

**IN THE UNITED STATES DISTRICT COURT**  
**NORTHERN DISTRICT OF GEORGIA**  
**ATLANTA DIVISION**

FILED IN CLERK'S OFFICE  
U.S.D.C. - Atlanta

NOV 14 2017

JAMES N. HATTEN, Clerk  
By:  Deputy Clerk

**MICROSOFT CORPORATION**

**Plaintiff,**

**v.**

**JOHN DOES 1-51,  
CONTROLLING MULTIPLE  
COMPUTER BOTNETS  
THEREBY INJURING  
MICROSOFT AND ITS  
CUSTOMERS**

**Defendants.**

**CASE NO.**

**1:17-CV-4566**

**FILED UNDER SEAL**

**DECLARATION OF MICHAEL ZWEIBACK IN SUPPORT OF  
MICROSOFT'S APPLICATION FOR AN EMERGENCY *EX PARTE*  
TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE  
RE: PRELIMINARY INJUNCTION**

**VOLUME 2 OF 3**



10/17/2017

Uniform Domain Name Dispute Resolution Policy - ICANN

[English \(/translations\)](#) [العربية \(/ar\)](#) [Español \(/es\)](#)[Français \(/fr\)](#) [Русский \(/ru\)](#) [中文 \(/zh\)](#)[Log In \(/users/sign\\_in\)](#) [Sign Up \(/users/sign\\_up\)](#)

Search ICANN.org

[GET STARTED \(/GET-STARTED\)](#)[NEWS & MEDIA \(/NEWS\)](#)[POLICY \(/POLICY\)](#)[PUBLIC COMMENT \(/PUBLIC-COMMENTS\)](#)[RESOURCES \(/RESOURCES\)](#)[COMMUNITY \(/COMMUNITY\)](#)[IANA STEWARDSHIP  
& ACCOUNTABILITY \(/STEWARDSHIP-ACCOUNTABILITY\)](#)[LANGUAGE PREFERENCE \(/TRANSLATIONS\)](#)

## Resources

## Uniform Domain Name (Domain Name) Dispute Resolution Policy

- ▶ [About ICANN  
\(Internet Corporation for  
Assigned Names  
and Numbers\)](#)

[\(/resources/pages/welcome-2012-02-25-en\)](#)

- ▶ [Board  
\(/resources/pages/board-of-directors-2014-03-19-en\)](#)

- ▶ [Accountability  
\(/resources/accountability\)](#)

- ▶ [Governance  
\(/resources/pages/governance-2012-02-25-en\)](#)

This page is available in:

English | [العربية \(http://www.icann.org/resources/pages/policy-2012-02-25-ar\)](#) |[Deutsch \(http://www.icann.org/resources/pages/policy-2012-02-25-de\)](#) |[Español \(http://www.icann.org/resources/pages/policy-2012-02-25-es\)](#) |[Français \(http://www.icann.org/resources/pages/policy-2012-02-25-fr\)](#) |[Italiano \(http://www.icann.org/resources/pages/policy-2012-02-25-it\)](#) |[日本語 \(http://www.icann.org/resources/pages/policy-2012-02-25-ja\)](#) |[한국어 \(http://www.icann.org/resources/pages/policy-2012-02-25-ko\)](#) |[Português \(http://www.icann.org/resources/pages/policy-2012-02-25-pt\)](#) |[Русский \(http://www.icann.org/resources/pages/policy-2012-02-25-ru\)](#) |[中文 \(http://www.icann.org/resources/pages/policy-2012-02-25-zh\)](#)

Policy Adopted: August 26, 1999

Implementation Documents Approved: October 24, 1999

### Notes:

10/17/2017

Uniform Domain Name Dispute Resolution Policy - ICANN

- Groups  
(/resources/pages/groups-2012-02-06-en)

**1. This policy is now in effect. See [www.icann.org/udrp/udrp-schedule.htm](http://www.icann.org/udrp/udrp-schedule.htm) ([udrp/udrp-schedule.htm](http://udrp/udrp-schedule.htm)) for the implementation schedule.**
- Business  
(/resources/pages/business)

**2. This policy has been adopted by all ICANN (Internet Corporation for Assigned Names and Numbers)-accredited registrars. It has also been adopted by certain managers of country-code top-level domains (e.g., .nu, .tv, .ws).**
- Civil Society  
(/resources/pages/civil-society-2016-05-24-en)

**3. The policy is between the registrar (or other registration authority in the case of a country-code top-level domain) and its customer (the domain-name holder or registrant). Thus, the policy uses "we" and "our" to refer to the registrar and it uses "you" and "your" to refer to the domain-name holder.**
- Complaints Office  
(/resources/pages/complaints-office-2017-04-26-en)

**Uniform Domain Name (Domain Name) Dispute Resolution Policy**  
(As Approved by ICANN (Internet Corporation for Assigned Names and Numbers) on October 24, 1999)
- Contractual Compliance  
(/resources/pages/compliance-2012-02-25-en)

**1. Purpose.** This Uniform Domain Name (Domain Name) Dispute Resolution Policy (the "Policy") has been adopted by the Internet Corporation for Assigned Names and Numbers ("ICANN (Internet Corporation for Assigned Names and Numbers)"), is incorporated by reference into your Registration Agreement, and sets forth the terms and conditions in connection with a dispute between you and any party other than us (the registrar) over the registration and use of an Internet domain name registered by you. Proceedings under Paragraph 4 of this Policy will be conducted according to the Rules for Uniform Domain Name (Domain Name) Dispute Resolution Policy (the "Rules of Procedure"), which are available at <https://www.icann.org/resources/pages/udrp-rules-2015-03-11-en> ([/resources/pages/udrp-rules-2015-03-11-en](http://resources/pages/udrp-rules-2015-03-11-en)), and the selected administrative-dispute-resolution service provider's supplemental rules.
- Registrars  
(/resources/pages/registrars-0d-2012-02-25-en)
- Registry Operators  
(/resources/pages/registries-46-2012-02-25-en)
- Domain Name (Domain Name) Registrants  
(/resources/pages/domain-name-registrants-2017-06-20-en)

**2. Your Representations.** By applying to register a domain name, or by asking us to maintain or renew a domain name registration, you hereby represent and warrant to us that (a) the statements that you made in your Registration Agreement are complete and accurate; (b) to your knowledge, the registration of the domain name will not infringe upon or otherwise violate the rights of any third party; (c) you are not registering the domain name for an unlawful purpose; and (d) you will not knowingly use the domain name in violation of any applicable laws or regulations. It is your responsibility to determine whether your domain name registration infringes or violates someone else's rights.
- GDD Metrics  
(/resources/pages/metrics-gdd-2015-01-30-en)
- Identifier Systems Security, Stability (Security, Stability and Resiliency) and Resiliency



10/17/2017

Uniform Domain Name Dispute Resolution Policy - ICANN

(OCTO IS-SSR)  
(/resources/pages/octo-  
ssr-2016-10-10-  
en)

**3. Cancellations, Transfers, and Changes.** We will cancel, transfer or otherwise make changes to domain name registrations under the following circumstances:

- ▶ ccTLDs  
(/resources/pages/cctlds-  
21-2012-02-25-  
en)
  - a. subject to the provisions of Paragraph 8, our receipt of written or appropriate electronic instructions from you or your authorized agent to take such action;
  - b. our receipt of an order from a court or arbitral tribunal, in each case of competent jurisdiction, requiring such action; and/or
  - c. our receipt of a decision of an Administrative Panel requiring such action in any administrative proceeding to which you were a party and which was conducted under this Policy or a later version of this Policy adopted by ICANN (Internet Corporation for Assigned Names and Numbers). (See Paragraph 4(i) and (k) below.)
- ▶ Internationalized Domain Names  
(/resources/pages/idn-  
2012-02-25-en)
 

We may also cancel, transfer or otherwise make changes to a domain name registration in accordance with the terms of your Registration Agreement or other legal requirements.
- ▶ Universal Acceptance Initiative  
(/resources/pages/universal-  
acceptance-2012-  
02-25-en)
 

**4. Mandatory Administrative Proceeding.**
- ▶ Policy  
(/resources/pages/policy-  
01-2012-02-25-  
en)
 

This Paragraph sets forth the type of disputes for which you are required to submit to a mandatory administrative proceeding. These proceedings will be conducted before one of the administrative-dispute-resolution service providers listed at [www.icann.org/en/dndr/udrp/approved-providers.htm](http://www.icann.org/en/dndr/udrp/approved-providers.htm) ([/en/dndr/udrp/approved-providers.htm](http://en/dndr/udrp/approved-providers.htm)) (each, a "Provider").
- ▶ Public Comment  
(/public-  
comments)
 

**a. Applicable Disputes.** You are required to submit to a mandatory administrative proceeding in the event that a third party (a "complainant") asserts to the applicable Provider, in compliance with the Rules of Procedure, that
- Root Zone (Root Zone) KSK Rollover  
(/resources/pages/ksk-  
rollover-2016-05-  
06-en)
  - (i) your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and
  - (ii) you have no rights or legitimate interests in respect of the domain name; and
  - (iii) your domain name has been registered and is being used in bad faith.
- ▶ Technical Functions  
(/resources/pages/technical-  
functions-2015-  
10-15-en)
- ▶ Contact (/contact)
- ▼ Help  
(/resources/pages/help-  
2012-02-03-en)

10/17/2017

Uniform Domain Name Dispute Resolution Policy - ICANN

Dispute  
Resolution  
(/resources/pages/dispute-  
resolution-2012-  
02-25-en)

In the administrative proceeding, the complainant must prove that each of these three elements are present.

▼ Domain Name  
(Domain Name)  
Dispute  
Resolution

**b. Evidence of Registration and Use in Bad Faith.** For the purposes of Paragraph 4(a)(iii), the following circumstances, in particular but without limitation, if found by the Panel to be present, shall be evidence of the registration and use of a domain name in bad faith:

(/resources/pages/dndr-  
2012-02-25-en)

(i) circumstances indicating that you have registered or you have acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of your documented out-of-pocket costs directly related to the domain name; or

▶ Charter  
Eligibility  
Dispute  
Resolution  
Policy

(/resources/pages/cedrp-  
2012-02-25-  
en)

(ii) you have registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that you have engaged in a pattern of such conduct; or

▶ Eligibility  
Requirements  
Dispute  
Resolution  
Policy

(/resources/pages/erdrp-  
2012-02-25-  
en)

(iii) you have registered the domain name primarily for the purpose of disrupting the business of a competitor; or

▶ Intellectual  
Property  
Defensive  
Registration  
Challenge  
Policy

(/resources/pages/ipdrp-  
2012-02-25-  
en)

(iv) by using the domain name, you have intentionally attempted to attract, for commercial gain, Internet users to your web site or other on-line location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of your web site or location or of a product or service on your web site or location.

▶ Qualification  
Challenge  
Policy

(/resources/pages/prdp-  
2012-02-25-  
en)

**c. How to Demonstrate Your Rights to and Legitimate Interests in the Domain Name (Domain Name) in Responding to a Complaint.** When you receive a complaint, you should refer to Paragraph 5 (/resources/pages/udrp-rules-2015-03-11-en#5) of the Rules of Procedure in determining how your response should be prepared. Any of the following circumstances, in particular but without limitation, if found by the Panel to be proved based on its evaluation of all evidence presented, shall demonstrate your rights or legitimate interests to the domain name for purposes of Paragraph 4(a)(ii):

▶ Restrictions  
Dispute  
Resolution  
Policy

(/resources/pages/rdrp-

10/17/2017

Uniform Domain Name Dispute Resolution Policy - ICANN

2012-02-25-en)

► Transfer  
Dispute  
Resolution  
Policy

(/resources/pages/tdrp-2012-02-25-en)

(i) before any notice to you of the dispute, your use of, or demonstrable preparations to use, the domain name or a name corresponding to the domain name in connection with a bona fide offering of goods or services; or

▼ Uniform  
Domain Name  
(Domain  
Name)  
Dispute  
Resolution  
Policy

(/resources/pages/udrp-2012-02-25-en)

(ii) you (as an individual, business, or other organization) have been commonly known by the domain name, even if you have acquired no trademark or service mark rights; or

(iii) you are making a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue.

Policy  
Document

(/resources/pages/policy-2012-02-25-en)

Providers

(/resources/pages/providers-2012-02-25-en)

Provider  
Approval  
Process

(/resources/pages/provider-approval-process-2012-02-25-en)

Rules

(/resources/pages/rules-be-2012-02-25-en)

Principal  
Documents

(/resources/pages/principal-2012-02-25-en)

Proceedings

(/resources/pages/proceedings-

**d. Selection of Provider.** The complainant shall select the Provider from among those approved by ICANN (Internet Corporation for Assigned Names and Numbers) by submitting the complaint to that Provider. The selected Provider will administer the proceeding, except in cases of consolidation as described in Paragraph 4(f).

**e. Initiation of Proceeding and Process and Appointment of Administrative Panel.** The Rules of Procedure state the process for initiating and conducting a proceeding and for appointing the panel that will resolve the dispute (the "Administrative Panel").

**f. Consolidation.** In the event of multiple disputes between you and a complainant, either you or the complainant may petition to consolidate the disputes before a single Administrative Panel. This petition shall be made to the first Administrative Panel appointed to hear a pending dispute between the parties. This Administrative Panel may consolidate before it any or all such disputes in its sole discretion, provided that the disputes being consolidated are governed by this Policy or a later version of this Policy adopted by ICANN (Internet Corporation for Assigned Names and Numbers).

**g. Fees.** All fees charged by a Provider in connection with any dispute before an Administrative Panel pursuant to this Policy shall be paid by the complainant, except in cases where you elect to expand the Administrative Panel from one to three panelists as provided in Paragraph 5(b)(iv) (/resources/pages/udrp-rules-2015-03-11-en#5biv) of the Rules of Procedure, in which case all fees will be split evenly by you and the complainant.



10/17/2017

Uniform Domain Name Dispute Resolution Policy - ICANN

2012-02-25-en)

Historical Documents  
(/resources/pages/historical-

2f-2012-02-25-en)

Timeline

(/resources/pages/schedule-2012-02-25-en)

**h. Our Involvement in Administrative Proceedings.** We do not, and will not, participate in the administration or conduct of any proceeding before an Administrative Panel. In addition, we will not be liable as a result of any decisions rendered by the Administrative Panel.

**i. Remedies.** The remedies available to a complainant pursuant to any proceeding before an Administrative Panel shall be limited to requiring the cancellation of your domain name or the transfer of your domain name registration to the complainant.

**j. Notification and Publication.** The Provider shall notify us of any decision made by an Administrative Panel with respect to a domain name you have registered with us. All decisions under this Policy will be published in full over the Internet, except when an Administrative Panel determines in an exceptional case to redact portions of its decision.

► Name Collision

(/resources/pages/name-collision-2013-12-06-en)

Registrar

Problems

(/news/announcement-2007-03-06-en)

Whois Data

Correction

(/resources/pages/dispute-resolution-2012-02-25-en)

Independent

Review Process

(/resources/pages/irp-questions-2010-06-19-en)

Request for

Reconsideration

(/resources/pages/reconsideration-2012-02-25-en)

**k. Availability of Court Proceedings.** The mandatory administrative proceeding requirements set forth in Paragraph 4 shall not prevent either you or the complainant from submitting the dispute to a court of competent jurisdiction for independent resolution before such mandatory administrative proceeding is commenced or after such proceeding is concluded. If an Administrative Panel decides that your domain name registration should be canceled or transferred, we will wait ten (10) business days (as observed in the location of our principal office) after we are informed by the applicable Provider of the Administrative Panel's decision before implementing that decision. We will then implement the decision unless we have received from you during that ten (10) business day period official documentation (such as a copy of a complaint, file-stamped by the clerk of the court) that you have commenced a lawsuit against the complainant in a jurisdiction to which the complainant has submitted under Paragraph 3(b)(xiii) (/resources/pages/udrp-rules-2015-03-11-en#3bxiii) of the Rules of Procedure. (In general, that jurisdiction is either the location of our principal office or of your address as shown in our Whois database. See Paragraphs 1 (/resources/pages/udrp-rules-2015-03-11-en#1mutualjurisdiction) and 3(b)(xiii) (/resources/pages/udrp-rules-2015-03-11-en#3bxiii) of the Rules of Procedure for details.) If we receive such documentation within the ten (10) business day period, we will not implement the Administrative Panel's decision, and we will take no further action, until we receive (i) evidence satisfactory to us of a resolution between the parties; (ii) evidence satisfactory to us that your lawsuit has been dismissed or withdrawn; or (iii) a copy of an order from such court dismissing your lawsuit or ordering that you do not have the right to continue to use your domain name.



10/17/2017

Uniform Domain Name Dispute Resolution Policy - ICANN

**5. All Other Disputes and Litigation.** All other disputes between you and any party other than us regarding your domain name registration that are not brought pursuant to the mandatory administrative proceeding provisions of Paragraph 4 shall be resolved between you and such other party through any court, arbitration or other proceeding that may be available.

**6. Our Involvement in Disputes.** We will not participate in any way in any dispute between you and any party other than us regarding the registration and use of your domain name. You shall not name us as a party or otherwise include us in any such proceeding. In the event that we are named as a party in any such proceeding, we reserve the right to raise any and all defenses deemed appropriate, and to take any other action necessary to defend ourselves.

**7. Maintaining the Status Quo.** We will not cancel, transfer, activate, deactivate, or otherwise change the status of any domain name registration under this Policy except as provided in Paragraph 3 above.

**8. Transfers During a Dispute.**

**a. Transfers of a Domain Name (Domain Name) to a New Holder.** You may not transfer your domain name registration to another holder (i) during a pending administrative proceeding brought pursuant to Paragraph 4 or for a period of fifteen (15) business days (as observed in the location of our principal place of business) after such proceeding is concluded; or (ii) during a pending court proceeding or arbitration commenced regarding your domain name unless the party to whom the domain name registration is being transferred agrees, in writing, to be bound by the decision of the court or arbitrator. We reserve the right to cancel any transfer of a domain name registration to another holder that is made in violation of this subparagraph.

**b. Changing Registrars.** You may not transfer your domain name registration to another registrar during a pending administrative proceeding brought pursuant to Paragraph 4 or for a period of fifteen (15) business days (as observed in the location of our principal place of business) after such proceeding is concluded. You may transfer administration of your domain name registration to another registrar during a pending court action or arbitration, provided that the domain name you have registered with us shall continue to be subject to the proceedings commenced against you in accordance with the terms of this Policy. In the event that you transfer a domain name registration to us during the pendency of a court action or arbitration, such dispute shall remain subject to the domain name dispute

10/17/2017

Uniform Domain Name Dispute Resolution Policy - ICANN

policy of the registrar from which the domain name registration was transferred.

