify the other Parties or third party and the Court Monitor in writing; (ii) permit the Party or third party who is alleged to be in noncompliance five business days to provide the Court Monitor and the other parties with a written response to the notice, which either shows that the party is in compliance, or proposes a plan to cure the noncompliance; and (iii) provide the Court Monitor and parties an opportunity to resolve the issue through discussion. The Court Monitor shall attempt to resolve any such issue of noncompliance as expeditiously as possible.

4. **Recordkeeping:** The Court Monitor shall maintain records of, but need not file those orders, reports and recommendations which are uncontested by the Parties or third parties and for which judicial review is not sought. The Court Monitor shall file on the court's docket all written orders, reports and recommendations for which judicial review is sought, along with any evidence that the Court Monitor believes will assist the court in reviewing the order, report, or recommendation. The Court Monitor shall preserve any documents the Monitor receives from the Parties.

5. **Periodic Reporting:** During the pendency of this case, the Court Monitor shall

provide periodic reports to the court and to the Parties concerning the status of Defendants' compliance with the Preliminary Injunction and other orders of the court or the Court Monitor, including progress, any barriers to compliance, and potential areas of noncompliance. The periodic reports shall also include a summary of all uncontested orders and determinations and a listing of *ex parte* communications. During the pendency of the case, the Court Monitor shall file a report with the court under this provision at least once every 30 days.

6. **Access to Information:** The Court Monitor shall have access to individuals and non-privileged information, documents and materials under the control of the Parties or third parties that the Monitor requires to perform his or her duties under this Order, subject to the terms of judicial review set forth herein. The Court Monitor may communicate with a Party's or a third party's counsel or staff on an *ex parte* basis if reasonably necessary to carry out the Court Monitor's duties under this Order. The Court Monitor may communicate with the court on an *ex parte* basis concerning non-substantive matters such as scheduling or the status of the Court Monitor's work. The Court Monitor may communicate with the court on an *ex parte* basis concerning substantive matters with 24 hours written notice to the Parties and any relevant third party. The Court Monitor shall document all *ex parte* oral communications with a Party's or third party's counsel or staff in a written memorandum to file summarizing the substance of the communications, the participants to the communication, the date and time of the communication and the purpose of the *ex parte* communication. At the time the Court Monitor submits his or her periodic reports to the court, the Monitor shall separately list his or her *ex parte* communications with the Parties.

7. **Engagement of Staff and Consultants:** The Court Monitor may hire staff or expert consultants to assist the Court Monitor in performing his or her duties. The Court

Monitor will provide the Parties advance written notice of his or her intention to hire a particular consultant, and such notice will include a resume and a description of duties of the consultant.

8. **Budget, Compensation, and Expenses:** Plaintiffs shall fund the Court Monitor's work. The Court Monitor shall incur only such fees and expenses as may be reasonably necessary to fulfill the Court Monitor's duties under this Order, or such other orders as the court may issue. Every 60 days the Court Monitor shall submit to Plaintiffs an itemized statement of fees and expenses. Plaintiffs shall pay such fees and expenses within 30 calendar days of receipt. The Court Monitor shall file such statements of fees and expenses with the reports set forth in Paragraph 5 above. If Plaintiffs dispute a statement, the Court Monitor shall submit the statement the court. The court will inspect any such disputed statement for regularity and reasonableness, make determinations regarding what portion of the statement is regular and reasonable, sign and transmit such finalized statement to Plaintiffs. Plaintiffs shall then remit to the Court Monitor any court-approved amount of any disputed statement, within 30 calendar days of court approval.

9. **Other Provisions:** As an agent and officer of the court, the Court Monitor and those working at the Court Monitor's direction shall enjoy the same protections from being compelled to give testimony and from liability for damages as those enjoyed by other federal judicial adjuncts performing similar functions. Nevertheless, any Party or non-party may request that the court direct the Court Monitor to disclose documents or other information reasonably necessary to an investigation or the litigation of legal claims in another judicial forum that are reasonably related to the Court Monitor's work under this Order. The Court shall not order the Court Monitor to disclose any information without providing the Parties notice and an opportunity to be heard. As required by Rule 53(b)(2) of the Federal Rules of Civil Procedure,

the court directs the Court Monitor to proceed with all reasonable diligence. The Court Monitor shall be discharged or replaced only upon an order of the Court. The parties, their successors in office, agents, and employees will observe faithfully the requirements of this Order and cooperate fully with the Court Monitor, and any staff or expert consultant employed by the Court Monitor, in the performance of their duties.

10. **Retention of Jurisdiction:** The Court will retain jurisdiction to enforce and modify the Preliminary Injunction during the pendency of this case.

IT IS FURTHER ORDERED that copies of this Order and all other pleadings and documents in this action may be served by any means authorized by law, including any one or combination of (1) personal delivery upon Defendants who provided accurate contact information in the U.S., if any; (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their Hosting Providers and as agreed to by Defendants in their Hosting Providers agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

