EXHIBIT 18

Originals

ORIGINAL DOCUMENT

Richard A. Jacobsen (RJ5136)
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, New York 10019
Telephone: (212) 506-5000
Facsimile: (212) 506-5151

Gabriel M. Ramsey
(pro hac vice application pending)
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, California 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

Attorneys for Plaintiffs
MICROSOFT CORPORATION,
FS-ISAC, INC. and NATIONAL AUTOMATED
CLEARING HOUSE ASSOCIATION

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORP., FS-ISAC, INC., and NATIONAL AUTOMATED CLEARING HOUSE ASSOCIATION,

Plaintiffs

v.

JOHN DOES 1-39 D/B/A Slavik, Monstr, IOO, Nu11, nvidiag, zebra7753, lexa_Mef, gss, iceIX, Harderman, Gribodemon, Aqua, aquaSecond, it, percent, cp01, hct, xman, Pepsi, miami, miamibc, petr0vich, Mr. ICQ, Tank, tankist, Kusunagi, Noname, Lucky, Bashorg, Indep, Mask, Enx, Benny, Bentley, Denis Lubimov, MaDaGaSka, Vkontake, rfcid, parik, reronic, Daniel, bx1, Daniel Hamza, Danielbx1, jah, Jonni, jtk, Veggi Roma, D frank, duo, Admin2010, h4x0rdz, Donsft, mary.J555, susanneon, kainehabe, virus_e_2003, spaishp, sere.bro, muddem, mechan1zm, vlad.dimitrov, jheto2002, sector.exploits AND JabberZeus Crew CONTROLLING COMPUTER BOTNETS THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS,

Defendants.

Case No. 12-1335

FILED UNDER SEAL

KORMAN, J.

MANN, M.J.

WFK [redacted] ***EX PARTE* TEMPORARY RESTRAINING ORDER, SEIZURE ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiffs Microsoft Corp. ("Microsoft"), the FS-ISAC, Inc. (Financial Services-Information Sharing and Analysis Center) ("FS-ISAC"), and the National Automated Clearing House Association ("NACHA") (collectively, the "Plaintiffs") have filed a Complaint for injunctive and other relief pursuant to, the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); violations of the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law of trespass, conversion, and unjust enrichment. Plaintiffs have also moved *ex parte* for an emergency temporary restraining order and seizure order pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C § 1116(d) (the "Lanham Act") and 28 U.S.C. § 1651(a) (the "All Writs Act"), and an order to show cause why a preliminary injunction should not be granted.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiffs' Application for an Emergency Temporary Restraining Order, Seizure Order, and Order to Show Cause for Preliminary Injunction ("TRO Application"), 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 under the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law of trespass, conversion, and unjust enrichment.

2. Microsoft owns the registered trademarks "Microsoft," "Windows," and "Outlook" used in connection with its services, software, and products. FS-ISAC's members

have invested in developing their brands, trademarks and trade names in association with the financial services they offer. NACHA owns the registered trademark "NACHA" and the NACHA logo used in conjunction with its services.

3. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law of trespass, conversion, and unjust enrichment.

4. 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 Defendants' ongoing violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law of trespass, conversion, and unjust enrichment. The evidence set forth in Plaintiffs' 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 laws by: (1) intentionally accessing and sending malicious software to the protected computers and operating systems of the customers or associated member organizations of Microsoft, FS-ISAC, and NACHA, without authorization, in order to infect those computers and make them part of the Zeus Botnets; (2) sending malicious software to configure, deploy and operate a botnet; (3) sending unsolicited spam e-mail to Microsoft's Hotmail accounts; (4) sending unsolicited spam e-mails that falsely indicate that they are from or approved by Plaintiffs or their associated member organizations, the purpose of which is to deceive

computer users into taking steps that will result in the infection of their computers with botnet code and/or the disclosure of personal and financial account information; (5) stealing personal and financial account information from computer users; (6) using stolen information to steal money from the financial accounts of those users; and (7) associating with one another in a common enterprise engaged in these illegal acts. There is good cause to believe that if such conduct continues, irreparable harm will occur to Plaintiffs and the public, including Plaintiffs' customers and associated member organizations. There is good cause to believe that the Defendants are engaging, and will continue to engage, in such unlawful actions if not immediately restrained from doing so by Order of this Court.