**9. Policy Modifications.** We reserve the right to modify this Policy at any time with the permission of ICANN (Internet Corporation for Assigned Names and Numbers). We will post our revised Policy at <URL (Uniform Resource Locator)> at least thirty (30) calendar days before it becomes effective. Unless this Policy has already been invoked by the submission of a complaint to a Provider, in which event the version of the Policy in effect at the time it was invoked will apply to you until the dispute is over, all such changes will be binding upon you with respect to any domain name registration dispute, whether the dispute arose before, on or after the effective date of our change. In the event that you object to a change in this Policy, your sole remedy is to cancel your domain name registration with us, provided that you will not be entitled to a refund of any fees you paid to us. The revised Policy will apply to you until you cancel your domain name registration

© 2017 Internet Corporation For Assigned Names and Numbers. [Privacy Policy \(/en/help/privacy\)](#)  
[Terms of Service \(/en/help/tos\)](#) [Cookie Policy \(/en/help/privacy-cookie-policy\)](#)

10/17/2017

Uniform Domain Name Dispute Resolution Policy - ANN

Who We Are	Contact Us	Accountability & Transparency	Governance	Help
<a href="#">Get Started</a> (/get-started)	<a href="#">Locations</a> (https://forms.icann.org/locations)	<a href="#">Accountability Mechanisms</a> (/en/news/in-focus/accountability/mechanisms)	<a href="#">Documents</a> (/en/about/governance/documents)	<a href="#">Dispute Resolution</a> (/en/help/dispute-resolution)
<a href="#">Learning</a> (/en/about/learning)	<a href="#">Global Support</a> (/resources/pages/customer-support-2015-06-22-en)	<a href="#">Independent Review Process</a> (/resources/pages/irp-2012-02-25-en)	<a href="#">Agreements</a> (/en/about/agreements)	<a href="#">Domain Name Dispute Resolution</a> (/en/help/dndr)
<a href="#">Participate</a> (/en/about/participate)	<a href="#">Security Team</a> (/about/staff/security)	<a href="#">Request for Reconsideration</a> (/groups/board/governance/about/financials)	<a href="#">Specific Reviews</a> (/resources/reviews/aoc)	<a href="#">Name Collision</a> (/en/help/name-collision)
<a href="#">Groups</a> (https://www.icann.org/2012-02-06-en)	<a href="#">PGP Keys</a> (/en/contact/pgp-keys)	<a href="#">Ombudsman</a> (/help/ombudsman)	<a href="#">Annual Report</a> (/about/annual-report)	<a href="#">Registrar Problems</a> (/en/news/announcements/announcements-mar07-en.htm)
<a href="#">Board of Directors</a> (/resources/pages/board-of-directors-2014-03-19-en)	<a href="#">Certificate Authority</a> (/contact/certificate-authority)	<a href="#">Empowered Community</a> (/ec)	<a href="#">Financials</a> (/en/about/financials)	<a href="#">WHOIS</a> (http://whois.icann.org/)
<a href="#">President's Corner</a> (/presidents-corner)	<a href="#">Registry Liaison</a> (/resources/pages/contact-f2-2012-02-25-en)		<a href="#">Document Disclosure</a> (/en/about/transparency)	
<a href="#">Staff</a> (/organization)			<a href="#">Planning</a> (/en/about/planning)	
<a href="#">Careers</a> (https://www.icann.org/careers)	<a href="#">Specific Reviews</a> (https://forms.icann.org/en/about/aoc-review/contact)		<a href="#">KPI Dashboard</a> (/progress)	
<a href="#">Newsletter</a> (/en/news/newsletter)	<a href="#">Organizational Reviews</a> (http://forms.icann.org/en/groups/reviews/contact)		<a href="#">RFPs</a> (/en/news/rfps)	
<a href="#">Public Responsibility</a> (https://www.icann.org/public-responsibility)	<a href="#">Complaints Office</a> (https://www.icann.org/complaints-office)		<a href="#">Litigation</a> (/en/news/litigation)	
	<a href="#">Request a Speaker</a> (http://forms.icann.org/en/contact/speakers)		<a href="#">Correspondence</a> (/en/news/correspondence)	
	<a href="#">For Journalists</a> (/en/news/press)			





10/17/2017

Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules") - ICANN

[English \(/translations\)](#) [العربية \(/ar\)](#) [Español \(/es\)](#)[Français \(/fr\)](#) [Русский \(/ru\)](#) [中文 \(/zh\)](#)[Log In \(/users/sign\\_in\)](#) [Sign Up \(/users/sign\\_up\)](#)

Search ICANN.org

[GET STARTED \(/GET-STARTED\)](#)[NEWS & MEDIA \(/NEWS\)](#)[POLICY \(/POLICY\)](#)[PUBLIC COMMENT \(/PUBLIC-COMMENTS\)](#)[RESOURCES \(/RESOURCES\)](#)[COMMUNITY \(/COMMUNITY\)](#)[IANA STEWARDSHIP  
& ACCOUNTABILITY \(/STEWARDSHIP-ACCOUNTABILITY\)](#)[LANGUAGE PREFERENCE \(/TRANSLATIONS\)](#)

## Resources

## Rules for Uniform Domain Name (Domain Name) Dispute Resolution Policy (the "Rules")

- ▶ [About ICANN  
\(Internet  
Corporation for  
Assigned Names  
and Numbers\)  
\(/resources/pages/welcome-2012-02-25-en\)](#)

This page is available in:

English |

[العربية \(http://www.icann.org/resources/pages/udrp-rules-2015-03-12-ar\)](http://www.icann.org/resources/pages/udrp-rules-2015-03-12-ar) |[Español \(http://www.icann.org/resources/pages/udrp-rules-2015-03-12-es\)](http://www.icann.org/resources/pages/udrp-rules-2015-03-12-es) |[Français \(http://www.icann.org/resources/pages/udrp-rules-2015-03-12-fr\)](http://www.icann.org/resources/pages/udrp-rules-2015-03-12-fr) |[日本語 \(http://www.icann.org/resources/pages/udrp-rules-2015-03-12-ja\)](http://www.icann.org/resources/pages/udrp-rules-2015-03-12-ja) |[한국어 \(http://www.icann.org/resources/pages/udrp-rules-2015-03-12-ko\)](http://www.icann.org/resources/pages/udrp-rules-2015-03-12-ko) |[Português \(http://www.icann.org/resources/pages/udrp-rules-2015-03-13-pt\)](http://www.icann.org/resources/pages/udrp-rules-2015-03-13-pt) |[Русский \(http://www.icann.org/resources/pages/udrp-rules-2015-03-12-ru\)](http://www.icann.org/resources/pages/udrp-rules-2015-03-12-ru) |[中文 \(http://www.icann.org/resources/pages/udrp-rules-2015-03-12-zh\)](http://www.icann.org/resources/pages/udrp-rules-2015-03-12-zh)

- ▶ [Board  
\(/resources/pages/board-of-directors-2014-03-19-en\)](#)
- ▶ [Accountability  
\(/resources/accountability\)](#)
- ▶ [Governance  
\(/resources/pages/governance-2012-02-25-en\)](#)

As approved by the ICANN (Internet Corporation for Assigned Names and Numbers) Board of Directors on 28 September 2013 [\(/resources/board-material/resolutions-2013-09-28-en#1.c\)](#).

10/17/2017

Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules") - ICANN

- ▶ Groups  
(/resources/pages/groups-2012-02-06-en)  
  
Business  
(/resources/pages/business-2012-02-25-en)  
  
Civil Society  
(/resources/pages/civil-society-2016-05-24-en)
  - ▶ Complaints Office  
(/resources/pages/complaints-office-2017-04-26-en)
  - ▶ Contractual Compliance  
(/resources/pages/compliance-2012-02-25-en)
- These Rules are in effect for all UDRP (Uniform Domain-Name Dispute Resolution Policy) proceedings in which a complaint is submitted to a provider on or after 31 July 2015. The prior version of the Rules, applicable to all proceedings in which a complaint was submitted to a Provider on or before 30 July 2015, is at <https://www.icann.org/resources/pages/rules-be-2012-02-25-en> (/resources/pages/rules-be-2012-02-25-en). UDRP (Uniform Domain-Name Dispute Resolution Policy) Providers may elect to adopt the notice procedures set forth in these Rules prior to 31 July 2015.**
- Administrative proceedings for the resolution of disputes under the Uniform Dispute Resolution Policy adopted by ICANN (Internet Corporation for Assigned Names and Numbers) shall be governed by these Rules and also the Supplemental Rules of the Provider administering the proceedings, as posted on its web site. To the extent that the Supplemental Rules of any Provider conflict with these Rules, these Rules supersede.

## 1 Definitions

In these Rules:

- ▶ Registrars  
(/resources/pages/registrars-0d-2012-02-25-en)
  - ▶ Registry Operators  
(/resources/pages/registries-46-2012-02-25-en)
  - ▶ Domain Name (Domain Name) Registrants  
(/resources/pages/domain-name-registrants-2017-06-20-en)
  - GDD Metrics  
(/resources/pages/metrics-gdd-2015-01-30-en)
  - ▶ Identifier Systems Security, Stability (Security, Stability and Resiliency) and Resiliency
- Complainant** means the party initiating a complaint concerning a domain-name registration.
- ICANN (Internet Corporation for Assigned Names and Numbers)** refers to the Internet Corporation for Assigned Names and Numbers.
- Lock** means a set of measures that a registrar applies to a domain name, which prevents at a minimum any modification to the registrant and registrar information by the Respondent, but does not affect the resolution of the domain name or the renewal of the domain name.
- Mutual Jurisdiction** means a court jurisdiction at the location of either (a) the principal office of the Registrar (provided the domain-name holder has submitted in its Registration Agreement to that jurisdiction for court adjudication of disputes concerning or arising from the use of the domain name) or (b) the domain-name holder's address as shown for the registration of the domain name in Registrar's Whois database at the time the complaint is submitted to the Provider.



10/17/2017

Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules") - ICANN

(OCTO IS-SSR)  
(/resources/pages/octo-  
ssr-2016-10-10-  
en)

- ▶ ccTLDs  
(/resources/pages/cctlds-  
21-2012-02-25-  
en)
- ▶ Internationalized  
Domain Names  
(/resources/pages/idn-  
2012-02-25-en)
- ▶ Universal  
Acceptance  
Initiative  
(/resources/pages/universal-  
acceptance-2012-  
02-25-en)
- ▶ Policy  
(/resources/pages/policy-  
01-2012-02-25-  
en)
- ▶ Public Comment  
(/public-  
comments)
- Root Zone (Root  
Zone) KSK  
Rollover  
(/resources/pages/ksk-  
rollover-2016-05-  
06-en)
- ▶ Technical  
Functions  
(/resources/pages/technical-  
functions-2015-  
10-15-en)
- ▶ Contact (/contact)
- ▶ Help  
(/resources/pages/help-  
2012-02-03-en)

**Panel** means an administrative panel appointed by a Provider to decide a complaint concerning a domain-name registration.

**Panelist** means an individual appointed by a Provider to be a member of a Panel.

**Party** means a Complainant or a Respondent.

**Pendency** means the time period from the moment a UDRP (Uniform Domain-Name Dispute Resolution Policy) complaint has been submitted by the Complainant to the UDRP (Uniform Domain-Name Dispute Resolution Policy) Provider to the time the UDRP (Uniform Domain-Name Dispute Resolution Policy) decision has been implemented or the UDRP (Uniform Domain-Name Dispute Resolution Policy) complaint has been terminated.

**Policy** means the Uniform Domain Name (Domain Name) Dispute Resolution Policy (/en/dndr/udrp/policy.htm) that is incorporated by reference and made a part of the Registration Agreement.

**Provider** means a dispute-resolution service provider approved by ICANN (Internet Corporation for Assigned Names and Numbers). A list of such Providers appears at <http://www.icann.org/en/dndr/udrp/approved-providers.htm> ([/en/dndr/udrp/approved-providers.htm](http://www.icann.org/en/dndr/udrp/approved-providers.htm)).

**Registrar** means the entity with which the Respondent has registered a domain name that is the subject of a complaint.

**Registration Agreement** means the agreement between a Registrar and a domain-name holder.

**Respondent** means the holder of a domain-name registration against which a complaint is initiated.

**Reverse Domain Name (Domain Name) Hijacking** means using the Policy in bad faith to attempt to deprive a registered domain-name holder of a domain name.

**Supplemental Rules** means the rules adopted by the Provider administering a proceeding to supplement these Rules. Supplemental Rules shall not be inconsistent with the Policy or these Rules and shall cover such topics as fees, word and page limits and guidelines, file size and format modalities, the means for

10/17/2017

Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules") - ICANN

communicating with the Provider and the Panel, and the form of cover sheets.

**Written Notice** means hardcopy notification by the Provider to the Respondent of the commencement of an administrative proceeding under the Policy which shall inform the respondent that a complaint has been filed against it, and which shall state that the Provider has electronically transmitted the complaint including any annexes to the Respondent by the means specified herein. Written notice does not include a hardcopy of the complaint itself or of any annexes.

## 2. Communications

(a) When forwarding a complaint, including any annexes, electronically to the Respondent, it shall be the Provider's responsibility to employ reasonably available means calculated to achieve actual notice to Respondent. Achieving actual notice, or employing the following measures to do so, shall discharge this responsibility:

(i) sending Written Notice of the complaint to all postal-mail and facsimile addresses (A) shown in the domain name's registration data in Registrar's Whois database for the registered domain-name holder, the technical contact, and the administrative contact and (B) supplied by Registrar to the Provider for the registration's billing contact; and

(ii) sending the complaint, including any annexes, in electronic form by e-mail to:

(A) the e-mail addresses for those technical, administrative, and billing contacts;

(B) postmaster@<the contested domain name>; and

(C) if the domain name (or "www." followed by the domain name) resolves to an active web page (other than a generic page the Provider concludes is maintained by a registrar or ISP (Internet Service Provider) for parking domain-names registered by multiple domain-name holders), any e-mail address shown or e-mail links on that web page; and

10/17/2017

Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules") - ICANN

(iii) sending the complaint, including any annexes, to any e-mail address the Respondent has notified the Provider it prefers and, to the extent practicable, to all other e-mail addresses provided to the Provider by Complainant under Paragraph 3(b)(v) (/en/help/dndr/udrp/rules#3bv).

(b) Except as provided in Paragraph 2(a) (/en/help/dndr/udrp/rules#2a), any written communication to Complainant or Respondent provided for under these Rules shall be made electronically via the Internet (a record of its transmission being available), or by any reasonably requested preferred means stated by the Complainant or Respondent, respectively (see Paragraphs 3(b)(iii) (/en/help/dndr/udrp/rules#3biii) and 5(b)(iii) (/en/help/dndr/udrp/rules#5biii)).

(c) Any communication to the Provider or the Panel shall be made by the means and in the manner (including, where applicable, the number of copies) stated in the Provider's Supplemental Rules.

(d) Communications shall be made in the language prescribed in Paragraph 11 (/en/help/dndr/udrp/rules#11).

(e) Either Party may update its contact details by notifying the Provider and the Registrar.

(f) Except as otherwise provided in these Rules, or decided by a Panel, all communications provided for under these Rules shall be deemed to have been made:

(i) if via the Internet, on the date that the communication was transmitted, provided that the date of transmission is verifiable; or, where applicable

(ii) if delivered by telecopy or facsimile transmission, on the date shown on the confirmation of transmission; or:

(iii) if by postal or courier service, on the date marked on the receipt.

(g) Except as otherwise provided in these Rules, all time periods calculated under these Rules to begin when a communication is



10/17/2017

Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules") - ICANN

made shall begin to run on the earliest date that the communication is deemed to have been made in accordance with Paragraph 2(f) (/en/help/dndr/udrp/rules#2f).

(h) Any communication by

(i) a Panel to any Party shall be copied to the Provider and to the other Party;

(ii) the Provider to any Party shall be copied to the other Party; and

(iii) a Party shall be copied to the other Party, the Panel and the Provider, as the case may be.

(i) It shall be the responsibility of the sender to retain records of the fact and circumstances of sending, which shall be available for inspection by affected parties and for reporting purposes. This includes the Provider in sending Written Notice to the Respondent by post and/or facsimile under Paragraph 2(a)(i).

(j) In the event a Party sending a communication receives notification of non-delivery of the communication, the Party shall promptly notify the Panel (or, if no Panel is yet appointed, the Provider) of the circumstances of the notification. Further proceedings concerning the communication and any response shall be as directed by the Panel (or the Provider).

### 3. The Complaint

(a) Any person or entity may initiate an administrative proceeding by submitting a complaint in accordance with the Policy and these Rules to any Provider approved by ICANN (Internet Corporation for Assigned Names and Numbers). (Due to capacity constraints or for other reasons, a Provider's ability to accept complaints may be suspended at times. In that event, the Provider shall refuse the submission. The person or entity may submit the complaint to another Provider.)

(b) The complaint including any annexes shall be submitted in electronic form and shall:

10/17/2017

Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules") - ICANN

- (i) Request that the complaint be submitted for decision in accordance with the Policy and these Rules;
- (ii) Provide the name, postal and e-mail addresses, and the telephone and telefax numbers of the Complainant and of any representative authorized to act for the Complainant in the administrative proceeding;
- (iii) Specify a preferred method for communications directed to the Complainant in the administrative proceeding (including person to be contacted, medium, and address information) for each of (A) electronic-only material and (B) material including hard copy (where applicable);
- (iv) Designate whether Complainant elects to have the dispute decided by a single-member or a three-member Panel and, in the event Complainant elects a three-member Panel, provide the names and contact details of three candidates to serve as one of the Panelists (these candidates may be drawn from any ICANN (Internet Corporation for Assigned Names and Numbers)-approved Provider's list of panelists);
- (v) Provide the name of the Respondent (domain-name holder) and all information (including any postal and e-mail addresses and telephone and telefax numbers) known to Complainant regarding how to contact Respondent or any representative of Respondent, including contact information based on pre-complaint dealings, in sufficient detail to allow the Provider to send the complaint as described in Paragraph 2(a) (/en/help/dndr/udrp/rules#2a);
- (vi) Specify the domain name(s) that is/are the subject of the complaint;
- (vii) Identify the Registrar(s) with whom the domain name(s) is/are registered at the time the complaint is filed;
- (viii) Specify the trademark(s) or service mark(s) on which the complaint is based and, for each mark, describe the goods or services, if any, with which the mark is used (Complainant may also separately describe other goods and services with

10/17/2017

Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules") - ICANN

which it intends, at the time the complaint is submitted, to use the mark in the future.);

(ix) Describe, in accordance with the Policy, the grounds on which the complaint is made including, in particular,

(1) the manner in which the domain name(s) is/are identical or confusingly similar to a trademark or service mark in which the Complainant has rights; and

(2) why the Respondent (domain-name holder) should be considered as having no rights or legitimate interests in respect of the domain name(s) that is/are the subject of the complaint; and

(3) why the domain name(s) should be considered as having been registered and being used in bad faith

(The description should, for elements (2) and (3), discuss any aspects of Paragraphs 4(b) (/en/dndr/udrp/policy.htm#4b) and 4(c) (/en/dndr/udrp/policy.htm#4c) of the Policy that are applicable. The description shall comply with any word or page limit set forth in the Provider's Supplemental Rules.);

(x) Specify, in accordance with the Policy, the remedies sought;

(xi) Identify any other legal proceedings that have been commenced or terminated in connection with or relating to any of the domain name(s) that are the subject of the complaint;

(xii) State that Complainant will submit, with respect to any challenges to a decision in the administrative proceeding canceling or transferring the domain name, to the jurisdiction of the courts in at least one specified Mutual Jurisdiction;

(xiii) Conclude with the following statement followed by the signature (in any electronic format) of the Complainant or its authorized representative:



10/17/2017

Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules") - ICANN

"Complainant agrees that its claims and remedies concerning the registration of the domain name, the dispute, or the dispute's resolution shall be solely against the domain-name holder and waives all such claims and remedies against (a) the dispute-resolution provider and panelists, except in the case of deliberate wrongdoing, (b) the registrar, (c) the registry administrator, and (d) the Internet Corporation for Assigned Names and Numbers, as well as their directors, officers, employees, and agents."

"Complainant certifies that the information contained in this Complaint is to the best of Complainant's knowledge complete and accurate, that this Complaint is not being presented for any improper purpose, such as to harass, and that the assertions in this Complaint are warranted under these Rules and under applicable law, as it now exists or as it may be extended by a good-faith and reasonable argument."; and

(xiv) Annex any documentary or other evidence, including a copy of the Policy applicable to the domain name(s) in dispute and any trademark or service mark registration upon which the complaint relies, together with a schedule indexing such evidence.

(c) The complaint may relate to more than one domain name, provided that the domain names are registered by the same domain-name holder.

#### 4. Notification of Complaint

(a) The Provider shall submit a verification request to the Registrar. The verification request will include a request to Lock the domain name.

(b) Within two (2) business days of receiving the Provider's verification request, the Registrar shall provide the information requested in the verification request and confirm that a Lock of the domain name has been applied. The Registrar shall not notify the Respondent of the proceeding until the Lock status has been

10/17/2017

Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules") - ICANN

applied. The Lock shall remain in place through the remaining Pendency of the UDRP (Uniform Domain-Name Dispute Resolution Policy) proceeding. Any updates to the Respondent's data, such as through the result of a request by a privacy or proxy provider to reveal the underlying customer data, must be made before the two (2) business day period concludes or before the Registrar verifies the information requested and confirms the Lock to the UDRP (Uniform Domain-Name Dispute Resolution Policy) Provider, whichever occurs first. Any modification(s) of the Respondent's data following the two (2) business day period may be addressed by the Panel in its decision.