IT IS SO ORDERED

Entered this ____ day of October, 2020. _____

United States District Judge

APPENDIX A

APPENDIX A

LIST OF IP ADDRESSES AND HOSTING COMPANIES ASSOCIATED WITH TRICKBOT'S COMMAND AND CONTROL SERVERS

IP Addresses of Command and Control Servers	Hosting Companies/Data Centers Where Defendants Have Placed the Command and Control Servers,
104.161.32.103 104.161.32.105 104.161.32.106 104.161.32.109 104.161.32.118	Input Output Flood, LLC d/b/a Ioflood 9030 W. Sahara Ave., Suite 703 Las Vegas, NV 89117 Input Output Flood, LLC d/b/a Ioflood c/o Phoenix NAP, LLC d/b/a phoenixNAP 3402 E University Dr. #6 Phoenix, AZ 85034
104.193.252.221	Hosting Solution Ltd. c/o Hurricane Electric LLC 48233 Warm Springs Blvd Fremont, CA 94539 Hurricane Electric LLC 760 Mission Ct. Fremont, CA 94539
107.155.137.19 107.155.137.28 107.155.137.7 162.216.0.163 23.239.84.132 23.239.84.136	Nodes Direct Holdings, LLC 1650 Margaret St Suite 302-351 Jacksonville, FL 32204 Nodes Direct Holdings, LLC 4495 Roosevelt Blvd, Suite 304-241 Jacksonville, FL 32210 Nodes Direct Holdings LLC c/o Cologix, Inc. 421 W. Church St., Suite 429 Jacksonville, FL 32202
107.174.192.162 107.175.184.201	Virtual Machine Solutions LLC 1600 Sawtelle Blvd., Suite 308 Los Angeles, CA 90025

	Virtual Machine Solutions LLC 2801 Robin Rd. Midwest City, OK 73110 Virtual Machine Solutions LLC c/o Velocity Servers, Inc. d/b/a ColoCrossing 325 Delaware Ave., Suite 300 Buffalo, NY 14202 Velocity Severs, Inc. d/b/a ColoCrossing 8185 Sheridan Dr Buffalo, NY 14221-6002
139.60.163.45	Hostkey USA, Inc. c/o Smyle & Associates 122 East 42nd St., Suite 3900 New York NY 10168 Hostkey USA, Inc. c/o Webair Internet Development Company Inc. 501 Franklin Avenue, Suite 200 Garden City, NY 11530 Hostkey USA, Inc. c/o Webair Internet Development Company Inc. 1025 Old Country Road Westbury, NY 11590 Hostkey USA, Inc. c/o Hurricane Electric LLC 501 Franklin Avenue, Suite 200 Garden City, NY 11530 Hurricane Electric LLC 760 Mission Ct. Fremont, CA 94539
156.96.46.27	Fastlink Network, Inc. 624. S. Grand Ave. Los Angeles, CA 90017 Fastlink Network, Inc. Fastlink Network – Newtrend Division P.O. Box 17295

	Encino, CA 91416 Fastlink Network, Inc. c/o Incorp Services, Inc. 5716 Corsa Ave, Suite 110 Westlake Village, CA 91362 Fastlink Network, Inc. 624. S. Grand Ave. Los Angeles, CA 90017 Fastlink Network, Inc. and VolumeDrive, Inc. 1143 Northern Blvd. Clarks Summit PA 18411 Fastlink Network, Inc. and VolumeDrive, Inc. 9 East Market St Wilkes Barre, PA 18701
195.123.241.13 195.123.241.55	Green Floid LLC c/o Business Filings Inc. 1200 South Pine Island Road Plantation, FL 33324 Green Floid LLC 119 Grimsby St. – Staten Island New York, NY 10306 Green Floid LLC 2707 East Jefferson Street Orlando, FL, 32803 Green Floid LLC ITL-Bulgaria Ltd. c/o Equinix, Inc. 1920 E. Maple Ave. El Segundo, CA 90245 Equinix, Inc. One Lagoon Dr. Redwood City, CA 94065

	Equinix, Inc. c/o United Agent Group, Inc. 4640 Admiralty Way, 5th Floor Marina del Rey, CA 90292
162.247.155.165	Twinservers Hosting Solutions Inc. 23 Meadowview Circle Nashua, NH 03062 Twinservers Hosting Solutions, Inc. c/o DataSite Atlanta BPC, LLC c/o Burges Property & Co. 1130 Powers Ferry Pl. Marietta, GA 30067 DataSite Atlanta BPC, LLC Burges Property & Co. 2658 Del Mar Heights Rd. #558 Del Mar, CA, 92014 Twinservers Hosting Solutions, Inc. c/o Performive LLC 1130 Powers Ferry Pl. Marietta, GA 30067 Performive LLC c/o Holt Ney Zatcoff & Wasserman, LLP 100 Galleria Parkway, Suite 1800 Atlanta, GA, 30339

APPENDIX A

LIST OF IP ADDRESSES AND HOSTING COMPANIES ASSOCIATED WITH TRICKBOT'S COMMAND AND CONTROL SERVERS

IP Addresses of Command and Control Servers	Hosting Companies/Data Centers Where Defendants Have Placed the Command and Control Servers
184.164.137.163	Secured Servers LLC 2353 W. University Dr., Bldg A. Tempe, AZ 85281
192.243.102.123	Cloud Equity Group LLC 14 Wall Street, FL20 New York, NY 10005 Conseev LLC 14 Wall Street, FL20 New York, NY 10005 Conseev LLC 848 N Rainbow Blvd Las Vegas, NV 89107-1103
107.155.137.19 107.155.137.28 107.155.137.7 162.216.0.163 23.239.84.132 23.239.84.136	Trunkspace Hosting 925 de Maisonneuve Ouest, Suite 150 Montreal, QC H3A0A5 c/o Nodes Direct Holdings, LLC 1650 Margaret St Suite 302-351 Jacksonville, FL 32204 Nodes Direct Holdings, LLC 4495 Roosevelt Blvd, Suite 304-241) Jacksonville, FL 32210 Nodes Direct Holdings LLC Cologix, Inc. 421 W. Church St., Suite 429 Jacksonville, FL 32202