5. 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 the botnet command and control software that is hosted at and otherwise operates through the Internet domains listed in Appendix A, the Internet Protocol (IP) addresses listed in Appendix B, and the file directories listed in Exhibit C, 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: (1) Defendants are engaged in activities that directly violate U.S. law and harm Plaintiffs and the public, including Plaintiffs' customers and member-organizations; (2) Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests; (3) Defendants are likely to delete or relocate the botnet command and control software at issue in Plaintiffs' TRO Application and the harmful, malicious, and trademark infringing software disseminated through these IP addresses and domains and to warn their associates engaged in such activities if informed of Plaintiffs' action. Plaintiffs' request for this emergency *ex parte* relief is not the result of any lack of diligence on Plaintiffs' part, but instead is based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P.

65(b) and 15 U.S.C. § 1116(d), good cause and the interests 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.

6. There is good cause to believe that Defendants have engaged in illegal activity using the data centers and/or Internet hosting providers identified in Appendix B to host the 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 identified in Appendix B.

7. There is good cause to believe that to immediately halt the injury caused by Defendants, data and evidence at Defendants' IP addresses identified in Appendix B must be preserved and held in escrow pending further order of the court, Defendants' computing resources related to such IP addresses must then be disconnected from the Internet, Defendants must be prohibited from accessing Defendants' computer resources related to such IP addresses and the data and evidence located on those computer resources must be secured and preserved.

8. There is good cause to believe that to immediately halt the injury caused by Defendants, and to ensure that future prosecution of this case is not rendered fruitless by attempts to delete, hide, conceal, or otherwise render inaccessible the software components that distribute unlicensed copies of Plaintiffs' registered trademarks and carry out other harmful conduct, with respect to Defendants' most current, active command and control IP addresses hosted at data centers operated by Continuum Data Centers LLC and Burstnet Technologies, Inc., the United States Marshals Service in the judicial districts where the data centers are located should be directed to seize, impound and deliver into the custody of third-party escrow service Stroz Friedberg, 1925 Century Park East, Suite 1350, Los Angeles, CA 90067, all of Defendants' computers, servers, electronic data storage devices, software, data or media associated with the IP addresses listed in Appendix B.

9. There is good cause to believe that Defendants have engaged in illegal

activity using the Internet domains identified in Appendix A to this order to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in Appendix A must be immediately redirected to the Microsoft-secured IP address 199.2.137.141 and thus made inaccessible to Defendants.

10. There is good cause to direct that third party Internet registries, data centers, hosting providers and free website hosting providers with a presence in the United States to reasonably assist in the implementation of this Order and refrain from frustrating the implementation and purposes of this Order, pursuant to 28 U.S.C. § 1651(a) (the All Writs Act). There is good cause to direct that U.S.-based ICANN communicate this order to foreign domain registries through which Defendants have registered domains subject to this Order.

11. There is good cause to believe that if Defendants are provided advance notice of Plaintiffs' TRO Application or this Order, they would move the botnet infrastructure, allowing them to continue their misconduct and that they would destroy, move, hide, conceal, or otherwise make inaccessible to the Court evidence of their misconduct, the botnet's activity, the infringing materials, the instrumentalities used to make the infringing materials, and the records evidencing the manufacture and distributing of the infringing materials.

12. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint 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, satisfy Fed. R. Civ. Pro. 4(f)(3), and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) personal delivery upon Defendants who provided to the data centers and Internet hosting providers contact information in the

U.S.; (2) personal delivery through the Hague Convention on Service Abroad or other treaties upon Defendants who provided contact information outside the United States; (3) transmission by e-mail, electronic messaging addresses, facsimile, and mail to the known email and messaging addresses of Defendants and to their contact information provided by Defendants to the domain registrars, registries, data centers, Internet hosting providers, and website providers who host the software code associated with the IP addresses in Appendix B, or through which domains in Appendix A are registered; and (4) publishing notice to the Defendants on a publicly available Internet website and in newspapers in jurisdictions where Defendants are believed to reside.