(c) The Provider shall review the complaint for administrative compliance with the Policy and these Rules and, if in compliance, shall forward the complaint, including any annexes, electronically to the Respondent and Registrar and shall send Written Notice of the complaint (together with the explanatory cover sheet prescribed by the Provider's Supplemental Rules) to the Respondent, in the manner prescribed by Paragraph 2(a) (/en/help/dndr/udrp/rules#2a), within three (3) calendar days following receipt of the fees to be paid by the Complainant in accordance with Paragraph 19 (/en/help/dndr/udrp/rules#19).

(d) If the Provider finds the complaint to be administratively deficient, it shall promptly notify the Complainant and the Respondent of the nature of the deficiencies identified. The Complainant shall have five (5) calendar days within which to correct any such deficiencies, after which the administrative proceeding will be deemed withdrawn without prejudice to submission of a different complaint by Complainant.

(e) If the Provider dismisses the complaint due to an administrative deficiency, or the Complainant voluntarily withdraws its complaint, the Provider shall inform the Registrar that the proceedings have been withdrawn, and the Registrar shall release the Lock within one (1) business day of receiving the dismissal or withdrawal notice from the Provider.

(f) The date of commencement of the administrative proceeding shall be the date on which the Provider completes its responsibilities under Paragraph 2(a) (/en/help/dndr/udrp/rules#2a) in connection with sending the complaint to the Respondent.

10/17/2017

Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules") - ICANN

(g) The Provider shall immediately notify the Complainant, the Respondent, the concerned Registrar(s), and ICANN (Internet Corporation for Assigned Names and Numbers) of the date of commencement of the administrative proceeding. The Provider shall inform the Respondent that any corrections to the Respondent's contact information during the remaining Pendency of the UDRP (Uniform Domain-Name Dispute Resolution Policy) proceedings shall be communicated to the Provider further to Rule 5(c)(ii) and 5(c)(iii).

## 5. The Response

(a) Within twenty (20) days of the date of commencement of the administrative proceeding the Respondent shall submit a response to the Provider.

(b) The Respondent may expressly request an additional four (4) calendar days in which to respond to the complaint, and the Provider shall automatically grant the extension and notify the Parties thereof. This extension does not preclude any additional extensions that may be given further to 5(d) of the Rules.

(c) The response, including any annexes, shall be submitted in electronic form and shall:

(i) Respond specifically to the statements and allegations contained in the complaint and include any and all bases for the Respondent (domain-name holder) to retain registration and use of the disputed domain name (This portion of the response shall comply with any word or page limit set forth in the Provider's Supplemental Rules.);

(ii) Provide the name, postal and e-mail addresses, and the telephone and telefax numbers of the Respondent (domain-name holder) and of any representative authorized to act for the Respondent in the administrative proceeding;

(iii) Specify a preferred method for communications directed to the Respondent in the administrative proceeding (including person to be contacted, medium, and address information) for each of (A) electronic-only material and (B) material including hard copy (where applicable);

10/17/2017

Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules") - ICANN

(iv) If Complainant has elected a single-member panel in the complaint (see Paragraph 3(b)(iv) (/en/help/dndr/udrp/rules#3biv)), state whether Respondent elects instead to have the dispute decided by a three-member panel;

(v) If either Complainant or Respondent elects a three-member Panel, provide the names and contact details of three candidates to serve as one of the Panelists (these candidates may be drawn from any ICANN (Internet Corporation for Assigned Names and Numbers)-approved Provider's list of panelists);

(vi) Identify any other legal proceedings that have been commenced or terminated in connection with or relating to any of the domain name(s) that are the subject of the complaint;

(vii) State that a copy of the response including any annexes has been sent or transmitted to the Complainant, in accordance with Paragraph 2(b) (/en/help/dndr/udrp/rules#2b); and

(viii) Conclude with the following statement followed by the signature (in any electronic format) of the Respondent or its authorized representative:

"Respondent certifies that the information contained in this Response is to the best of Respondent's knowledge complete and accurate, that this Response is not being presented for any improper purpose, such as to harass, and that the assertions in this Response are warranted under these Rules and under applicable law, as it now exists or as it may be extended by a good-faith and reasonable argument."; and

(ix) Annex any documentary or other evidence upon which the Respondent relies, together with a schedule indexing such documents.

(d) If Complainant has elected to have the dispute decided by a single-member Panel and Respondent elects a three-member



10/17/2017

Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules") - ICANN

Panel, Respondent shall be required to pay one-half of the applicable fee for a three-member Panel as set forth in the Provider's Supplemental Rules. This payment shall be made together with the submission of the response to the Provider. In the event that the required payment is not made, the dispute shall be decided by a single-member Panel.

(e) At the request of the Respondent, the Provider may, in exceptional cases, extend the period of time for the filing of the response. The period may also be extended by written stipulation between the Parties, provided the stipulation is approved by the Provider.

(f) If a Respondent does not submit a response, in the absence of exceptional circumstances, the Panel shall decide the dispute based upon the complaint.

## 6. Appointment of the Panel and Timing of Decision

(a) Each Provider shall maintain and publish a publicly available list of panelists and their qualifications.

(b) If neither the Complainant nor the Respondent has elected a three-member Panel (Paragraphs 3(b)(iv) (/en/help/dndr/udrp/rules#3biv) and 5(b)(iv) (/en/help/dndr/udrp/rules#5biv)), the Provider shall appoint, within five (5) calendar days following receipt of the response by the Provider, or the lapse of the time period for the submission thereof, a single Panelist from its list of panelists. The fees for a single-member Panel shall be paid entirely by the Complainant.

(c) If either the Complainant or the Respondent elects to have the dispute decided by a three-member Panel, the Provider shall appoint three Panelists in accordance with the procedures identified in Paragraph 6(e) (/en/help/dndr/udrp/rules#6e). The fees for a three-member Panel shall be paid in their entirety by the Complainant, except where the election for a three-member Panel was made by the Respondent, in which case the applicable fees shall be shared equally between the Parties.

(d) Unless it has already elected a three-member Panel, the Complainant shall submit to the Provider, within five (5) calendar

10/17/2017

Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules") - ICANN

days of communication of a response in which the Respondent elects a three-member Panel, the names and contact details of three candidates to serve as one of the Panelists. These candidates may be drawn from any ICANN (Internet Corporation for Assigned Names and Numbers)-approved Provider's list of panelists.

(e) In the event that either the Complainant or the Respondent elects a three-member Panel, the Provider shall endeavor to appoint one Panelist from the list of candidates provided by each of the Complainant and the Respondent. In the event the Provider is unable within five (5) calendar days to secure the appointment of a Panelist on its customary terms from either Party's list of candidates, the Provider shall make that appointment from its list of panelists. The third Panelist shall be appointed by the Provider from a list of five candidates submitted by the Provider to the Parties, the Provider's selection from among the five being made in a manner that reasonably balances the preferences of both Parties, as they may specify to the Provider within five (5) calendar days of the Provider's submission of the five-candidate list to the Parties.

(f) Once the entire Panel is appointed, the Provider shall notify the Parties of the Panelists appointed and the date by which, absent exceptional circumstances, the Panel shall forward its decision on the complaint to the Provider.

## 7. Impartiality and Independence

A Panelist shall be impartial and independent and shall have, before accepting appointment, disclosed to the Provider any circumstances giving rise to justifiable doubt as to the Panelist's impartiality or independence. If, at any stage during the administrative proceeding, new circumstances arise that could give rise to justifiable doubt as to the impartiality or independence of the Panelist, that Panelist shall promptly disclose such circumstances to the Provider. In such event, the Provider shall have the discretion to appoint a substitute Panelist.

## 8. Communication Between Parties and the Panel

No Party or anyone acting on its behalf may have any unilateral communication with the Panel. All communications between a Party and the Panel or the Provider shall be made to a case administrator appointed by the Provider in the manner prescribed in the Provider's Supplemental Rules.

## 9. Transmission of the File to the Panel

The Provider shall forward the file to the Panel as soon as the Panelist is appointed in the case of a Panel consisting of a single member, or as soon as the last Panelist is appointed in the case of a three-member Panel.

## 10. General Powers of the Panel

(a) The Panel shall conduct the administrative proceeding in such manner as it considers appropriate in accordance with the Policy and these Rules.

(b) In all cases, the Panel shall ensure that the Parties are treated with equality and that each Party is given a fair opportunity to present its case.

(c) The Panel shall ensure that the administrative proceeding takes place with due expedition. It may, at the request of a Party or on its own motion, extend, in exceptional cases, a period of time fixed by these Rules or by the Panel.

(d) The Panel shall determine the admissibility, relevance, materiality and weight of the evidence.

(e) A Panel shall decide a request by a Party to consolidate multiple domain name disputes in accordance with the Policy and these Rules.

## 11. Language of Proceedings

(a) Unless otherwise agreed by the Parties, or specified otherwise in the Registration Agreement, the language of the administrative proceeding shall be the language of the Registration Agreement, subject to the authority of the Panel to determine otherwise, having regard to the circumstances of the administrative proceeding.

(b) The Panel may order that any documents submitted in languages other than the language of the administrative proceeding be accompanied by a translation in whole or in part into the language of the administrative proceeding.

## 12. Further Statements

In addition to the complaint and the response, the Panel may request, in its sole discretion, further statements or documents from either of the Parties.

## 13. In-Person Hearings

There shall be no in-person hearings (including hearings by teleconference, videoconference, and web conference), unless the Panel determines, in its sole discretion and as an exceptional matter, that such a hearing is necessary for deciding the complaint.

## 14. Default

(a) In the event that a Party, in the absence of exceptional circumstances, does not comply with any of the time periods established by these Rules or the Panel, the Panel shall proceed to a decision on the complaint.

(b) If a Party, in the absence of exceptional circumstances, does not comply with any provision of, or requirement under, these Rules or any request from the Panel, the Panel shall draw such inferences therefrom as it considers appropriate.

## 15. Panel Decisions

(a) A Panel shall decide a complaint on the basis of the statements and documents submitted and in accordance with the Policy, these Rules and any rules and principles of law that it deems applicable.

(b) In the absence of exceptional circumstances, the Panel shall forward its decision on the complaint to the Provider within fourteen (14) days of its appointment pursuant to Paragraph 6 (/en/help/dndr/udrp/rules#6).

(c) In the case of a three-member Panel, the Panel's decision shall be made by a majority.

(d) The Panel's decision shall be in writing, provide the reasons on which it is based, indicate the date on which it was rendered and identify the name(s) of the Panelist(s).



10/17/2017

Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules") - ICANN

(e) Panel decisions and dissenting opinions shall normally comply with the guidelines as to length set forth in the Provider's Supplemental Rules. Any dissenting opinion shall accompany the majority decision. If the Panel concludes that the dispute is not within the scope of Paragraph 4(a) (/en/dndr/udrp/policy.htm#4a) of the Policy, it shall so state. If after considering the submissions the Panel finds that the complaint was brought in bad faith, for example in an attempt at Reverse Domain Name (Domain Name) Hijacking or was brought primarily to harass the domain-name holder, the Panel shall declare in its decision that the complaint was brought in bad faith and constitutes an abuse of the administrative proceeding.

## 16. Communication of Decision to Parties

(a) Within three (3) business days after receiving the decision from the Panel, the Provider shall communicate the full text of the decision to each Party, the concerned Registrar(s), and ICANN (Internet Corporation for Assigned Names and Numbers). The concerned Registrar(s) shall within three (3) business days of receiving the decision from the Provider communicate to each Party, the Provider, and ICANN (Internet Corporation for Assigned Names and Numbers) the date for the implementation of the decision in accordance with the Policy.

(b) Except if the Panel determines otherwise (see Paragraph 4(j) (/en/dndr/udrp/policy.htm#4j) of the Policy), the Provider shall publish the full decision and the date of its implementation on a publicly accessible web site. In any event, the portion of any decision determining a complaint to have been brought in bad faith (see Paragraph 15(e) (/en/help/dndr/udrp/rules#15e) of these Rules) shall be published.

## 17. Settlement or Other Grounds for Termination

(a) If, before the Panel's decision, the Parties agree on a settlement, the Panel shall terminate the administrative proceeding. A settlement shall follow steps 17(a)(i) – 17(a)(vii):

(i) The Parties provide written notice of a request to suspend the proceedings because the parties are discussing settlement to the Provider.

10/17/2017

Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules") - ICANN

(ii) The Provider acknowledges receipt of the request for suspension and informs the Registrar of the suspension request and the expected duration of the suspension.

(iii) The Parties reach a settlement and provide a standard settlement form to the Provider further to the Provider's supplemental rules and settlement form. The standard settlement form is not intended to be an agreement itself, but only to summarize the essential terms of the Parties' separate settlement agreement. The Provider shall not disclose the completed standard settlement form to any third party.

(iv) The Provider shall confirm to the Registrar, copying the Parties, the outcome of the settlement as it relates to actions that need to be taken by the Registrar.

(v) Upon receiving notice from the Provider further to 17(a) (iv), the Registrar shall remove the Lock within two (2) business days.

(vi) The Complainant shall confirm to the Provider that the settlement as it relates to the domain name(s) has been implemented further to the Provider's supplemental rules.

(vii) The Provider will dismiss the proceedings without prejudice unless otherwise stipulated in the settlement.

(b) If, before the Panel's decision is made, it becomes unnecessary or impossible to continue the administrative proceeding for any reason, the Panel shall terminate the administrative proceeding, unless a Party raises justifiable grounds for objection within a period of time to be determined by the Panel.

## 18. Effect of Court Proceedings

(a) In the event of any legal proceedings initiated prior to or during an administrative proceeding in respect of a domain-name dispute that is the subject of the complaint, the Panel shall have the discretion to decide whether to suspend or terminate the administrative proceeding, or to proceed to a decision.

10/17/2017

Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules") - ICANN

(b) In the event that a Party initiates any legal proceedings during the Pendency of an administrative proceeding in respect of a domain-name dispute that is the subject of the complaint, it shall promptly notify the Panel and the Provider. See Paragraph 8 (/en/help/dndr/udrp/rules#8) above.

## 19. Fees

(a) The Complainant shall pay to the Provider an initial fixed fee, in accordance with the Provider's Supplemental Rules, within the time and in the amount required. A Respondent electing under Paragraph 5(b)(iv) (/en/help/dndr/udrp/rules#5biv) to have the dispute decided by a three-member Panel, rather than the single-member Panel elected by the Complainant, shall pay the Provider one-half the fixed fee for a three-member Panel. See Paragraph 5(c) (/en/help/dndr/udrp/rules#5c). In all other cases, the Complainant shall bear all of the Provider's fees, except as prescribed under Paragraph 19(d) (/en/help/dndr/udrp/rules#19d). Upon appointment of the Panel, the Provider shall refund the appropriate portion, if any, of the initial fee to the Complainant, as specified in the Provider's Supplemental Rules.

(b) No action shall be taken by the Provider on a complaint until it has received from Complainant the initial fee in accordance with Paragraph 19(a) (/en/help/dndr/udrp/rules#19a).

(c) If the Provider has not received the fee within ten (10) calendar days of receiving the complaint, the complaint shall be deemed withdrawn and the administrative proceeding terminated.

(d) In exceptional circumstances, for example in the event an in-person hearing is held, the Provider shall request the Parties for the payment of additional fees, which shall be established in agreement with the Parties and the Panel.

## 20. Exclusion of Liability

Except in the case of deliberate wrongdoing, neither the Provider nor a Panelist shall be liable to a Party for any act or omission in connection with any administrative proceeding under these Rules.

10/17/2017

Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules") - ICANN

## 21. Amendments

The version of these Rules in effect at the time of the submission of the complaint to the Provider shall apply to the administrative proceeding commenced thereby. These Rules may not be amended without the express written approval of ICANN (Internet Corporation for Assigned Names and Numbers).

© 2017 Internet Corporation For Assigned Names and Numbers. [Privacy Policy \(/en/help/privacy\)](#)

[Terms of Service \(/en/help/tos\)](#)

[Cookie Policy \(/en/help/privacy-cookie-policy\)](#)



10/17/2017

Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules") - ICANN

Who We Are	Contact Us	Accountability & Transparency	Governance	Help
<a href="#">Get Started</a> (/get-started)	<a href="#">Locations</a> (https://forms.icann.org/locations)	<a href="#">Accountability Mechanisms</a> (/en/news/in-focus/accountability/mechanisms)	<a href="#">Documents</a> (/en/about/governance/documents)	<a href="#">Dispute Resolution</a> (/en/help/dispute-resolution)
<a href="#">Learning</a> (/en/about/learning)	<a href="#">Global Support</a> (/resources/pages/customer-support-2015-06-22-en)	<a href="#">Independent Review Process</a> (/resources/pages/irp-2012-02-25-en)	<a href="#">Agreements</a> (/en/about/agreements)	<a href="#">Domain Name Dispute Resolution</a> (/en/help/dndr)
<a href="#">Participate</a> (/en/about/participate)	<a href="#">Security Team</a> (/about/staff/security)	<a href="#">Request for Reconsideration</a> (/groups/board/governance/about/5days)	<a href="#">Specific Reviews</a> (/resources/reviews/aoc)	<a href="#">Name Collision</a> (/en/help/name-collision)
<a href="#">Groups</a> (https://www.icann.org/2012-02-06-en)	<a href="#">PGP Keys</a> (/en/contact/pgp-keys)	<a href="#">Ombudsman</a> (/help/ombudsman)	<a href="#">Annual Report</a> (/about/annual-report)	<a href="#">Registrar Problems</a> (/en/news/announcements/announcements-mar07-en.htm)
<a href="#">Board of Directors</a> (/resources/pages/board-of-directors-2014-03-19-en)	<a href="#">Certificate Authority</a> (/contact/certificate-authority)	<a href="#">Empowered Community</a> (/ec)	<a href="#">Financials</a> (/en/about/financials)	<a href="#">WHOIS</a> (http://whois.icann.org/)
<a href="#">President's Corner</a> (/presidents-corner)	<a href="#">Registry Liaison</a> (/resources/pages/contact-2012-02-25-en)	<a href="#">Planning</a> (/en/about/planning)	<a href="#">Document Disclosure</a> (/en/about/transparency)	
<a href="#">Staff</a> (/organization)	<a href="#">Specific Reviews</a> (https://forms.icann.org/en/about/aoc-review/contact)	<a href="#">KPI Dashboard</a> (/progress)	<a href="#">Litigation</a> (/en/news/litigation)	
<a href="#">Careers</a> (https://www.icann.org/careers)	<a href="#">Organizational Reviews</a> (http://forms.icann.org/en/groups/reviews/contact)	<a href="#">RFPs</a> (/en/news/rfps)	<a href="#">Correspondence</a> (/en/news/correspondence)	
<a href="#">Newsletter</a> (/en/news/newsletter)	<a href="#">Complaints Office</a> (https://www.icann.org/complaints-office)			
<a href="#">Public Responsibility</a> (https://www.icann.org/public-responsibility)	<a href="#">Request a Speaker</a> (http://forms.icann.org/en/contact/speakers)			
	<a href="#">For Journalists</a> (/en/news/press)			



# Afilias Domain Anti-Abuse Policy

Revised 27 June 2017

To report potential abuse to Afilias please email [abuse@afilias.info](mailto:abuse@afilias.info).

The following policy ("Afilias Domain Anti-Abuse Policy") is announced pursuant to section 3.5.2 of the Registry-Registrar Agreement ("RRA") in effect between Afilias and each of its Registrars, and is effective upon thirty days' notice by Afilias to Registrars. Abusive use(s) of domain names within Afilias owned and operated Top Level Domains (TLDs) should not be tolerated.

The nature of such abuses creates security and stability issues for the registry, registrars and registrants, as well as for users of the Internet in general. Afilias defines abusive use as the wrong or excessive use of power, position or ability, and includes, without limitation, the following:

- Illegal or fraudulent actions;
- Spam: The use of electronic messaging systems to send unsolicited bulk messages. The term applies to e-mail spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of Websites and Internet forums. An example, for purposes of illustration, would be the use of email in denial-of-service attacks;
- Phishing: The use of counterfeit Web pages that are designed to trick recipients into divulging sensitive data such as usernames, passwords, or financial data;
- Pharming: The redirecting of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning;
- Willful distribution of malware: The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent. Examples include, without limitation, computer viruses, worms, keyloggers, and trojan horses;
- Fast flux hosting: Use of fast-flux techniques to disguise the location of Websites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities. Fast-flux techniques use DNS to frequently change the location on the Internet to which the domain name of an Internet host or name server resolves. Fast flux hosting may be used only with prior permission of Afilias;
- Botnet command and control: Services run on a domain name that are used to control a collection of compromised computers or "zombies," or to direct denial-of-service attacks (DDoS attacks);
- Distribution of child pornography; and
- Illegal Access to Other Computers or Networks: Illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). Also, any activity that might be used as a precursor to an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity).

Pursuant to Section 3.6.5 of the RRA, Afilias reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name(s) on registry lock, hold or similar status, that it deems necessary, in its discretion; (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any

dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of Afiliat, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement or (5) to correct mistakes made by Afiliat or any Registrar in connection with a domain name registration. Afiliat also reserves the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute. Abusive uses, as defined above, undertaken with respect to domain names within the TLD shall give rise to the right of Afiliat to take such actions under Section 3.6.5 of the RRA in its sole discretion.

Registrars shall include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.





1 DAVID SHONKA  
Acting General Counsel

**FILED**

JUN - 2 2009

RICHARD J. KLECKING  
CLERK, U.S. DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN JOSE

2 Ethan Arenson, DC # 473296  
3 Carl Settlemeyer, DC # 454272  
4 Philip Tumminio, DC # 985624  
Federal Trade Commission  
600 Pennsylvania Avenue, N.W.  
5 Washington, DC 20580  
(202) 326-2204 (Arenson)  
6 (202) 326-2019 (Settlemeyer)  
(202) 326-2204 (Tumminio)  
7 (202) 326-3395 *facsimile*  
earenson@ftc.gov  
8 csettlemeyer@ftc.gov  
ptumminio@ftc.gov

9 Attorneys for Plaintiff Federal Trade Commission

11 **UNITED STATES DISTRICT COURT**  
12 **NORTHERN DISTRICT OF CALIFORNIA**  
13 **San Jose Division**

14 **Federal Trade Commission,**

15 **Plaintiff,**

16 **v.**

17 **Pricewert LLC d/b/a 3FN.net, Triple Fiber**  
18 **Network, APS Telecom and APX Telecom,**  
19 **APS Communications, and APS**  
**Communication,**

20 **Defendant.**

09-2407  
Case No. 09-02447 RMW

**EX PARTE TEMPORARY  
RESTRAINING ORDER AND  
ORDER TO SHOW CAUSE**

21 Plaintiff, the Federal Trade Commission ("FTC" or "Commission"), pursuant to Section  
22 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b), has filed a  
23 Complaint for Injunctive and Other Equitable Relief, and has moved *ex parte* for a temporary  
24 restraining order and for an order to show cause why a preliminary injunction should not be  
25 granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure.

26 **FINDINGS**

27 The Court has considered the pleadings, declarations, exhibits, and memoranda filed in

28 TRO and  
Order to Show Cause

12

1 support of the Commission's motion and finds that:

- 2 1. This Court has jurisdiction over the subject matter of this case and there is good  
3 cause to believe that it will have jurisdiction over all parties hereto; the Complaint  
4 states a claim upon which relief may be granted against the Defendant under  
5 Section 5(a) of the FTC Act, 15 U.S.C. § 45(a) (2006).
- 6 2. There is good cause to believe that Pricewert LLC also d/b/a 3FN.net, Triple Fiber  
7 Network, APS Telecom and APX Telecom, APS Communications, and APS  
8 Communication (the "Defendant"), has engaged in and is likely to engage in acts or  
9 practices that violate Section 5(a) of the FTC Act, 15 U.S.C. § 45(a) (2006), and  
10 that the Commission is, therefore, likely to prevail on the merits of this action;
- 11 3. There is good cause to believe that immediate and irreparable harm will result from  
12 the Defendant's ongoing violations of Section 5(a) of the FTC Act unless the  
13 Defendant is restrained and enjoined by Order of this Court. The evidence set  
14 forth in the Commission's Memorandum of Law in Support of *Ex Parte* Motion  
15 for Temporary Restraining Order and Order to Show Cause ("TRO Motion"), and  
16 the accompanying declarations and exhibits, demonstrates that the Commission is  
17 likely to prevail on its claim that Defendant has engaged in unfair acts or practices  
18 in violation of Section 5(a) of the FTC Act by: recruiting, distributing and hosting  
19 electronic code or content that inflicts harm upon consumers, including, but not  
20 limited to, child pornography, botnet command and control servers, spyware,  
21 viruses, trojans, and phishing-related sites; and configuring, deploying, and  
22 operating botnets. There is good cause to believe that the Defendant will continue  
23 to engage in such unlawful actions if not immediately restrained from doing so by  
24 Order of this Court;
- 25 4. There is good cause to believe that immediate and irreparable damage to this  
26 Court's ability to grant effective final relief will result from the sale, transfer, or  
27 other disposition or concealment by the Defendant of its assets, business records,  
28

1 or other discoverable evidence if the Defendant receives advance notice of this  
2 action. Based on the evidence cited in the Commission's Motion and  
3 accompanying declarations and exhibits, the Commission is likely to be able to  
4 prove that: (1) the Defendant has operated through a series of maildrops and shell  
5 companies, with a principal place of business and its principals located outside of  
6 the United States; (2) the Defendant has continued its unlawful operations  
7 unabated despite requests from the Internet security community to cease its  
8 injurious activities; (3) the Defendant is engaged in activities that directly violate  
9 U.S. law and cause significant harm to consumers; and (4) that Defendant is likely  
10 to relocate the harmful and malicious code it hosts and/or warn its criminal  
11 clientele of this action if informed of the Commission's action. The Commission's  
12 request for this emergency *ex parte* relief is not the result of any lack of diligence  
13 on the Commission's part, but instead is based upon the nature of the Defendant's  
14 unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b) and Civil  
15 L.R. 65-1, good cause and the interests of justice require that this Order be Granted  
16 without prior notice to the Defendant, and, accordingly, the Commission is relieved  
17 of the duty to provide the Defendant with prior notice of the Commission's motion;

- 18 5. There is good cause to believe that the Defendant, which is controlled by  
19 individuals outside of the United States, has engaged in illegal activity using Data  
20 Centers and Upstream Service Providers based in the United States and that to  
21 immediately halt the injury caused by Defendant, such Data Centers and Upstream  
22 Service Providers must be ordered to immediately disconnect Defendant's  
23 computing resources from the Internet without providing advance notice to the  
24 Defendant, prevent the Defendant and others from accessing such computer  
25 resources, and prevent the destruction of data located on these computer resources;  
26 6. Weighing the equities and considering the Plaintiff's likelihood of ultimate  
27 success, this Order is in the public interest; and  
28



- 1 7. Fed. R. Civ. P. 65(c) does not require security of the United States or an officer or  
2 agency thereof for the issuance of a restraining order.  
3

4 **DEFINITIONS**

5 For the purpose of this order, the following definitions shall apply:

- 6 1. **"Assets"** means any legal or equitable interest in, right to, or claim to, any real,  
7 personal, or intellectual property of Defendant or held for the benefit of Defendant  
8 wherever located, including, but not limited to, chattel, goods, instruments,  
9 equipment, fixtures, general intangibles, effects, leaseholds, contracts, mail or  
10 other deliveries, shares of stock, inventory, checks, notes, accounts, credits,  
11 receivables (as those terms are defined in the Uniform Commercial Code), cash,  
12 and trusts, including but not limited to any other trust held for the benefit of  
13 Defendant.  
14 2. **"Botnet"** means a network of computers that have been compromised by malicious  
15 code and surreptitiously programmed to follow instructions issued by a Botnet  
16 Command and Control Server.  
17 3. **"Botnet Command and Control Server"** means a computer or computers used to  
18 issue instructions to, or otherwise control, a Botnet.  
19 4. The term **"Child Pornography"** shall have the same meaning as provided in 18  
20 U.S.C. § 2256.  
21 5. **"Data Center"** means any person or entity that contracts with third parties to house  
22 computer servers and associated equipment, and provides the infrastructure to  
23 support such equipment, such as power or environmental controls.  
24 6. **"Day"** shall have the meaning prescribed by and time periods in this Order shall be  
25 calculated pursuant to Fed. R. Civ. P. 6(a).  
26 7. **"Defendant"** means Pricewert LLC also d/b/a 3FN.net, Triple Fiber Network,  
27 APS Telecom, APX Telecom, APS Communications, APS Communication, and  
28

1 any other names under which it does business, and any subsidiaries, corporations,  
2 partnerships, or other entities directly or indirectly owned, managed, or controlled  
3 by Pricewert LLC.

- 4 8. **"Document"** is synonymous in meaning and equal in scope to the usage of the  
5 term in the Federal Rules of Civil Procedure 34(a), and includes writing, drawings,  
6 graphs, charts, Internet sites, Web pages, Web sites, electronic correspondence,  
7 including e-mail and instant messages, photographs, audio and video recordings,  
8 contracts, accounting data, advertisements (including, but not limited to,  
9 advertisements placed on the World Wide Web), FTP Logs, Server Access Logs,  
10 USENET Newsgroup postings, World Wide Web pages, books, written or printed  
11 records, handwritten notes, telephone logs, telephone scripts, receipt books,  
12 ledgers, personal and business canceled checks and check registers, bank  
13 statements, appointment books, computer records, and other data compilations  
14 from which information can be obtained and translated. A draft or non-identical  
15 copy is a separate document within the meaning of the term.

- 16 9. **"Phishing"** means the use of email, Internet web sites, or other means to mimic or  
17 copy the appearance of a trustworthy entity for the purpose of duping consumers  
18 into disclosing personal information, such as account numbers and passwords.

- 19 10. **"Representatives"** means the following persons or entities who receive actual  
20 notice of this temporary restraining order by personal service or otherwise: (1) the  
21 Defendant's officers, agents, servants, employees, and attorneys; and (2) all other  
22 persons who are in active concert or participation with Defendant or its officers,  
23 agents, servants, employees, or attorneys. A Data Center or Upstream Service  
24 Provider that continues to provide services to Defendant after receiving actual  
25 notice of this temporary restraining order is a Representative.

- 26 11. **"Spyware"** means any type of software that is surreptitiously installed on a  
27 computer and, without the consent of the user, could collect information from a  
28

1 computer, could allow third parties to control remotely the use of a computer, or  
2 could facilitate botnet communications.

3 12. **"Trojan Horse"** means a computer program with an apparent or actual useful  
4 function that contains additional, undisclosed malicious code, including but not  
5 limited to spyware, viruses, or code that facilitates the surreptitious download or  
6 installation of other software code.

7 13. **"Upstream Service Provider"** means any entity that provides the means to  
8 connect to the Internet, including, but not limited to, the subleasing of Internet  
9 Protocol addresses.

10 14. **"Viruses"** means computer programs designed to spread from one computer to  
11 another and to interfere with the operation of the computers they infect.

## 12 **PROHIBITED BUSINESS ACTIVITIES**

### 13 **I.**

14 **IT IS THEREFORE ORDERED** that, Defendant and its Representatives are temporarily  
15 restrained and enjoined from recruiting or willingly distributing or hosting Child Pornography,  
16 Botnet Command and Control Servers, Spyware, Viruses, Trojan Horses, Phishing-related sites, or  
17 similar electronic code or content that inflicts harm upon consumers.

### 18 **II.**

19 **IT IS FURTHER ORDERED** that Defendant and its Representatives are temporarily  
20 restrained and enjoined from configuring, deploying, operating, or otherwise participating in or  
21 otherwise willingly facilitating, any Botnet.

## 22 **SUSPENSION OF INTERNET CONNECTIVITY**

### 23 **III.**

24 **IT IS FURTHER ORDERED** that, pending determination of the Commission's request  
25 for a preliminary injunction, that:

26 A. Any Data Center in active concert or participation with and providing services to Defendant  
27 or Defendant's officers, agents, servants, or employees shall immediately, and without notifying  
28



1 Defendant or Defendant's officers, agents, servants, or employees, take all reasonable and  
2 necessary steps to make inaccessible to the Defendant and all other persons, all computers, servers  
3 or electronic data storage devices or media and the content stored thereupon (hereafter "computer  
4 resources"), leased, owned or operated by Defendant or Defendant's officers agents, servants, or  
5 employees and located on premises owned by, or within the control of, the Data Center. Such  
6 steps shall, at a minimum, include:

- 7 1. disconnecting such computer resources from the Internet and all other networks;
- 8 2. securing the area where such computer resources are located in a manner reasonably  
9 calculated to deny access to the Defendant and its officers, agents, servants, or  
10 employees; and
- 11 3. if such Data Center restricts access to its facilities by means of access credentials,  
12 suspending all access credentials issued to Defendant or Defendant's officers,  
13 agents, servants, or employees;

14 B. Any Upstream Service Provider in active concert or participation with and providing  
15 services to Defendant or Defendant's officers, agents, servants, or employees shall immediately,  
16 and without notifying Defendant or Defendant's officers, agents, servants, or employees, take all  
17 reasonable and necessary steps to deny Internet connectivity to the Defendant and Defendant's  
18 officers, agents, servants, and employees, including, but not limited to, suspending any IP  
19 addresses assigned to the Defendant or Defendant's officers, agents, servants, or employees by the  
20 Upstream Service Provider, and refraining from reassigning such IP addresses;

21 C. Any Data Center or Upstream Service Provider described in subparagraphs A and B above  
22 providing services to Defendant or Defendant's officers, agents, servants, or employees, shall  
23 preserve and retain documents relating to the Defendant or the Defendant's officers, agents,  
24 servants, or employees; and

25 D. Agents of the Commission and other law enforcement agencies are permitted to enter the  
26 premises of any of Defendant's Data Centers and Upstream Service Providers described in  
27 subparagraphs A and B above to serve copies of this Order and to verify that the Data Centers and  
28



1 Upstream Service Providers have taken the reasonable and necessary steps described in sub-  
2 paragraphs A and B of this Paragraph.  
3 *Provided, however,* nothing in Paragraph III shall be interpreted to deny access to any law  
4 enforcement agency granted access pursuant to a court order, search warrant, or other lawful  
5 process.

#### 6 **ASSET FREEZE**

#### 7 **IV.**

8 **IT IS FURTHER ORDERED** that the Defendant and its Representatives are hereby  
9 temporarily restrained and enjoined from:

10 A. Transferring, liquidating, converting, encumbering, pledging, loaning, selling,  
11 concealing, dissipating, disbursing, assigning, spending, withdrawing, granting a lien or security  
12 interest or other interest in, or otherwise disposing of any funds, real or personal property,  
13 accounts, contracts, consumer lists, shares of stock, or other assets, or any interest therein,  
14 wherever located, that are: (1) owned or controlled by the Defendant, in whole or in part, for the  
15 benefit of the Defendant; (2) in the actual or constructive possession of the Defendant; or (3)  
16 owned, controlled by, or in the actual or constructive possession of any corporation, partnership, or  
17 other entity directly or indirectly owned, managed, or controlled by any the Defendant, including,  
18 but not limited to, any assets held by or for, or subject to access by, the Defendant, at any bank or  
19 savings and loan institution, or with any broker-dealer, escrow agent, title company, commodity  
20 trading company, precious metals dealer, or other financial institution or depository of any kind;  
21 and

22 B. Opening or causing to be opened any safe deposit boxes titled in the name of the  
23 Defendant, or subject to access by the Defendant.

24 *Provided, however,* that the assets affected by Paragraph IV shall include: (1) all of the  
25 assets of the Defendant existing as of the date this Order was entered; and (2) for assets obtained  
26 after the date this Order was entered, only those assets of the Defendant that are derived from  
27 conduct prohibited in Paragraphs I and II of this Order.

28 TRO and  
Order to Show Cause

**FINANCIAL REPORTS AND ACCOUNTING**

**V.**

**IT IS FURTHER ORDERED** that the Defendant, within five (5) days of receiving notice of this Order, shall provide the Commission with completed financial statements, verified under oath and accurate as of the date of entry of this Order, on the forms attached to this Order as Attachment A.

**RETENTION OF ASSETS AND PRODUCTION OF RECORDS  
BY FINANCIAL INSTITUTIONS**

**VI.**

**IT IS FURTHER ORDERED** that, any financial or brokerage institution, business entity, or person served with a copy of this Order that holds, controls, or maintains custody of any account or asset of the Defendant, or has held, controlled or maintained custody of any such account or asset at any time prior to the date of entry of this Order, shall:

A. Hold and retain within its control and prohibit the withdrawal, removal, assignment, transfer, pledge, encumbrance, disbursement, dissipation, conversion, sale, or other disposal of any such asset except by further order of the Court; and

B. Deny all persons access to any safe deposit box that is:

1. titled in the name of the Defendant; or
2. otherwise subject to access by Defendant.

**FOREIGN ASSET REPATRIATION AND ACCOUNTING**

**VII.**

**IT IS FURTHER ORDERED** that:

A. Defendant and its Representatives shall immediately upon service of this Order, or as soon as relevant banking hours permit, transfer to the territory of the United States to a blocked account whose funds cannot be withdrawn without further order of the court all funds and assets in foreign countries held: (1) by Defendant; (2) for its benefit; or (3) under its direct or indirect control, jointly or singly; and

TRO and  
Order to Show Cause

1 B. Defendant shall, within five (5) days of receiving notice of this Order each provide  
2 the Commission with a full accounting, verified under oath and accurate as of the date of this  
3 Order, of all funds, documents, and assets outside of the United States which are: (1) titled in the  
4 Defendant's name; or (2) held by any person or entity for the benefit of the Defendant; or (3) under  
5 the direct or indirect control, whether jointly or singly, of the Defendant; and

6 C. Defendant and its Representatives are temporarily restrained and enjoined from  
7 taking any action, directly or indirectly, which may result in the encumbrance or dissipation of  
8 foreign assets, including but not limited to:

- 9 1. Sending any statement, letter, fax, e-mail or wire transmission, telephoning or  
10 engaging in any other act, directly or indirectly, that results in a determination by a  
11 foreign trustee or other entity that a "duress" event has occurred under the terms of a  
12 foreign trust agreement; or
- 13 2. Notifying any trustee, protector or other agent of any foreign trust or other related  
14 entities of the existence of this Order, or that an asset freeze is required pursuant to  
15 a Court Order, until such time that a full accounting has been provided pursuant to  
16 this Paragraph.

#### 17 ACCESS TO BUSINESS RECORDS

#### 18 VIII.

19 IT IS FURTHER ORDERED that the Defendant shall allow the Commission's  
20 representatives, agents, and assistants access to the Defendant's business records to inspect and  
21 copy documents so that the Commission may prepare for the preliminary injunction hearing and  
22 identify and locate assets. Accordingly, the Defendant shall, within forty-eight (48) hours of  
23 receiving notice of this Order, produce to the Commission and the Commission's representatives,  
24 agents, and assistants for inspection, inventory, and/or copying, at Federal Trade Commission, 600  
25 Pennsylvania Avenue NW, Room H-286, Washington DC 20580, Attention: Ethan Arenson, the  
26 following materials: (1) all client information, including, but not limited to, names, phone  
27 numbers, addresses, email addresses, and payment information for all clients of Defendant's  
28



1 services; (2) contracts; (3) correspondence, including, but not limited to, electronic correspondence  
2 and Instant Messenger communications, that refer or relate to the Defendant's services; and (4)  
3 accounting information, including, but not limited to, profit and loss statements, annual reports,  
4 receipt books, ledgers, personal and business canceled checks and check registers, bank statements,  
5 and appointment books.