13. There is good cause to believe that the harm to Plaintiffs of denying the relief requested in their TRO Application outweighs any harm to any legitimate interests of Defendants and that there is no undue burden to any third party.

TEMPORARY RESTRAINING ORDER AND SEIZURE ORDER

IT IS THEREFORE ORDERED as follows:

A. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from: Intentionally accessing and sending malicious software 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 the botnet; sending malicious software to configure, deploy and operate a botnet; sending unsolicited spam e-mail to Microsoft's Hotmail accounts; sending unsolicited spam e-mail that falsely indicate that they are from or approved by Plaintiffs or Plaintiffs' associated member organizations; creating false websites that falsely indicate that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations; or stealing information, money or property from Plaintiffs, Plaintiffs' customers or Plaintiffs' member organizations, or undertaking any similar activity that inflicts harm on Plaintiffs, or the public, including Plaintiffs' customers or associated member organizations.

B. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from configuring, deploying, operating or otherwise participating in or facilitating the botnets described in the TRO Application, including but not limited to the command and control software hosted at and operating through the domains and IP addresses set forth herein and through any other component or element of the botnets in any location.

C. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from using the trademarks "Microsoft," "Windows," "Outlook," "NACHA," the NACHA logo, trademarks of financial institution members of FS-ISAC and/or other trademarks; trade names; service marks; or Internet Domain addresses or names; or acting in any other manner which suggests in any way that Defendants' products or services come from or are somehow sponsored or affiliated with Plaintiffs or Plaintiffs' associated member organizations, and from otherwise unfairly competing with Plaintiffs, misappropriating that which rightfully belongs to Plaintiffs or Plaintiffs' customers or Plaintiffs' associated member organizations, or passing off their goods or services as Plaintiffs or Plaintiffs' associated member organizations.

D. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from infringing Plaintiffs' registered trademarks, Registration Nos. 2872708, 85467641, 2463510, 3419145 and others.

E. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from using in connection with Defendants' activities any false or deceptive designation, representation or description of Defendants' or of their representatives' activities, whether by symbols, words, designs or statements, which would damage or injure Plaintiffs or give Defendants an unfair competitive advantage or result in deception of consumers.

F. Defendants' materials bearing infringing marks, the means of making the counterfeit marks, and records documenting the manufacture, sale, or receipt of things

involved in such violation, in the possession of data centers operated by Continuum Data Centers LLC and Burstnet Technologies, Inc. all pursuant to 15 U.S.C. §1116(d), shall be seized:

1. The seizure at the foregoing data centers and hosting providers shall take place no later than seven (7) days after the date of issue of this order. The seizure may continue from day to day, for a period not to exceed three (3) days, until all items have been seized. The seizure shall be made by the United States Marshals Service. The United States Marshals Service in the judicial districts where the foregoing data centers and hosting providers are located are directed to coordinate with each other and with Plaintiffs and their attorneys in order to carry out this Order such that disablement and seizure of the servers is effected simultaneously, to ensure that Defendants are unable to operate the botnet during the pendency of this case. In order to facilitate such coordination, the United States Marshals in the relevant jurisdictions are set forth, as follows:

a. Northern District of Illinois
U.S. Marshal: Darryl K. McPherson
219 S. Dearborn Street, Room 2444
Chicago, IL 60604
(312) 353-5290

b. Middle District of Pennsylvania
U.S. Marshal: Martin J. Pane
Federal Building
Washington Avenue & Linden Street, Room 231
Scranton, PA 18501
(570) 346-7277

2. The United States Marshals and their deputies shall be accompanied by Plaintiffs' attorneys and forensic experts at the foregoing described seizure, to assist with identifying, inventorying, taking possession of and isolating Defendants' computer resources, command and control software and other software components that are seized. The United States Marshals shall seize Defendants' computers, servers, electronic data storage devices or media associated with Defendants' IP addresses at the hosting companies

set forth above, or a live image of Defendants' data and information on said computers, servers, electronic data storage devices or media, as reasonably determined by the U.S. Marshals Service, Microsoft's forensic experts and/or attorneys. The United States Marshals shall preserve up to four hours of Internet traffic to and from Defendants' servers associated with the IP addresses at the hosting companies set forth above, before disconnecting those computers from the Internet.