6 *Provided, however, this Paragraph excludes any record or other information pertaining to a*  
7 *subscriber or customer of an electronic communications service or a remote computing service as*  
8 *those terms are defined in the Electronic Communications Privacy Act, 18 U.S.C. § 2703(c)*  
9 *(2006).*

10 The Commission shall return produced materials pursuant to this Paragraph within five (5)  
11 days of completing said inventory and copying.

## 12 **EXPEDITED DISCOVERY**

### 13 **IX.**

14 **IT IS FURTHER ORDERED** that pursuant to Federal Rules of Civil Procedure 30(a),  
15 31(a), 34, and 45, and notwithstanding the provisions of Federal Rules of Civil Procedure 26(d)  
16 and (f), 30(a)(2)(A)-(C), and 31(a)(2)(A)-(C), the Commission is granted leave, at any time after  
17 entry of this Order to:

18 A. Take the deposition of any person or entity, whether or not a party, for the purpose  
19 of discovering the nature, location, status, and extent of the assets of the Defendant; the location of  
20 any premises where the Defendant conducts business operations; and

21 B. Demand the production of documents from any person or entity, whether or not a  
22 party, relating to the nature, status, and extent of the assets of the Defendant; the location of any  
23 premises where the Defendant, directly or through any third party, conducts business operations.

24 Three (3) calendar days notice shall be deemed sufficient for any such deposition, five (5) calendar  
25 days notice shall be deemed sufficient for the production of any such documents, and twenty-four  
26 (24) hours notice shall be deemed sufficient for the production of any such documents that are  
27 maintained or stored only as electronic data. The provisions of this Section shall apply both to  
28

TRO and  
Order to Show Cause



1 parties to this case and to non-parties. The limitations and conditions set forth in Federal Rules of  
2 Civil Procedure 30(a)(2)(B) and 31(a)(2)(B) regarding subsequent depositions of an individual  
3 shall not apply to depositions taken pursuant to this Section. Any such depositions taken pursuant  
4 to this Section shall not be counted toward any limit on the number of depositions under the  
5 Federal Rules of Civil Procedure or the Local Rules of Civil Procedure for the United States  
6 District Court for Northern District of California, including those set forth in Federal Rules of Civil  
7 Procedure 30(a)(2)(A) and 31(a)(2)(A).

#### 8 **PRESERVATION OF RECORDS**

##### 9 **X.**

10 **IT IS FURTHER ORDERED** that the Defendant and its Representatives are hereby  
11 temporarily restrained and enjoined from destroying, erasing, mutilating, concealing, altering,  
12 transferring, writing over, or otherwise disposing of, in any manner, directly or indirectly, any  
13 documents or records of any kind that relate to the business practices or business finances of the  
14 Defendant, including but not limited to, computerized files and storage media on which  
15 information has been saved (including, but not limited to, hard drives, DVDs, CD-ROMS, zip  
16 disks, floppy disks, punch cards, magnetic tape, backup tapes, and computer chips), and any and all  
17 equipment needed to read any such documents or records, FTP logs, Service Access Logs,  
18 USENET Newsgroup postings, World Wide Web pages, books, written or printed records,  
19 handwritten notes, telephone logs, telephone scripts, receipt books, ledgers, personal and business  
20 canceled checks and check registers, bank statements, appointment books, copies of federal, state  
21 or local business or personal income or property tax returns, and other documents or records of any  
22 kind that relate to the business practices or finances of the Defendant or its officers, agents,  
23 servants, or employees.

#### 24 **RECORD KEEPING/BUSINESS OPERATIONS**

##### 25 **XI.**

26 **IT IS FURTHER ORDERED** that the Defendant is hereby temporarily restrained and  
27 enjoined from:

28 TRO and  
Order to Show Cause

1 A. Failing to maintain documents that, in reasonable detail, accurately, fairly, and  
2 completely reflect its income, disbursements, transactions, and use of money; and

3 B. Creating, operating, or exercising any control over any business entity, including  
4 any partnership, limited partnership, joint venture, sole proprietorship, or corporation, without first  
5 providing the Commission with a written statement disclosing: (1) the name of the business entity;  
6 (2) the address and telephone number of the business entity; (3) the names of the business entity's  
7 officers, directors, principals, managers and employees; and (4) a detailed description of the  
8 business entity's intended activities.

9 **DISTRIBUTION OF ORDER BY DEFENDANT**

10 **XII.**

11 **IT IS FURTHER ORDERED** that the Defendant shall immediately provide a copy of this  
12 Order to each of its subsidiaries, Upstream Service Providers, Data Centers, divisions, sales  
13 entities, successors, assigns, officers, directors, employees, independent contractors, client  
14 companies, agents, and attorneys, and shall, within ten (10) days from the date of entry of this  
15 Order, provide the Commission with a sworn statement that it has complied with this provision of  
16 the Order, which statement shall include the names, physical addresses, and e-mail addresses of  
17 each such person or entity who received a copy of the Order.

18 **SERVICE OF ORDER**

19 **XIII.**

20 **IT IS FURTHER ORDERED** that copies of this Order may be served by any means  
21 authorized by law, including facsimile transmission, upon any financial institution or other entity  
22 or person that may have possession, custody, or control of any documents of the Defendant, or that  
23 may otherwise be subject to any provision of this Order.

24 **DURATION OF TEMPORARY RESTRAINING ORDER**

25 **XIV.**

26 **IT IS FURTHER ORDERED** that the Temporary Restraining Order granted herein shall  
27 expire on June 15, 2009 at 9:00 a.m., unless within such time, the Order, for good cause shown, is

28 TRO and  
Order to Show Cause

1 extended for an additional period not to exceed ten (10) days, or unless it is further extended  
2 pursuant to Federal Rule of Civil Procedure 65.

3 **ORDER TO SHOW CAUSE REGARDING**  
4 **PRELIMINARY INJUNCTION**  
5 **XV.**

6 **IT IS FURTHER ORDERED**, pursuant to Federal Rule of Civil Procedure 65(b) that the  
7 Defendant shall appear before this Court on the 15th day of June, 2009, at 9:00 a.m., to show  
8 cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling  
9 on the Complaint against the Defendant, enjoining it from the conduct temporarily restrained by  
10 the preceding provisions of this order.

11 **SERVICE OF PLEADINGS, MEMORANDA, AND OTHER EVIDENCE**

12 **XVI.**

13 **IT IS FURTHER ORDERED** that the Defendant shall file with the Court and serve on  
14 the Commission's counsel any answering affidavits, pleadings, motions, expert reports or  
15 declarations, and/or legal memoranda no later than four (4) days prior to the hearing on the  
16 Commission's request for a preliminary injunction. The Commission may file responsive or  
17 supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on  
18 counsel for the Defendant no later than one (1) day prior to the preliminary injunction hearing in  
19 this matter. Provided that service shall be performed by personal or overnight delivery, facsimile  
20 or electronic mail, and documents shall be delivered so that they shall be received by the other  
21 parties no later than 4:00 p.m. (Pacific Daylight Time) on the appropriate dates listed in this  
22 Paragraph.

23 **MOTION FOR LIVE TESTIMONY; WITNESS IDENTIFICATION**

24 **XVII.**

25 **IT IS FURTHER ORDERED** that the question of whether this Court should enter a  
26 preliminary injunction pursuant to Rule 65 of the Federal Rules of Civil Procedure enjoining the  
27 Defendant during the pendency of this action shall be resolved on the pleadings, declarations,  
28 exhibits, and memoranda filed by, and oral argument of, the parties. Live testimony shall be heard



only on further order of this Court or on motion filed with the Court and served on counsel for the other parties at least three (3) days prior to the preliminary injunction hearing in this matter. Such motion shall set forth the name, address, and telephone number of each proposed witness, a detailed summary or affidavit revealing the substance of each proposed witness's expected testimony, and an explanation of why the taking of live testimony would be helpful to this Court. Any papers opposing a timely motion to present live testimony or to present live testimony in response to another party's timely motion to present live testimony shall be filed with this Court and served on the other parties at least two (2) days 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 Daylight Time) on the appropriate dates provided in this Paragraph.

#### SERVICE UPON THE COMMISSION

#### XVIII.

**IT IS FURTHER ORDERED** that, with regard to any correspondence or pleadings related to this Order, service on the Commission shall be performed by overnight mail delivery to the attention of Ethan Arenson at the Federal Trade Commission, 600 Pennsylvania Avenue, NW, Room H-286, Washington, DC 20580.

//

//

//

TRO and  
Order to Show Cause



**RETENTION OF JURISDICTION**

**XIX.**

**IT IS FURTHER ORDERED** that this Court shall retain jurisdiction of this matter for all purposes. No security is required of any agency of the United States for the issuance of a restraining order. Fed. R. Civ. P. 65(c).

**SO ORDERED**, this Second day of June, 2009, at 4:10 p.m.

  
UNITED STATES DISTRICT JUDGE

## ATTACHMENT A

**FEDERAL TRADE COMMISSION**

**FINANCIAL STATEMENT OF CORPORATE DEFENDANT**

---

**Instructions:**

1. Complete all items. Enter "None" or "N/A" ("Not Applicable") where appropriate. If you cannot fully answer a question, explain why.
2. In completing this financial statement, "the corporation" refers not only to this corporation but also to each of its predecessors that are not named defendants in this action.
3. When an Item asks for information about assets or liabilities "held by the corporation," include ALL such assets and liabilities, located within the United States or elsewhere, held by the corporation or held by others for the benefit of the corporation.
4. Attach continuation pages as needed. On the financial statement, state next to the Item number that the Item is being continued. On the continuation page(s), identify the Item number being continued.
5. Type or print legibly.
6. An officer of the corporation must sign and date the completed financial statement on the last page and initial each page in the space provided in the lower right corner.

**Penalty for False Information:**

Federal law provides that any person may be imprisoned for not more than five years, fined, or both, if such person:

- (1) "in any matter within the jurisdiction of any department or agency of the United States knowingly and willfully falsifies, conceals or covers up by any trick, scheme, or device a material fact, or makes any false, fictitious or fraudulent statements or representations, or makes or uses any false writing or document knowing the same to contain any false, fictitious or fraudulent statement or entry" (18 U.S.C. § 1001);
- (2) "in any . . . statement under penalty of perjury as permitted under section 1746 of title 28, United States Code, willfully subscribes as true any material matter which he does not believe to be true" (18 U.S.C. § 1621); or
- (3) "in any (. . . statement under penalty of perjury as permitted under section 1746 of title 28, United States Code) in any proceeding before or ancillary to any court or grand jury of the United States knowingly makes any false material declaration or makes or uses any other information . . . knowing the same to contain any false material declaration." (18 U.S.C. § 1623)

For a felony conviction under the provisions cited above, federal law provides that the fine may be not more than the greater of (i) \$250,000 for an individual or \$500,000 for a corporation, or (ii) if the felony results in pecuniary gain to any person or pecuniary loss to any person other than the defendant, the greater of twice the gross gain or twice the gross loss. 18 U.S.C. § 3571.

---

**BACKGROUND INFORMATION****Item 1. General Information**

Corporation's Full Name \_\_\_\_\_

Primary Business Address \_\_\_\_\_ From (Date) \_\_\_\_\_

Telephone No. \_\_\_\_\_ Fax No. \_\_\_\_\_

E-Mail Address \_\_\_\_\_ Internet Home Page \_\_\_\_\_

All other current addresses &amp; previous addresses for past five years, including post office boxes and mail drops:

Address \_\_\_\_\_ From/Until \_\_\_\_\_

Address \_\_\_\_\_ From/Until \_\_\_\_\_

Address \_\_\_\_\_ From/Until \_\_\_\_\_

All predecessor companies for past five years:

Name &amp; Address \_\_\_\_\_ From/Until \_\_\_\_\_

Name &amp; Address \_\_\_\_\_ From/Until \_\_\_\_\_

Name &amp; Address \_\_\_\_\_ From/Until \_\_\_\_\_

**Item 2. Legal Information**

Federal Taxpayer ID No. \_\_\_\_\_ State &amp; Date of Incorporation \_\_\_\_\_

State Tax ID No. \_\_\_\_\_ State \_\_\_\_\_ Profit or Not For Profit \_\_\_\_\_

Corporation's Present Status: Active \_\_\_\_\_ Inactive \_\_\_\_\_ Dissolved \_\_\_\_\_

If Dissolved: Date dissolved \_\_\_\_\_ By Whom \_\_\_\_\_

Reasons \_\_\_\_\_

Fiscal Year-End (Mo./Day) \_\_\_\_\_ Corporation's Business Activities \_\_\_\_\_

**Item 3. Registered Agent**

Name of Registered Agent \_\_\_\_\_

Address \_\_\_\_\_ Telephone No. \_\_\_\_\_



**Item 4. Principal Stockholders**

List all persons and entities that own at least 5% of the corporation's stock.

<u>Name &amp; Address</u>	<u>% Owned</u>

**Item 5. Board Members**

List all members of the corporation's Board of Directors.

<u>Name &amp; Address</u>	<u>% Owned</u>	<u>Term (From/Until)</u>

**Item 6. Officers**

List all of the corporation's officers, including *de facto* officers (individuals with significant management responsibility whose titles do not reflect the nature of their positions).

<u>Name &amp; Address</u>	<u>% Owned</u>

**Item 7. Attorneys**

List all attorneys retained by the corporation during the last three years.

<u>Name</u>	<u>Firm Name</u>	<u>Address</u>

I am submitting this financial statement with the understanding that it may affect action by the Federal Trade Commission or a federal court. I have used my best efforts to obtain the information requested in this statement. The responses I have provided to the items above are true and contain all the requested facts and information of which I have notice or knowledge. I have provided all requested documents in my custody, possession, or control. I know of the penalties for false statements under 18 U.S.C. § 1001, 18 U.S.C. § 1621, and 18 U.S.C. § 1623 (five years imprisonment and/or fines). I certify under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Executed on:

\_\_\_\_\_  
(Date)

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Corporate Position



1 DAVID SHONKA  
Acting General Counsel

2 Ethan Arenson, DC # 473296  
3 Carl Settlemeyer, DC # 454272  
Philip Tumminio, DC # 985624  
4 Federal Trade Commission  
600 Pennsylvania Avenue, N.W.  
5 Washington, DC 20580  
(202) 326-2204 (Arenson)  
6 (202) 326-2019 (Settlemeyer)  
(202) 326-2204 (Tumminio)  
7 (202) 326-3395 *facsimile*  
earenson@ftc.gov  
8 csettlemeyer@ftc.gov  
ptumminio@ftc.gov  
9

E-Filed on 6/15/09

Attorneys for Plaintiff Federal Trade Commission

10  
11 **UNITED STATES DISTRICT COURT**  
12 **NORTHERN DISTRICT OF CALIFORNIA**  
13 **San Jose Division**

14 **Federal Trade Commission,**

15 **Plaintiff,**

16 **v.**

17 **Pricewert LLC d/b/a 3FN.net, Triple Fiber**  
18 **Network, APS Telecom and APX Telecom,**  
**APS Communications, and APS**  
**Communication,**

19 **Defendant.**  
20

**Case No. C-09-2407 RMW**

**PRELIMINARY INJUNCTION**

21 Plaintiff, the Federal Trade Commission ("FTC" or "Commission"), pursuant to Section  
22 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b), has filed a  
23 Complaint for Injunctive and Other Equitable Relief, and moved *ex parte* for a temporary  
24 restraining order and for an order to show cause why a preliminary injunction should not be  
25 granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure. On June 2, 2009, this  
26 Court granted the Commission's motion and entered a Temporary Restraining Order and Order to  
27 Show Cause against Defendant Pricewert LLC also d/b/a 3FN.net, Triple Fiber Network, APS  
28 Telecom and APX Telecom, APS Communications, and APS Communication (D.E. 12). On  
June 5, 2009 the court directed the FTC to submit a proposal for expeditiously addressing the



1 concerns of innocent third parties who claimed to be suffering harm as a result of the Temporary  
2 Restraining Order. This request was prompted by written communication to the court by two non-  
3 parties. The hearing on the Order to show Cause as to why a preliminary injunction should not  
4 issue was held on June 15, 2009. The FTC appeared through its counsel Ethan Arenson and  
5 Philip Tumminio. Karl S. Kronenberger of Kronenberger Burgoyne, LLP appeared on behalf of  
6 third parties Suren Ter-Saakov and Tsuren LLC. Although the court had received communication  
7 from Max Christopher who was identified as "Defendant's authorized representative and  
8 interpreter" indicating that counsel for defendant or a representative would appear, no one  
9 appeared on behalf of defendant. After reviewing the papers and hearing the comments of  
10 counsel, the Court makes the following findings and orders.

### 11 12 **FINDINGS**

13 The court has considered the pleadings, declarations, exhibits, and memoranda filed in  
14 support of the Commission's motion for a preliminary injunction and finds that:

- 15 1. This court has jurisdiction over the subject matter of this case and there is good  
16 cause to believe that it will have jurisdiction over all parties hereto; the Complaint  
17 states a claim upon which relief may be granted against the Defendant under  
18 Section 5(a) of the FTC Act, 15 U.S.C. § 45(a) (2006).
- 19 2. There is good cause to believe that Pricewert LLC also d/b/a 3FN.net, Triple Fiber  
20 Network, APS Telecom and APX Telecom, APS Communications, and APS  
21 Communication (the "Defendant"), has engaged in and is likely to engage in acts or  
22 practices that violate Section 5(a) of the FTC Act, 15 U.S.C. § 45(a) (2006), and  
23 that the Commission is, therefore, likely to prevail on the merits of this action;
- 24 3. There is good cause to believe that immediate and irreparable harm will result from  
25 the Defendant's ongoing violations of Section 5(a) of the FTC Act unless the  
26 Defendant is restrained and enjoined by Order of this court. The evidence set forth  
27 in the Commission's Memorandum of Law in Support of *Ex Parte* Motion for  
28 Temporary Restraining Order and Order to Show Cause ("TRO Motion"), and the

1 accompanying declarations and exhibits, demonstrates that the Commission is  
2 likely to prevail on its claim that Defendant has engaged in unfair acts or practices  
3 in violation of Section 5(a) of the FTC Act by: recruiting, distributing and hosting  
4 electronic code or content that inflicts harm upon consumers, including, but not  
5 limited to, child pornography, botnet command and control servers, spyware,  
6 viruses, trojans, and phishing-related sites; and configuring, deploying, and  
7 operating botnets. There is good cause to believe that the Defendant will continue  
8 to engage in such unlawful actions if not immediately restrained from doing so by  
9 Order of this court;

10 4. There is good cause to believe that immediate and irreparable damage to this  
11 court's ability to grant effective final relief will result from the sale, transfer, or  
12 other disposition or concealment by the Defendant of its assets, business records,  
13 or other discoverable evidence. Based on the evidence cited in the Commission's  
14 TRO Motion and accompanying declarations and exhibits, the Commission is  
15 likely to be able to prove that: (1) the Defendant has operated through a series of  
16 maildrops and shell companies, with a principal place of business and its principals  
17 located outside of the United States; (2) the Defendant has continued its unlawful  
18 operations unabated despite requests from the Internet security community to cease  
19 its injurious activities; and (3) the Defendant is engaged in activities that directly  
20 violate U.S. law and cause significant harm to consumers;

21 5. There is good cause to believe that the Defendant, which is controlled by  
22 individuals outside of the United States, has engaged in illegal activity using Data  
23 Centers and Upstream Service Providers based in the United States and that to  
24 immediately halt the injury caused by Defendant, such Data Centers and Upstream  
25 Service Providers must be ordered to immediately disconnect or to maintain  
26 disconnection of Defendant's computing resources from the Internet, prevent the  
27 Defendant and others from accessing such computer resources, and prevent the  
28 destruction of data located on these computer resources;

6. Weighing the equities and considering the Plaintiff's likelihood of ultimate success, this Order is in the public interest; and
7. Fed. R. Civ. P. 65(c) does not require security of the United States or an officer or agency thereof for the issuance of a preliminary injunction.