3. Stroz Friedberg, 1925 Century Park East, Suite 1350, Los Angeles, CA 90067, tel. (310) 623-3301, will act as substitute custodian of any and all data and properties seized and evidence preserved pursuant to this Order and shall hold harmless the United States Marshals Service, arising from any acts, incidents, or occurrences in connection with the seizure and possession of the defendants' property, including any third-party claims, and the United States Marshal shall be discharged of his or her duties and responsibilities for safekeeping of the seized materials.

4. The United States Marshals accomplishing such seizure are permitted to enter the premises of the data centers operated by Continuum Data Centers LLC and Burstnet Technologies, Inc. in order to serve copies of this Order, carry out the terms of this Order and to verify compliance with this Order. The United States Marshals shall employ whatever reasonable means are necessary to carry out the terms of this Order and to inspect the contents of or connect to any computers, servers, electronic data storage devices, media, room, closets, cabinets, vehicles, containers or desks or documents and to dismantle any equipment utilized by Defendants to carry out the activities prohibited by this Order.

G. Pursuant to the All Writs Act and to effect discovery of the true identities of the John Doe defendants, the domain registries with a presence in the U.S. identified in Appendix A to this Order and the data centers and hosting providers with a U.S. presence identified in Appendix B to this Order, shall:

1. Coordinate with Microsoft to redirect all traffic to the domains in Appendix A to secure servers at a Microsoft-secured IP address: 199.2.137.141, and take all

steps required to propagate the foregoing domain registry changes to domain name registrars;

2. Permit the United States Marshals Service, with the assistance of Stroz Friedberg, to preserve up to four hours of Internet traffic to and from the servers corresponding to each IP addresses set for in Appendix B;

3. Following the preservation of Internet traffic ordered above, disable Defendants' IP addresses set forth in Appendix B (including through any backup systems) so that they can no longer be accessed over the Internet, connected to, or communicated with in any way except as explicitly provided for in this Order;

4. Transfer any content and software hosted on Defendants' IP addresses listed in Appendix B that are not associated with Defendants to new IP addresses not listed in Appendix B; notify any non-party owners of such content or software of the new IP addresses, and direct them to contact Microsoft's Counsel, Gabriel M. Ramsey, Orrick Herrington & Sutcliffe, 1000 Marsh Road, Menlo Park, CA 90425-1015, (Tel: 650-614-7400), to facilitate any follow-on action;

5. Preserve and produce to Plaintiffs documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the IP addresses set forth in Appendix B, 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 and contact records;

6. Provide reasonable assistance in implementing the terms of this Order and shall take no action to frustrate the implementation of this Order, including the provision of sufficient and reasonable access to offices, facilities, computer networks, computers and services, so that the United States Marshals Service, Plaintiffs, and Plaintiffs' attorneys and/or representatives may directly supervise and confirm the implementation of this Order against Defendants;

H. Pursuant to the All Writs Act ICANN is directed to communicate this Order

to foreign domain registries identified in Appendix A to this Order.

I. Defendants are directed to permanently disable access to the file paths identified in Appendix C; permanently delete or otherwise disable the content at those file paths; and take all necessary steps to ensure that a such file paths are not re-enabled nor the content recreated. Pursuant to the All Writs Act, U.S. based free website hosting providers of the domains set forth in Appendix C are directed to permanently delete or otherwise disable the content at the file paths in Appendix C.

J. All parties subject to this order shall refrain from providing notice or warning of this Order to Defendants, their representatives or persons who are in active concert or participation with them, until this Order is fully executed. Third-parties subject to this order may share the order within their organizations or with partner organizations (such as domain registrars), only to the extent reasonably necessary to implement the Order.