#### DEFINITIONS

For the purpose of this order, the following definitions shall apply:

1. **"Assets"** means any legal or equitable interest in, right to, or claim to, any real, personal, or intellectual property of Defendant or held for the benefit of Defendant wherever located, including, but not limited to, chattel, goods, instruments, equipment, fixtures, general intangibles, effects, leaseholds, contracts, mail or other deliveries, shares of stock, inventory, checks, notes, accounts, credits, receivables (as those terms are defined in the Uniform Commercial Code), cash, and trusts, including but not limited to any other trust held for the benefit of Defendant.
2. **"Botnet"** means a network of computers that have been compromised by malicious code and surreptitiously programmed to follow instructions issued by a Botnet Command and Control Server.
3. **"Botnet Command and Control Server"** means a computer or computers used to issue instructions to, or otherwise control, a Botnet.
4. The term **"Child Pornography"** shall have the same meaning as provided in 18 U.S.C. § 2256.
5. **"Data Center"** means any person or entity that contracts with third parties to house computer servers and associated equipment, and provides the infrastructure to support such equipment, such as power or environmental controls.
6. **"Day"** shall have the meaning prescribed by and time periods in this Order shall be calculated pursuant to Fed. R. Civ. P. 6(a).



- 1       7.     **"Defendant"** means Pricewert LLC also d/b/a 3FN.net, Triple Fiber Network,  
2       APS Telecom, APX Telecom, APS Communications, APS Communication, and  
3       any other names under which it does business, and any subsidiaries, corporations,  
4       partnerships, or other entities directly or indirectly owned, managed, or controlled  
5       by Pricewert LLC.
- 6       8.     **"Document"** is synonymous in meaning and equal in scope to the usage of  
7       the term in the Federal Rules of Civil Procedure 34(a), and includes  
8       writing, drawings, graphs, charts, Internet sites, Web pages, Web sites,  
9       electronic correspondence, including e-mail and instant messages,  
10      photographs, audio and video recordings, contracts, accounting data,  
11      advertisements (including, but not limited to, advertisements placed on the  
12      World Wide Web), FTP Logs, Server Access Logs, USENET Newsgroup  
13      postings, World Wide Web pages, books, written or printed records,  
14      handwritten notes, telephone logs, telephone scripts, receipt books, ledgers,  
15      personal and business canceled checks and check registers, bank  
16      statements, appointment books, computer records, and other data  
17      compilations from which information can be obtained and translated. A  
18      draft or non-identical copy is a separate document within the meaning of  
19      the term.
- 20      9.     **"Phishing"** means the use of email, Internet web sites, or other means to mimic or  
21      copy the appearance of a trustworthy entity for the purpose of duping consumers  
22      into disclosing personal information, such as account numbers and passwords.
- 23      10.    **"Representatives"** means the following persons or entities who receive actual  
24      notice of this preliminary injunction by personal service or otherwise: (1) the  
25      Defendant's officers, agents, servants, employees, and attorneys; and (2) all other  
26      persons who are in active concert or participation with Defendant or its officers,  
27      agents, servants, employees, or attorneys. A Data Center or Upstream Service  
28      Provider that continues to provide services to Defendant after receiving actual



notice of this preliminary injunction is a Representative.

11. "Spyware" means any type of software that is surreptitiously installed on a computer and, without the consent of the user, could collect information from a computer, could allow third parties to control remotely the use of a computer, or could facilitate botnet communications.
12. "Trojan Horse" means a computer program with an apparent or actual useful function that contains additional, undisclosed malicious code, including but not limited to spyware, viruses, or code that facilitates the surreptitious download or installation of other software code.
13. "Upstream Service Provider" means any entity that provides the means to connect to the Internet, including, but not limited to, the subleasing of Internet Protocol addresses.
14. "Viruses" means computer programs designed to spread from one computer to another and to interfere with the operation of the computers they infect.

## PROHIBITED BUSINESS ACTIVITIES

### I.

**IT IS THEREFORE ORDERED** that, Defendant and its Representatives are preliminarily restrained and enjoined from recruiting or willingly distributing or hosting Child Pornography, Botnet Command and Control Servers, Spyware, Viruses, Trojan Horses, Phishing-related sites, or similar electronic code or content that inflicts harm upon consumers.

### II.

**IT IS FURTHER ORDERED** that Defendant and its Representatives are preliminarily restrained and enjoined from configuring, deploying, operating, or otherwise participating in or otherwise willingly facilitating, any Botnet.

**SUSPENSION OF INTERNET CONNECTIVITY**

**III.**

**IT IS FURTHER ORDERED** that, pending resolution of the merits of this case, that:

A. Any Data Center in active concert or participation with and providing services to Defendant or Defendant's officers, agents, servants, or employees shall, if it has not already done so in compliance with the Temporary Restraining Order previously issued in this case, immediately and without prior notification to Defendant or Defendant's officers, agents, servants, or employees, take all reasonable and necessary steps to make inaccessible to the Defendant and all other persons, except as otherwise ordered herein, all computers, servers or electronic data storage devices or media and the content stored thereupon (hereafter "computer resources"), leased, owned or operated by Defendant or Defendant's officers agents, servants, or employees and located on premises owned by, or within the control of, the Data Center and shall, if it has already taken such steps in compliance with the Temporary Restraining Order previously issued in this case, continue to make those computer resources inaccessible to the Defendant and all other persons, except as otherwise ordered herein. Such steps shall, at a minimum, include:

1. disconnecting such computer resources from the Internet and all other networks;
2. securing the area where such computer resources are located in a manner reasonably calculated to deny access to the Defendant and its officers, agents, servants, or employees; and
3. if such Data Center restricts access to its facilities by means of access credentials, suspending all access credentials issued to Defendant or Defendant's officers, agents, servants, or employees;

B. Any Upstream Service Provider in active concert or participation with and providing services to Defendant or Defendant's officers, agents, servants, or employees shall, if it has not already done so in compliance with the Temporary Restraining Order previously issued in this case, immediately, and without notifying Defendant or Defendant's officers, agents, servants, or employees in advance, take all reasonable and necessary steps to deny Internet connectivity to the Defendant and Defendant's officers, agents, servants, and employees, including, but not limited

1 to, suspending any IP addresses assigned to the Defendant or Defendant's officers, agents, servants,  
2 or employees by the Upstream Service Provider, and refraining from reassigning such IP addresses,  
3 and shall, if it has already taken such steps in compliance with the Temporary Restraining Order  
4 previously issued in this case, continue to deny Internet connectivity to the Defendant and  
5 Defendant's officers, agents, servants, and employees;

6 C. Any Data Center or Upstream Service Provider described in subparagraphs A and B  
7 above providing services to Defendant or Defendant's officers, agents, servants, or employees,  
8 shall preserve and retain documents relating to the Defendant or the Defendant's officers, agents,  
9 servants, or employees; and

10 D. Agents of the Commission and other law enforcement agencies are permitted to  
11 enter the premises of any of Defendant's Data Centers and Upstream Service Providers described  
12 in subparagraph A and B above to serve copies of this Order and to verify that the Data Centers  
13 and Upstream Service Providers have taken the reasonable and necessary steps described in sub-  
14 paragraphs A and B of this Paragraph.

15 *Provided, however,* nothing in Paragraph III shall be interpreted to deny access to any law  
16 enforcement agency granted access pursuant to a court order, search warrant, or other lawful  
17 process, or to deny access to any receiver appointed by this court.

18  
19 **ASSET FREEZE**

20 **IV.**

21 **IT IS FURTHER ORDERED** that the Defendant and its Representatives are hereby  
22 preliminarily restrained and enjoined from:

23 A. Transferring, liquidating, converting, encumbering, pledging, loaning, selling,  
24 concealing, dissipating, disbursing, assigning, spending, withdrawing, granting a lien or security  
25 interest or other interest in, or otherwise disposing of any funds, real or personal property,  
26 accounts, contracts, consumer lists, shares of stock, or other assets, or any interest therein,  
27 wherever located, that are: (1) owned or controlled by the Defendant, in whole or in part, for the  
28 benefit of the Defendant; (2) in the actual or constructive possession of the Defendant; or (3)



1 owned, controlled by, or in the actual or constructive possession of any corporation, partnership, or  
2 other entity directly or indirectly owned, managed, or controlled by the Defendant, including, but  
3 not limited to, any assets held by or for, or subject to access by, the Defendant, at any bank or  
4 savings and loan institution, or with any broker-dealer, escrow agent, title company, commodity  
5 trading company, precious metals dealer, or other financial institution or depository of any kind;  
6 and

7 B. Opening or causing to be opened any safe deposit boxes titled in the name of the  
8 Defendant, or subject to access by the Defendant.

9 *Provided, however,* that the assets affected by Paragraph IV shall include: (1) all of the  
10 assets of the Defendant existing as of the date this Order was entered; and (2) for assets obtained  
11 after the date this Order was entered, only those assets of the Defendant that are derived from  
12 conduct prohibited in Paragraphs I and II of this Order.

#### 13 14 **FINANCIAL REPORTS AND ACCOUNTING**

##### 15 **V.**

16 **IT IS FURTHER ORDERED** that the Defendant, if it has not already done so in  
17 compliance with the Temporary Restraining Order previously issued in this case, shall within five  
18 (5) business days of receiving notice of this Order provide the Commission with completed  
19 financial statements, verified under oath and accurate as of the date of entry of this Order, on the  
20 forms attached to this Order as **Attachment A**.

#### 21 22 **RETENTION OF ASSETS AND PRODUCTION OF RECORDS** 23 **BY FINANCIAL INSTITUTIONS**

##### 24 **VI.**

25 **IT IS FURTHER ORDERED** that, any financial or brokerage institution, business entity,  
26 or person served with a copy of this Order that holds, controls, or maintains custody of any account  
27 or asset of the Defendant, or has held, controlled or maintained custody of any such account or  
28 asset at any time prior to the date of entry of this Order, shall:



1 A. Hold and retain within its control and prohibit the withdrawal, removal, assignment,  
2 transfer, pledge, encumbrance, disbursement, dissipation, conversion, sale, or other disposal of any  
3 such asset except by further order of the court; and

4 B. Deny all persons access to any safe deposit box that is:

- 5 1. titled in the name of the Defendant; or
- 6 2. otherwise subject to access by Defendant.

7  
8 **FOREIGN ASSET REPATRIATION AND ACCOUNTING**

9 **VII.**

10 **IT IS FURTHER ORDERED that:**

11 A. Defendant and its Representatives shall, if it has not already done so in compliance  
12 with the Temporary Restraining Order previously issued in this case, immediately upon service of  
13 this Order, or as soon as relevant banking hours permit, transfer to the territory of the United States  
14 to a blocked account whose funds cannot be withdrawn without further order of the court all funds  
15 and assets in foreign countries held: (1) by Defendant; (2) for its benefit; or (3) under its direct or  
16 indirect control, jointly or singly; and

17 B. Defendant shall, if it has not already done so in compliance with the Temporary  
18 Restraining Order previously issued in this case, within five (5) business days of receiving notice  
19 of this Order provide the Commission with a full accounting, verified under oath and accurate as of  
20 the date of this Order, of all funds, documents, and assets outside of the United States which are:  
21 (1) titled in the Defendant's name; or (2) held by any person or entity for the benefit of the  
22 Defendant; or (3) under the direct or indirect control, whether jointly or singly, of the Defendant;  
23 and

24 C. Defendant and its Representatives are preliminarily restrained and enjoined from  
25 taking any action, directly or indirectly, which may result in the encumbrance or dissipation of  
26 foreign assets, including but not limited to:

- 27 1. Sending any statement, letter, fax, e-mail or wire transmission, telephoning or  
28 engaging in any other act, directly or indirectly, that results in a determination by a

1 foreign trustee or other entity that a "duress" event has occurred under the terms of a  
2 foreign trust agreement; or

- 3 2. Notifying any trustee, protector or other agent of any foreign trust or other related  
4 entities of the existence of this Order, or that an asset freeze is required pursuant to  
5 a court Order, until such time that a full accounting has been provided pursuant to  
6 this Paragraph.

7  
8 **ACCESS TO BUSINESS RECORDS**

9 **VIII.**

10 **IT IS FURTHER ORDERED** that the Defendant, if it has not already done so in  
11 compliance with the Temporary Restraining Order previously issued in this case, shall allow the  
12 Commission's representatives, agents, and assistants access to the Defendant's business records to  
13 inspect and copy documents. Accordingly, the Defendant shall, within forty-eight (48) hours of  
14 receiving notice of this Order, produce to the Commission and the Commission's representatives,  
15 agents, and assistants for inspection, inventory, and/or copying, at Federal Trade Commission, 600  
16 Pennsylvania Avenue NW, Room H-286, Washington DC 20580, Attention: Ethan Arenson, the  
17 following materials: (1) all client information, including, but not limited to, names, phone  
18 numbers, addresses, email addresses, and payment information for all clients of Defendant's  
19 services; (2) contracts; (3) correspondence, including, but not limited to, electronic correspondence  
20 and Instant Messenger communications, that refer or relate to the Defendant's services; and (4)  
21 accounting information, including, but not limited to, profit and loss statements, annual reports,  
22 receipt books, ledgers, personal and business canceled checks and check registers, bank statements,  
23 and appointment books.

24 *Provided, however,* this Paragraph excludes any record or other information pertaining to a  
25 subscriber or customer of an electronic communications service or a remote computing service as  
26 those terms are defined in the Electronic Communications Privacy Act, 18 U.S.C. § 2703(c)  
27 (2006).

1 The Commission shall return produced materials pursuant to this Paragraph within five (5)  
2 days of completing said inventory and copying.

3  
4 **COMMENCEMENT OF DISCOVERY**

5 **IX.**

6 **IT IS FURTHER ORDERED** that pursuant to Federal Rules of Civil Procedure 30(a),  
7 31(a), 34, and 45, and notwithstanding the provisions of Federal Rules of Civil Procedure 26(d)  
8 and (f), 30(a)(2)(A)-(C), and 31(a)(2)(A)-(C), the Commission is granted leave, at any time after  
9 entry of this Order, to commence discovery.

10  
11 **PRESERVATION OF RECORDS**

12 **X.**

13 **IT IS FURTHER ORDERED** that the Defendant and its Representatives are hereby  
14 preliminarily restrained and enjoined from destroying, erasing, mutilating, concealing, altering,  
15 transferring, writing over, or otherwise disposing of, in any manner, directly or indirectly, any  
16 documents or records of any kind that relate to the business practices or business finances of the  
17 Defendant, including but not limited to, computerized files and storage media on which  
18 information has been saved (including, but not limited to, hard drives, DVDs, CD-ROMS, zip  
19 disks, floppy disks, punch cards, magnetic tape, backup tapes, and computer chips), and any and all  
20 equipment needed to read any such documents or records, FTP logs, Service Access Logs,  
21 USENET Newsgroup postings, World Wide Web pages, books, written or printed records,  
22 handwritten notes, telephone logs, telephone scripts, receipt books, ledgers, personal and business  
23 canceled checks and check registers, bank statements, appointment books, and other documents or  
24 records of any kind that relate to the business practices or finances of the Defendant or its officers,  
25 agents, servants, or employees.

**RECORD KEEPING/BUSINESS OPERATIONS****XI.**

**IT IS FURTHER ORDERED** that the Defendant is hereby preliminarily restrained and enjoined from:

- A. Failing to maintain documents that, in reasonable detail, accurately, fairly, and completely reflect its income, disbursements, transactions, and use of money; and
- B. Creating, operating, or exercising any control over any business entity, including any partnership, limited partnership, joint venture, sole proprietorship, or corporation, without first providing the Commission with a written statement disclosing: (1) the name of the business entity; (2) the address and telephone number of the business entity; (3) the names of the business entity's officers, directors, principals, managers and employees; and (4) a detailed description of the business entity's intended activities.

**DISTRIBUTION OF ORDER BY DEFENDANT****XII.**

**IT IS FURTHER ORDERED** that the Defendant shall immediately provide a copy of this Order to each of its subsidiaries, Upstream Service Providers, Data Centers, divisions, sales entities, successors, assigns, officers, directors, employees, independent contractors, client companies, agents, and attorneys, and shall, within ten (10) calendar days from the date of entry of this Order, provide the Commission with a sworn statement that it has complied with this provision of the Order, which statement shall include the names, physical addresses, and e-mail addresses of each such person or entity who received a copy of the Order.

**SERVICE OF ORDER****XIII.**

**IT IS FURTHER ORDERED** that copies of this Order may be served by any means authorized by law, including facsimile transmission, upon any financial institution or other entity or person that may have possession, custody, or control of any documents of the Defendant, or that



1 may otherwise be subject to any provision of this Order.

2  
3 **SERVICE UPON THE COMMISSION**

4 **XIV.**

5 **IT IS FURTHER ORDERED** that, with regard to any correspondence or pleadings related  
6 to this Order, service on the Commission shall be performed by overnight mail delivery to the  
7 attention of Ethan Arenson at the Federal Trade Commission, 600 Pennsylvania Avenue, NW,  
8 Room H-286, Washington, DC 20580.

9  
10 **MODIFICATION OF ORDER**

11 **XV.**

12 The court has concerns about the potential hardship this Order may impose on the  
13 defendant and others, arising from information provided by the defendant and a few third-parties  
14 who have communicated with the court. By Order made contemporaneously with this Order, the  
15 court has appointed a receiver to expeditiously deal with any claim by a third party that it has  
16 suffered harm as a result of the restraining order or will suffer harm as a result of this Preliminary  
17 Injunction. The court has also noted in the submission by Max Christopher, defendant's purported  
18 representative, that defendant "is not going to hide or not appear in court," that "defendant always  
19 has been willing to cooperate with authorities and is ready to assist the investigation" and is "ready  
20 to cooperate and provide any information [it has] on its servers." Further, the submission by Mr.  
21 Christopher notes that the asset freeze has limited defendant's opportunities to obtain legal  
22 representation and defend and respond. Therefore, **IT IS FURTHER ORDERED** that defendant  
23 may, on 48 hours' notice to parties who have appeared, seek modification of this Order including  
24 immediate release of funds necessary to pay for legal representation on behalf of defendant.

25  
26 **RETENTION OF JURISDICTION**

27 **XIV.**

28 **IT IS FURTHER ORDERED** that this court shall retain jurisdiction of this matter for all

1 purposes. No security is required of any agency of the United States for the issuance of a  
2 preliminary injunction. Fed. R. Civ. P. 65(c).

3 **SO ORDERED**, this 15th day of June, 2009.

4  
5 

6  
7 RONALD M. WHYTE  
United States District Judge  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1 Notice of this document has been electronically sent to:

2 Counsel for Plaintiff:

3 Ethan Arenson earenson@ftc.gov  
4 Carl Settlemyer csettlemyer@ftc.gov  
Philip Tumminio ptumminio@ftc.gov

6 Counsel for Defendants:

7 (no appearance)

8 Counsel for Proposed Intervenors:

9 Karl Stephen Kronenberger karl@KBInternetlaw.com  
10 Jeffrey Michael Rosenfeld Jeff@KBInternetlaw.com

12 Counsel are responsible for distributing copies of this document to co-counsel that have not  
13 registered for e-filing under the court's CM/ECF program.

16 Dated: 6/15/09

17 TER  
Chambers of Judge Whyte

## ATTACHMENT A



**FEDERAL TRADE COMMISSION**  
**FINANCIAL STATEMENT OF CORPORATE DEFENDANT**

---

**Instructions:**

1. Complete all items. Enter "None" or "N/A" ("Not Applicable") where appropriate. If you cannot fully answer a question, explain why.
2. In completing this financial statement, "the corporation" refers not only to this corporation but also to each of its predecessors that are not named defendants in this action.
3. When an Item asks for information about assets or liabilities "held by the corporation," include ALL such assets and liabilities, located within the United States or elsewhere, held by the corporation or held by others for the benefit of the corporation.
4. Attach continuation pages as needed. On the financial statement, state next to the Item number that the Item is being continued. On the continuation page(s), identify the Item number being continued.
5. Type or print legibly.
6. An officer of the corporation must sign and date the completed financial statement on the last page and initial each page in the space provided in the lower right corner.

**Penalty for False Information:**

Federal law provides that any person may be imprisoned for not more than five years, fined, or both, if such person:

- (1) "in any matter within the jurisdiction of any department or agency of the United States knowingly and willfully falsifies, conceals or covers up by any trick, scheme, or device a material fact, or makes any false, fictitious or fraudulent statements or representations, or makes or uses any false writing or document knowing the same to contain any false, fictitious or fraudulent statement or entry" (18 U.S.C. § 1001);
- (2) "in any . . . statement under penalty of perjury as permitted under section 1746 of title 28, United States Code, willfully subscribes as true any material matter which he does not believe to be true" (18 U.S.C. § 1621); or
- (3) "in any ( . . . statement under penalty of perjury as permitted under section 1746 of title 28, United States Code) in any proceeding before or ancillary to any court or grand jury of the United States knowingly makes any false material declaration or makes or uses any other information . . . knowing the same to contain any false material declaration." (18 U.S.C. § 1623).

For a felony conviction under the provisions cited above, federal law provides that the fine may be not more than the greater of (i) \$250,000 for an individual or \$500,000 for a corporation, or (ii) if the felony results in pecuniary gain to any person or pecuniary loss to any person other than the defendant, the greater of twice the gross gain or twice the gross loss. 18 U.S.C. § 3571.

---

**BACKGROUND INFORMATION**

**Item 1. General Information**

Corporation's Full Name \_\_\_\_\_

Primary Business Address \_\_\_\_\_ From (Date) \_\_\_\_\_

Telephone No. \_\_\_\_\_ Fax No. \_\_\_\_\_

E-Mail Address \_\_\_\_\_ Internet Home Page \_\_\_\_\_

All other current addresses & previous addresses for past five years, including post office boxes and mail drops:

Address \_\_\_\_\_ From/Until \_\_\_\_\_

Address \_\_\_\_\_ From/Until \_\_\_\_\_

Address \_\_\_\_\_ From/Until \_\_\_\_\_

All predecessor companies for past five years:

Name & Address \_\_\_\_\_ From/Until \_\_\_\_\_

Name & Address \_\_\_\_\_ From/Until \_\_\_\_\_

Name & Address \_\_\_\_\_ From/Until \_\_\_\_\_

**Item 2. Legal Information**

Federal Taxpayer ID No. \_\_\_\_\_ State & Date of Incorporation \_\_\_\_\_

State Tax ID No. \_\_\_\_\_ State \_\_\_\_\_ Profit or Not For Profit \_\_\_\_\_

Corporation's Present Status: Active \_\_\_\_\_ Inactive \_\_\_\_\_ Dissolved \_\_\_\_\_

If Dissolved: Date dissolved \_\_\_\_\_ By Whom \_\_\_\_\_

Reasons \_\_\_\_\_

Fiscal Year-End (Mo./Day) \_\_\_\_\_ Corporation's Business Activities \_\_\_\_\_

**Item 3. Registered Agent**

Name of Registered Agent \_\_\_\_\_

Address \_\_\_\_\_ Telephone No. \_\_\_\_\_

**Item 4. Principal Stockholders**

List all persons and entities that own at least 5% of the corporation's stock.

<u>Name &amp; Address</u>	<u>% Owned</u>

**Item 5. Board Members**

List all members of the corporation's Board of Directors.

<u>Name &amp; Address</u>	<u>% Owned</u>	<u>Term (From/Until)</u>

**Item 6. Officers**

List all of the corporation's officers, including *de facto* officers (individuals with significant management responsibility whose titles do not reflect the nature of their positions).

<u>Name &amp; Address</u>	<u>% Owned</u>

**Item 7. Attorneys**

List all attorneys retained by the corporation during the last three years.

<u>Name</u>	<u>Firm Name</u>	<u>Address</u>

I am submitting this financial statement with the understanding that it may affect action by the Federal Trade Commission or a federal court. I have used my best efforts to obtain the information requested in this statement. The responses I have provided to the items above are true and contain all the requested facts and information of which I have notice or knowledge. I have provided all requested documents in my custody, possession, or control. I know of the penalties for false statements under 18 U.S.C. § 1001, 18 U.S.C. § 1621, and 18 U.S.C. § 1623 (five years imprisonment and/or fines). I certify under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Executed on:

\_\_\_\_\_  
(Date)

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Corporate Position





UNITED STATES DISTRICT COURT  
FOR THE CENTRAL DISTRICT OF CALIFORNIA

February 2005 Grand Jury

11	UNITED STATES OF AMERICA,	)	Case No. CR	DS-1060
12	Plaintiff,	)		
13	v.	)	I N D I C T M E N T	
14	JEANSON JAMES ANCHETA,	)	[18 U.S.C. § 371: Conspiracy;	
15	Defendant.	)	18 U.S.C. §§ 1030(a)(5)(A)(i),	
16		)	(a)(5)(B)(i), and 1030(b): Attempted	
17		)	Transmission of a Code, Information,	
18		)	Program or Command to a Protected	
19		)	Computer; 18 U.S.C. §§ 1030(a)(5)(A)(i)	
20		)	and (a)(5)(B)(v): Transmission of	
21		)	a Code, Information, Program or	
		)	Command to a Protected Computer	
		)	Used By a Government Entity;	
		)	18 U.S.C. § 1030(a)(4): Accessing	
		)	Protected Computers to Conduct Fraud;	
		)	18 U.S.C. § 1956(a)(1)(A)(i):	
		)	Promotional Money Laundering; 21 U.S.C.	
		)	§ 853: Criminal Forfeiture]	

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS

At all times relevant to this indictment:

DEFENDANT JEANSON JAMES ANCHETA

1. Defendant JEANSON JAMES ANCHETA ("ANCHETA") was an individual residing in Los Angeles County, within the Central District of California.

1       2.    ANCHETA possessed at least one computer at his residence,  
2   and accessed the Internet from the telephone line located there.

3       3.    ANCHETA used the following email accounts:  
4   gridin@gmail.com; iamjames85@yahoo.com, jazzsanjoy@peoplepc.com,  
5   resili3nt@gmail.com, resilient24@earthlink.net,  
6   resjames@sbcglobal.net, and resjames@yahoo.com.

7       4.    ANCHETA used the following user name: ir Resilient.

8       5.    ANCHETA used the following nicknames: aa, fortunecookie,  
9   gjrj, Resilient, ResilientT, ServiceMode, and SHK.

10   UNINDICTED CO-CONSPIRATOR IN BOCA RATON, FLORIDA

11       6.    An unindicted co-conspirator residing in Boca Raton,  
12   Florida (hereinafter referred to as "SoBe"), was a computer user  
13   with experience in launching computer attacks, and as set forth  
14   below, was involved in the conspiracy to access protected computers  
15   to commit fraud.

16       7.    SoBe possessed at least one computer at the Florida  
17   residence, and accessed the Internet from a cable line located  
18   there.

19       8.    SoBe used the following email accounts:  
20   r00t3dx@hotmail.com and syzt3m@gmail.com.

21       9.    SoBe used the following user name: Serlissmc.

22       10.   SoBe used the following other nicknames: ebos, shksobe,  
23   syzt3m, and vapidz.

24   INTERNET SERVICE PROVIDERS

25       11.   Many individuals and businesses obtain their access to  
26   the Internet through businesses known as Internet Service Providers  
27   ("ISPs").

28   //

1 12. ISPs offer their customers access to the Internet using  
2 telephone or other telecommunications lines. ISPs provide Internet  
3 e-mail accounts that allow users to communicate with other Internet  
4 users by sending and receiving electronic messages through the  
5 ISPs' servers. ISPs remotely store electronic files on their  
6 customers' behalf, and may provide other services unique to each  
7 particular ISP.

8 America Online

9 13. America Online, Inc. ("AOL") was an ISP headquartered in  
10 Dulles, Virginia.

11 14. In addition to Internet access, Internet e-mail accounts,  
12 and remote storage of electronic files, AOL also offered its  
13 customers a free online service called AOL Instant Messenger  
14 ("AIM"), which allowed users to communicate in real time.

15 INTERNET HOSTING COMPANIES

16 15. Internet hosting companies provide individuals or  
17 businesses with large scale access to the Internet through the use  
18 of computers large enough to be capable of providing one or more  
19 services to other computers on the Internet. These large computers  
20 are commonly referred to as "servers" or "boxes." Use of a server  
21 is often combined with access to a larger network of computers.  
22 The services of Internet hosting companies enable customers to  
23 conduct activity on the Internet, such as operate web sites,  
24 administer networks, or run email systems.

25 EasyDedicated

26 16. EasyDedicated International B.V. was an Internet hosting  
27 company located in Amsterdam, Netherlands.

28 //.



1 17. EasyDedicated provided its customers with large scale  
2 Internet connectivity, access to networks of computers, and the use  
3 of servers and other hardware.

4 18. EasyDedicated provided these services to customers  
5 residing outside of the Netherlands through its online business,  
6 EasyDedicated.com.

7 FDCServers

8 19. FDCServers was an Internet hosting company located in  
9 Chicago, Illinois.

10 20. FDCServers provided its customers with large scale  
11 Internet connectivity, access to networks of computers, and the use  
12 of servers and other hardware.

13 The Planet

14 21. The Planet was an Internet hosting company located in  
15 Dallas, Texas.

16 22. The Planet provided its customers with large scale  
17 Internet connectivity, access to networks of computers, and the use  
18 of servers and other hardware.

19 Sago Networks

20 23. Sago Networks was an Internet hosting company located in  
21 Tampa, Florida.

22 24. Sago Networks provided its customers with large scale  
23 Internet connectivity, access to networks of computers, and the use  
24 of servers and other hardware.

25 ADVERTISING SERVICE COMPANIES

26 25. Online merchants often hire advertising service companies  
27 to send traffic to their web sites. These advertising service  
28 companies in turn maintain advertising affiliate programs, whereby

1 an individual, typically someone who operates a web site, is hired  
2 to place on the website certain links advertising the merchant's  
3 product or business, and is then compensated based upon the number  
4 of visitors to the website that click on that link.

5 26. Some advertising service companies with multiple online  
6 merchant clients compensate their affiliates each time a type of  
7 software known as "adware" is successfully installed on a visitor's  
8 computer. Adware collects information about an Internet user in  
9 order to display advertisements in the user's Web browser based  
10 upon information it collects from the user's browsing patterns.

11 27. Adware is usually installed on an Internet user's  
12 computer only upon notice or if the user performs some action, like  
13 clicking a button, installing a software package, or agreeing to  
14 enhance the functionality of a Web browser by adding a toolbar or  
15 additional search box.

16 28. Advertising service companies typically identify their  
17 affiliates by some type of identification number or code that is  
18 included in the adware; they then tally up the number of installs  
19 and periodically pay the affiliate based upon a percentage of the  
20 number of installs, usually through Paypal, direct bank deposit, or  
21 by check mailed to the affiliate.

22 Gammacash

23 29. Gamma Entertainment, Inc. was an advertising service  
24 company located in Quebec, Canada.

25 30. Gamma Entertainment was associated with the web sites  
26 www.toolbarcash.com, www.gammacash.com, and www.xxxtoolbar.com.  
27 These web sites were advertising service web sites which offered  
28 advertising affiliate programs pertaining to the installation of

1 adware.

2 31. Gamma Entertainment compensated its affiliates for each  
3 installation of adware made with notice to and/or consent from any  
4 Internet user,

5 LOUDcash

6 32. CDT Inc. was an advertising service company located in  
7 Quebec, Canada. CDT was associated with advertising service web  
8 sites called www.loudmarketing.com and www.loudcash.com. Through  
9 these web sites, CDT offered an advertising affiliate program  
10 called "LOUDcash" or "lc."

11 33. LOUDcash compensated its affiliates for each installation  
12 of adware made with notice to and/or consent from any Internet  
13 user.

14 34. In or about April 2005, 180solutions, an advertising  
15 service company located in Bellevue, Washington, acquired CDT, Inc.  
16 As a result, LOUDcash became a subsidiary of a company called Zango  
17 Nevada LLC and was renamed ZangoCash.

18 PAYPAL

19 35. Paypal, Inc. was an online payment solutions company  
20 located in San Jose, California.

21 36. Paypal used a website located at www.paypal.com to enable  
22 any individual or business with an e-mail address to securely,  
23 easily and quickly send and receive payments online. Paypal's  
24 service built on the existing financial infrastructure of bank  
25 accounts and credit cards to create a real time payment solution.

26 CHINA LAKE NAVAL AIR FACILITY

27 37. The Weapons Division of the United States Naval Air  
28 Warfare Center was located in China Lake, California.

1 38. This federal government facility maintained a computer  
2 network for its exclusive use called chinalake.navy.mil.

3 39. The Weapons Division used this network in furtherance of  
4 national defense.

5 DEFENSE INFORMATION SYSTEM AGENCY

6 40. The Defense Information Systems Agency ("DISA") was part  
7 of the United States Department of Defense ("DOD"), and was  
8 headquartered in Falls Church, Virginia.

9 41. DISA was a combat support agency responsible for  
10 planning, engineering, acquiring, fielding, and supporting global  
11 network based solutions to serve the needs of the President, the  
12 Vice-President, the Secretary of Defense, and various other DOD  
13 components, under all conditions of peace and war.

14 42. DISA maintained and exclusively used a computer network  
15 called disa.mil in furtherance of its national defense mission.

16 NEXUS TO COMMERCE

17 43. The computers belonging to EasyDedicated, FDCServers,  
18 Sago Networks, and The Planet were used in interstate and foreign  
19 commerce and communication.

20 COMPUTER TERMINOLOGY

21 Bot

22 44. The term "bot" is derived from the word "robot" and  
23 commonly refers to a software program that performs repetitive  
24 functions, such as indexing information on the Internet. Bots have  
25 been created to perform tasks automatically on Internet Relay Chat  
26 ("IRC") servers. The term "bot" also refers to computers that have  
27 been infected with a program used to control or launch distributed  
28 denial of service attacks against other computers.



### Botnet

45. A "botnet" is typically a network of computers infected with bots that are used to control or attack computer systems. Botnets are often created by spreading a computer virus or worm that propagates throughout the Internet, gaining unauthorized access to computers on the Internet, and infecting the computer with a particular bot program. The botnet is then controlled by a user, often through the use of a specified channel on Internet Relay Chat. A botnet can consist of tens of thousands of infected computers. The unsuspecting infected or compromised computers are often referred to as "zombies" or "drones" and are used to launch distributed denial of service attacks.

### Clickers

46. "Clickers" refer to malicious code or exploits that redirect victim machines to specified web sites or other Internet resources. Clickers can be used for advertising purposes or to lead a victim computer to an infected resource where the machine will be attacked further by other malicious code.

### Distributed Denial of Service Attack

47. A distributed denial of service attack or "DDOS attack" is a type of malicious computer activity where an attacker causes a network of compromised computers to "flood" a victim computer with large amounts of data or specified computer commands. A DDOS attack typically renders the victim computer unable to handle legitimate network traffic and often the victim computer will be unable to perform its intended function and legitimate users are denied the services of the computer. Depending on the type and intensity of the DDOS attack, the victim computer and its network

1 may become completely disabled and require significant repair.

2 Domain Name Server

3 48. A "domain" is a set of subjects and objects on the  
4 Internet which share common security policies, procedures, and  
5 rules, and are managed by the same management system. A "domain  
6 name" identifies where on the World Wide Web the domain is located.  
7 A "domain name server" or "DNS" translates or maps domain names to  
8 Internet Protocol ("IP") addresses and vice versa. Domain name  
9 servers maintain central lists of domain names/IP addresses,  
10 translate or map the domain names in an Internet request, and then  
11 send the request to other servers on the Internet until the  
12 specified address is found.

13 Exe

14 49. "Exe" is short for "executable" or ".exe" or executable  
15 file, and refers to a binary file containing a program that is  
16 ready to be executed or run by a computer. Hackers many times  
17 refer to their malicious programs or code as ".exe" or "exe." For  
18 example Hacker1 may ask Hacker2, "Did your exe spread over the  
19 network?"

20 Exploit

21 50. An "exploit" is computer code written to take advantage  
22 of a vulnerability or security weakness in a computer system or  
23 software.

24 Internet Protocol Address

25 51. An "Internet protocol address" or "IP address" is a  
26 unique numeric address used by computers on the Internet. An IP  
27 address is designated by a series of four numbers, each in the  
28 range 0-255, separated by periods (e.g., 121.56.97.178). Every

1 computer connected to the Internet must be assigned an IP address  
2 so that Internet traffic sent from and directed to that computer  
3 may be directed properly from its source to its destination. Most  
4 ISPs control a range of IP addresses, which they assign to their  
5 subscribers. No two computers on the Internet can have the same IP  
6 address at the same time. Thus, at any given moment, an IP address  
7 is unique to the computer to which it has been assigned.

#### 8 Internet Relay Chat

9 52. Internet Relay Chat ("IRC") is a network of computers  
10 connected through the Internet that allows users to communicate  
11 with others in real time text (known as "chat"). IRC users utilize  
12 specialized client software to use the service and can access a  
13 "channel" which is administered by one or more "operators" or  
14 "ops." IRC channels are sometimes dedicated to a topic and are  
15 identified by a pound sign and a description of the topic such as  
16 "#miamidolphins." IRC channels are also used to control botnets  
17 that are used to launch DDOS attacks, send unsolicited commercial  
18 email, and generate advertising affiliate income.

#### 19 Internet Relay Chat Daemon

20 53. Internet Relay Chat Daemon ("IRCD") is a computer program  
21 used to create an IRC server on which people can chat with each  
22 other via the Internet.

#### 23 Port

24 54. A "port" is a process that permits the operating system  
25 of a computer to know what to do with incoming traffic. A computer  
26 does not have physical ports. Rather, a port is a process that  
27 permits the computer to process information as it arrives at the  
28 computer. All incoming traffic has a "header" as well as its

1 content. Part of the header information identifies the port to  
2 which the incoming information is addressed. For example, Port 80  
3 is, by convention, website traffic. As a packet of information is  
4 received, the computer operating system notes that it is addressed  
5 to Port 80 and sends the packet to the web operating software.  
6 Similarly, Port 25 is for incoming e-mail. When the operating  
7 system sees a packet of information addressed to Port 25, it  
8 directs the packet to the e-mail software.

#### 9 Root/Administrative Privileges

10 55. Also known as "superuser" privileges, a user that has  
11 "root" or "administrator" status on a system has access to the  
12 system at a level sufficient to allow the user to make changes to  
13 the system in ways that a regular user accessing the system cannot.

#### 14 Server

15 56. A "server" or "box" is a centralized computer that  
16 provides services for other computers connected to it via a  
17 network. The other computers attached to a server are sometimes  
18 called "clients." In a large company, it is common for individual  
19 employees to have client computers on their desktops. When the  
20 employees access their email, or access files stored on the network  
21 itself, those files are pulled electronically from the server where  
22 they are stored, and are sent to the client's computer via the  
23 network. In larger networks, it is common for servers to be  
24 dedicated to a single task. For example, a server that is  
25 configured so that its sole task is to support a World Wide Web  
26 site is known simply as a "web server." Similarly, a server that  
27 only stores and processes email is known as a "mail server."

28 //



Spam & Proxies

57. "Spam" refers to unsolicited commercial email.

"Spamming" refers to the mass or bulk distribution of unsolicited commercial email.

58. Some spammers use software to extract and harvest target screen names and email addresses from newsgroups, chat rooms, email servers, and other areas of the Internet. Others simply enlist the "bulk e-mail services" of foreign or overseas companies.

59. Often spammers use computers infected with malicious code and made vulnerable to subsequent unauthorized access by routing spam through the victim computer in order to mask their originating email and IP address information. In this way, the infected computer serves as a "proxy" for the true spammer.

SynFlood

60. A "synflood" is a type of DDOS attack where a computer or network of computers send a large number of "syn" data packets to a targeted computer. Syn packets are sent by a computer that is requesting a connection with a destination computer. A synflood typically involves thousands of compromised computers in a botnet that flood a computer system on the Internet with "syn" packets containing false source information. The flood of syn packets causes the victimized computer to use all of its resources to respond to the requests and renders it unable to handle legitimate traffic.

Toolbar

61. A "toolbar" is a row or column of on-screen buttons used to activate functions in the application. Toolbars used as adware or malicious code often cause advertisements to pop up on the

1 infected user's computer.