K. Anyone interfering with the execution of this Order is subject to arrest by federal or state law enforcement officials.

IT IS FURTHER ORDERED that the registries of the domains identified in Exhibit A to this Order (the "Registries") shall implement the provisions of this order in the following fashion:

1. For currently unregistered domains, the domain name registrant for the domains shall be changed to "Microsoft Corp." and the domain name registration point of contact shall be changed to the Microsoft Digital Crimes Unit, with full contact details to be provided hereafter to the domains registries by Microsoft Corp., and associated WHOIS information shall be changed accordingly;

2. For currently registered domains, the domain name registrant information and point of contact shall not be changed and associated WHOIS information shall not be changed;

3. Domain names shall not be deleted or otherwise made available for registration by any party, but rather should remain active and redirected to IP address

199.2.137.141.

4. Domains shall not be transferred to any other person or registrar, pending further order of the court;

5. The Registries shall assume authority for name resolution of domain names to IP address 199.2.137.141, using the name servers of the Registries;

6. Name resolution services shall not be suspended;

7. The Registries shall work with Plaintiffs in good faith to implement this order expeditiously.

IT IS FURTHER ORDERED, notwithstanding 15 U.S.C. § 1116(6), which provides in relevant part that "[a]n order under this subsection, together with the supporting documents, shall be sealed until the person against whom the order is directed has an opportunity to contest such order," that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) by personal delivery upon defendants who provided contact information in the U.S.; (2) personal delivery through the Hague Convention on Service Abroad upon defendants who provided contact information outside the U.S.; (3) by transmission by e-mail, electronic messaging addresses, facsimile and mail to the known contact information of Defendants and to such contact information provided by defendants to the data centers, Internet hosting providers and domain registrars who hosted the software code associated with the IP addresses set forth at Appendix B or through which domains in Appendix A are registered; and (4) by publishing notice to Defendants on a publicly available Internet website or in newspapers in the jurisdictions where Defendants are believed to reside.

IT IS FURTHER ORDERED, notwithstanding 15 U.S.C. § 1116(6), service providers required to take action under this Order and may disclose this Order to employees, agents or other service providers as may reasonably be necessary to implement the Order.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b), 15 U.S.C. §1116(d)(10) and 28 U.S.C. § 1651(a) (the All Writs Act) that Defendants shall

appear before this Court within no more than 28 days from the date of this order, to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this Order. The hearing on Plaintiffs' motion for Preliminary Injunction shall take place on Mar. 29, 2012 at 10 A.m, in Courtroom 636 of the United States District Court, 225 Cadman Plaza East, Brooklyn, NY 11201.

IT IS FURTHER ORDERED that Plaintiffs shall post bond in the amount of $300,000 as cash to be paid into the Court registry.

IT IS FURTHER ORDERED that Plaintiffs shall compensate the data centers, Internet hosting providers and/or domain registries and/or website providers identified in Appendices A, B and C at prevailing rates for technical assistance rendered in implementing the Order.

IT IS FURTHER ORDERED that this Order shall be implemented with the least degree of interference with the normal operation of the data centers and Internet hosting providers and/or domain registries and/or website providers identified in Appendices A, B and C consistent with thorough and prompt implementation of this Order.

IT IS FURTHER ORDERED, specifically with regard to the preserved Internet traffic to and from the servers corresponding to the IP address listed in Exhibit B, that this evidence shall be preserved, held in escrow and kept under seal by Stroz Friedberg, and not accessed by any party, pending further order of this Court.

IT IS FURTHER ORDERED, specifically with regard to the Internet traffic that is redirected from the domains listed in Exhibit A to the Microsoft-secured IP address 199.2.137.141, that Microsoft shall not record more than the IP addresses of incoming connections.

IT IS FURTHER ORDERED that Defendants shall file with the Court and serve on Plaintiffs counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than four (4) days prior to the hearing on Plaintiffs' request

for a preliminary injunction. Plaintiffs may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Pacific Standard Time) on the appropriate dates listed in this paragraph.

IT IS SO ORDERED

Entered this 19th day of March, 2012.

U.S.D.J.