2 Trojan

3 62. A "Trojan" or "Trojan Horse" is a malicious program that  
4 is disguised as a harmless application or is secretly integrated  
5 into legitimate software. A Trojan is typically silently installed  
6 and hides from the user. Although typically not self-replicating,  
7 additional components can be added to a Trojan to enable its  
8 propagation. A Trojan often allows a malicious attacker to gain  
9 unauthorized remote access to a compromised computer, infect files,  
10 or damage systems.

11 Uniform Resource Locator ("URL")

12 63. "Uniform Resource Locator" or "URL" is the unique address  
13 which identifies a resource on the Internet for routing purposes,  
14 such as <http://www.cnn.com>.

15 Worm

16 64. A "worm" is a program that replicates itself over a  
17 computer network and usually performs malicious actions, such as  
18 exhausting the computer's resources and possibly shutting the  
19 system down. Unlike a virus, a worm needs little or no human  
20 assistance to spread.

21 //

22 //

23 //

24 //

25 //

26 //

27 //

28 //

**COUNT ONE**

[18 U.S.C. § 371]

65. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64 of this Indictment.

**OBJECTS OF THE CONSPIRACY**

66. Beginning at least as early as June 25, 2004, and continuing through at least as late as September 15, 2004, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA, and others known and unknown to the Grand Jury, knowingly conspired, confederated, and agreed with each other:

a. To knowingly cause the transmission of a program, information, code and command, and as a result of such conduct, intentionally cause damage without authorization to a computer used in interstate and foreign commerce and communication, and cause loss during a one-year period aggregating at least \$5,000 in value, in violation of 18 U.S.C. §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), and 1030(b); and

b. To access without authorization a computer used in interstate and foreign commerce and communication, and intentionally initiate the transmission from and through that computer of multiple commercial electronic mail messages that affect interstate and foreign commerce, in violation of 18 U.S.C. §§ 1037(a)(1), 1037(b)(2)(A), and 1037(b)(2)(F).

**MEANS BY WHICH THE CONSPIRACY WAS TO BE ACCOMPLISHED**

67. The objects of the conspiracy were to be accomplished as follows:

1       68. ANCHETA would obtain access to a server from an Internet  
2 hosting company.

3       69. ANCHETA would use the server as an IRC server by running  
4 an IRCD.

5       70. ANCHETA would create a channel in IRC which he  
6 controlled.

7       71. ANCHETA would develop a worm which would cause infected  
8 computers, unbeknownst to the users of the infected computers, to:

9           a. report to the IRC channel he controlled;

10           b. scan for other computers vulnerable to similar  
11 infection; and

12           c. succumb to future unauthorized accesses, including  
13 for use as proxies for spamming.

14       72. ANCHETA would use the server to disseminate the worm,  
15 infect vulnerable computers connected to the Internet, and cause  
16 thousands of victim computers per day to report to the IRC channel  
17 he controlled on the server.

18       73. ANCHETA would then advertise the sale of bots for the  
19 purpose of launching DDOS attacks or using the bots as proxies to  
20 send spam.

21       74. ANCHETA would sell up to 10,000 bots or proxies at a  
22 time.

23       75. ANCHETA would discuss with purchasers the nature and  
24 extent of the DDOS or proxy spamming they were interested in  
25 conducting, and recommend the number of bots or proxies necessary  
26 to accomplish the specified attack.

27       76. ANCHETA would set the price based upon the number of bots  
28 or proxies purchased.



1        77. For an additional price, ANCHETA would provide the  
2 purchaser with worm or exe, and set up or configure it for the  
3 particular purchaser's use so that it would cause the purchased  
4 bots or proxies to spread or propagate.

5        78. For an additional price, ANCHETA would create a separate  
6 channel on his IRC server, rally or direct the purchased bots to  
7 that channel, and grant the purchaser access to the IRC server and  
8 control over that channel.

9        79. ANCHETA would accept payments through Paypal.

10       80. ANCHETA would either describe, or direct the purchaser to  
11 describe, the nature of the transaction in Paypal as "hosting" or  
12 "web hosting" or "dedicated box" services, in order to mask the  
13 true nature of the transaction.

14       81. Once he received payment, ANCHETA would set up or  
15 configure the purchased botnet for the purchaser, test the botnet  
16 with the purchaser in order to ensure that DDOS attacks or proxy  
17 spamming would be successfully carried out, or advise the purchaser  
18 about how to properly maintain, update, and strengthen the  
19 purchased botnet.

20       OVERT ACTS

21       82. In furtherance of the conspiracy, and to accomplish the  
22 objects of the conspiracy, defendant JEANSON JAMES ANCHETA and  
23 others known and unknown to the Grand Jury, committed various overt  
24 acts in Los Angeles County, within the Central District of  
25 California, and elsewhere, including the following:

26       Opening for Business

27       83. On or about June 25, 2004, ANCHETA leased a server from  
28 Sago Networks.

1       84. In or about early July 2004, ANCHETA ran an IRCD so that  
2 he could use the server he leased from Sago Networks as an IRC  
3 server.

4       85. In or about early July 2004, ANCHETA modified for his own  
5 purposes a Trojan called "rxbot," a malicious code known to provide  
6 a nefarious computer attacker with unauthorized remote  
7 administrative level control of an infected computer by using  
8 commands sent over IRC.

9       86. In or about early July 2004, ANCHETA used the modified  
10 rxbot to scan for and exploit vulnerable computers connected to the  
11 Internet, causing them to rally or be directed to a channel in IRC  
12 which he controlled, to scan for other computers vulnerable to  
13 similar infection, and to remain vulnerable to further unauthorized  
14 access.

15       87. In or about early July 2004, ANCHETA created a channel in  
16 IRC called #botz4sale.

17       88. In or about early July 2004, ANCHETA inserted a link in  
18 IRC channel #botz4sale to an advertisement and price list  
19 pertaining to the sale of bots and proxies.

20 Sale to Circa

21       89. On or about July 10, 2004, during a chat in IRC, an  
22 unindicted co-conspirator using the nickname "circa" asked ANCHETA  
23 to sell her 10,000 bots so that she could "mail from the proxies."

24       90. On or about July 10, 2004, during a chat in IRC, ANCHETA  
25 asked circa how much she made "off proxies," to which circa  
26 responded, "I make pretty good money."

27       91. Between on or about July 10, 2004 and August 7, 2004,  
28 ANCHETA sold bots to circa and received payments from circa via

1 | Paypal totaling approximately \$400.

2 | Sale to KiD

3 | 92. On or about July 19, 2004, during a chat in IRC, an  
4 | unindicted co-conspirator using the nickname KiD told ANCHETA that  
5 | he needed a more effective worm to expand his existing 2,500-strong  
6 | botnet.

7 | 93. On or about July 20, 2004, ANCHETA sold the worm he had  
8 | used to create the bots and proxies advertised on #botz4sale to  
9 | KiD, and received payment for the worm through Paypal.

10 | 94. On or about July 22, 2004, during a chat in IRC, KiD  
11 | asked ANCHETA "wats [sic] the best ddos command" for the worm KiD  
12 | had purchased from ANCHETA.

13 | 95. On or about July 22, 2004, during a chat in IRC, ANCHETA  
14 | told KiD that he had more than 40,000 bots for sale, commenting,  
15 | "more than I can handle, I can't even put them all online because I  
16 | don't have enough servers, so I'm not even sure how many I got."

17 | Sale to zxpl

18 | 96. On or about July 23, 2004, during a chat in IRC, ANCHETA  
19 | told an unindicted co-conspirator using the nickname "zxpl" that  
20 | his worm caused 1,000 to 10,000 new bots to join his botnet over  
21 | the course of only three days.

22 | 97. On or about July 23, 2004, during a chat in IRC, zxpl  
23 | told ANCHETA that his own server could hold only 7,000 bots, and  
24 | asked ANCHETA to conduct a synflood DDOS attack against an IP  
25 | address belonging to King Pao Electronic Co., Ltd. in Taipei,  
26 | Taiwan, which zxpl identified for ANCHETA.

27 | 98. On or about July 23, 2004, during a chat in IRC, zxpl  
28 | offered to buy ANCHETA's worm with advertising affiliate proceeds

1 zxpL had generated using his own botnet.

2 99. On or about July 24, 2004, during a chat in IRC, zxpL  
3 again asked ANCHETA to conduct a synflood DDOS attack, this time  
4 against an IP address belonging to Sanyo Electric Software Co.,  
5 Ltd. in Osaka, Japan, which zxpL identified for ANCHETA.

6 100. On or about July 26, 2004, zxpL asked ANCHETA to create a  
7 separate IRC channel for the bots he would purchase from ANCHETA.

8 101. By on or about August 2, 2004, ANCHETA sold an exe and  
9 1,500 bots to zxpL and received payment through Paypal, bringing  
10 the number of bots available to zxpL for DDOS attacks to at least  
11 8,500.

12 102. On or about August 3, 2004, during a chat in IRC, zxpL  
13 told ANCHETA, "ur [your] bot spreads uber fast."

14 Improving the Business

15 103. In or about August 2004, ANCHETA updated his  
16 advertisement to increase the price of bots and proxies, to limit  
17 the purchase of bots to 2,000 "due to massive orders," and to warn,  
18 "I am not responsible for anything that happens to you or your bots  
19 after you see your amount of bots you purchased in your room [IRC  
20 channel]."

21 Sales to Daytona and MLG

22 104. On or about August 6, 2004, ANCHETA sold an exe and 250  
23 bots to an unindicted co-conspirator using the nickname "Daytona,"  
24 and received payment through Paypal.

25 105. On or about August 6, 2004 through August 9, 2004, during  
26 several chats in IRC, ANCHETA educated Daytona about how to  
27 maintain and use the bots Daytona had purchased from ANCHETA.

28 //



1        106. On or about August 9, 2004, during chats in IRC, Daytona  
2 asked ANCHETA to sell Daytona additional bots, explaining, "I need  
3 the bots bad . . . I need the bots . . . I need them bots . . .  
4 send asap."

5        107. On or about August 9, 2004, ANCHETA sold an additional  
6 400 bots to Daytona, and received payment through Paypal.

7        108. The next day, on or about August 10, 2004, Daytona  
8 introduced ANCHETA to another potential buyer, an unindicted co-  
9 conspirator using the nickname "MLG".

10       109. On or about August 10, 2004, during a chat in IRC, MLG  
11 told ANCHETA that he needed the bots to launch DDOS attacks,  
12 explaining, it "just doesn't feel the same unless ya do 'em  
13 yourself. . :) [smile]."

14       110. On or about August 10, 2004, Daytona gave MLG 100 of the  
15 bots Daytona had purchased from ANCHETA.

16       111. On or about August 10, 2004, MLG sent ANCHETA payment  
17 through Paypal.

18       112. On or about August 10, 2004, ANCHETA gave 250 bots to  
19 Daytona, who kept 150 of them as payment from MLG for brokering the  
20 sale between ANCHETA and MLG.

21       Sale to Teh1

22       113. On or about July 13, 2004, during a chat in IRC,  
23 unindicted co-conspirator "Teh1" asked ANCHETA to sell him a worm  
24 or exe that would cause advertising affiliate adware to  
25 surreptitiously install on bots in a 2,000 strong botnet.

26       114. On or about July 13, 2004, during a chat in IRC, ANCHETA  
27 agreed to give Teh1 the requested exe, told Teh1, "Keep making your  
28 bots download my .exe" until Teh1's botnet generated at least \$50

1 in proceeds from surreptitious advertising affiliate adware  
2 installs, and instructed Tehl to then transfer the \$50 to ANCHETA  
3 as payment for the exe.

4 115. Between on or about July 14, 2004 and on or about August  
5 12, 2004, ANCHETA and Tehl continued to negotiate the sale of the  
6 exe.

7 116. On or about August 12, 2004, ANCHETA sold an exe to Tehl,  
8 and received payment through Paypal.

9 Sale to Sploit

10 117. On or about August 21, 2004, ANCHETA sold \$300 worth of  
11 bots to an unindicted co-conspirator using the nickname "Sploit".

12 118. During a subsequent chat in IRC, Sploit explained to  
13 ANCHETA that he needed to purchase bots for spamming because he  
14 owned a data center in Japan that he used for "100% spam,"  
15 commenting to ANCHETA, "I can mail from those to the U.S., plus  
16 they get decent speeds."

17 Sales to O\_2iginal

18 119. On or about August 21, 2004, during a chat in IRC,  
19 ANCHETA told an unindicted co-conspirator using the nickname  
20 "o\_2riginal" that he was hosting "around 100k bots total," that in  
21 a week and a half 1,000 of his bots scanned and infected another  
22 10,000, and that his botnet would be bigger if he had not used some  
23 himself for "ddosing."

24 120. On or about August 21, 2004, during a chat in IRC,  
25 o\_2riginal warned ANCHETA that he should make sure "to filter out  
26 shit though like .gov and .mils" after his bots scanned and  
27 infected other computers.

28 //

1 121. On or about August 21, 2004, during a chat in IRC,  
2 o\_2riginal told ANCHETA that o\_2riginal was a "big spam[mer]," that  
3 he "got all this work but not enough resources," that he wanted to  
4 buy 1,000 bots "for packeting and a fucking proxy subscription,"  
5 and asked, "If I use these bots as proxies will they go down  
6 easily?", to which ANCHETA responded, "on my bots, yeah, fo  
7 shizzle."

8 122. On or about August 21, 2004, during a subsequent chat in  
9 IRC, ANCHETA offered to sell o\_2riginal 7,000 proxies, explaining  
10 that the life of the proxies "depends on how long it takes the  
11 server to ban the proxies that ur mailing through."

12 123. On or about August 21, 2004, ANCHETA sold o\_2riginal  
13 3,000 proxies, and received payment through Paypal.

14 124. On or about August 23, 2004, ANCHETA sold o\_2riginal  
15 2,000 bots and an exe that would cause the purchased bots to spread  
16 or propagate, and received payment through Paypal.

17 125. From on or about August 23, 2004 through September 15,  
18 2004, during chats in IRC, ANCHETA advised O\_2riginal how to  
19 maintain, update, and strengthen the purchased botnet.

20 Sale to Seminole Pride

21 126. On or about August 23, 2004, an unindicted co-conspirator  
22 using the nickname "Seminole Pride" sent ANCHETA payment through  
23 Paypal for the purchase of 100 bots and the exe that would cause  
24 the purchased bots to spread or propagate.

25 127. On or about August 24, 2004, Seminole Pride provided  
26 ANCHETA with the server name "irc.dsstrust.com" and the channel .  
27 "#floodz" so that ANCHETA could load the exe and rally or direct  
28 the purchased bots to that channel.

1 128. On or about August 24, 2004, ANCHETA completed the sale  
2 to Seminole Pride by loading the exe and rallying or directing the  
3 purchased bots to IRC channel #floodz.

4 Sale to Longwordus

5 129. On or about September 15, 2004, during a chat on AIM, an  
6 unindicted co-conspirator using the nickname "Longwordus" asked  
7 ANCHETA to purchase 1,000 bots and an exe to cause the bots to  
8 spread or propagate.

9 130. On or about September 15, 2004, ANCHETA sold 1,000 bots  
10 and exe to Longwordus, and received payment through Paypal.

11 131. On or about September 15, 2004, ANCHETA set up or  
12 configured the exe for Longwordus and helped him test the purchased  
13 botnet.

14 Sale to a Confidential Source

15 132. On or about August 4, 2004, during a chat on AIM, ANCHETA  
16 told a confidential source that he earned \$1,000 in two weeks by  
17 selling bots and proxies, and that he would be willing to sell some  
18 to the confidential source.

19 133. On or about August 13, 2004, during a chat on AIM, when  
20 the confidential source told ANCHETA that he wanted to purchase  
21 bots to conduct DDOS attacks against some web sites, ANCHETA  
22 inquired whether the confidential source knew "rx" and understood  
23 how to launch "rx dDOS attacks."

24 134. On August 24, 2004, when the confidential source, posing  
25 as a different user, contacted ANCHETA over AIM and asked "to buy  
26 some bots for proxys," ANCHETA confirmed his ability to do so and  
27 asked the confidential source to contact him "in a few hours."  
28



1       135. On August 25, 2004, when the confidential source, posing  
2 as yet another user, contacted ANCHETA over AIM and asked to  
3 purchase a large botnet consisting of 20,000 compromised computers  
4 with good attack power and the ability to send spam, ANCHETA told  
5 the confidential source that he would be willing to sell only up to  
6 2,000 bots.

7       136. On August 25, 2004, during a chat on AIM, when the  
8 confidential source asked ANCHETA whether 2,000 bots would be  
9 "enough to drop a site," ANCHETA confirmed that 2,000 bots would be  
10 capable of launching various types of DDOS attacks, including a  
11 synflood.

12       137. On August 25, 2004, during a chat on AIM, when the  
13 confidential source specifically explained to ANCHETA that he  
14 needed a botnet strong and stable enough to launch a synflood DDOS  
15 attack against a business competitor operating a web site at 500  
16 megabits per second, ANCHETA confirmed again that 2,000 of his bots  
17 would be "plenty" to take down that specific site.

18       138. On or about August 31, 2004, ANCHETA sold the  
19 confidential source 2,000 bots, the exe to cause the bots to  
20 spread, and space on ANCHETA's IRC server to host the purchased  
21 botnet, receiving payment through Paypal.

22       139. On or about September 1, 2004, during a chat in IRC,  
23 ANCHETA sent the confidential source a file to download the  
24 purchased exe, and requested that the confidential source run the  
25 exe to enable the particular IRC channel ANCHETA had set up for the  
26 confidential source to accept bots.

27 //

28 //

1 140. On or about September 1, 2004, during a chat in IRC,  
2 ANCHETA accessed his botnet and issued commands to rally or direct  
3 2,000 bots to join the particular IRC channel ANCHETA had set up  
4 for the confidential source.

5 //

6 //

7 //

8 //

9 //

10 //

11 //

12 //

13 //

14 //

15 //

16 //

17 //

18 //

19 //

20 //

21 //

22 //

23 //

24 //

25 //

26 //

27 //

28 //

## COUNT TWO

[18 U.S.C. §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), and 1030(b)]

141. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64, as well as paragraphs 66 through 88 and 96 through 103 of this Indictment.

142. Beginning on or about July 23, 2004 and continuing through on or about August 3, 2004, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA attempted to knowingly cause the transmission of a program, information, code and command, and as a result of such conduct, intentionally cause damage without authorization to a computer used in interstate and foreign commerce and communication, namely, defendant JEANSON JAMES ANCHETA supplied an unindicted co-conspirator using the nickname zxpl with malicious computer code and unauthorized access to 1,500 compromised computers in order to launch distributed denial of service attacks against protected computers using IP addresses 210.209.57.1 and 219.106.106.37 and belonging to King Pao Electronic Co., Ltd. and Sanyo Electric Software Co., Ltd., respectively, which, as a result of such conduct, would have caused, if completed, loss during a one-year period aggregating at least \$5,000 in value.

//

//

//

//

//

//

**COUNT THREE**

[18 U.S.C. §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), and 1030(b)]

143. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64, as well as paragraphs 66 through 88, 103, and 132 through 140 of this Indictment.

144. Beginning on or about August 25, 2004 and continuing through on or about September 1, 2004, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA attempted to knowingly cause the transmission of a program, information, code and command, and as a result of such conduct, intentionally cause damage without authorization to a computer used in interstate and foreign commerce and communication, namely, defendant JEANSON JAMES ANCHETA supplied a confidential source with malicious computer code, unauthorized access to 2,000 compromised computers, and use of an IRC server, all in order to launch distributed denial of service attacks against protected computers operating a web site at 500 megabits per second belonging to a business competitor of the confidential source, which, as a result of such conduct, would have caused, if completed, loss during a one-year period aggregating at least \$5,000 in value.

//

//

//

//

//

//

//



## COUNT FOUR

[18 U.S.C. § 371]

145. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64, as well as paragraphs 98, 113, and 114 of this Indictment.

OBJECTS OF THE CONSPIRACY

146. Beginning at least as early as August 2004 and continuing through at least as late as August 2005, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA, and others known and unknown to the Grand Jury, knowingly conspired, confederated, and agreed with each other:

a. To knowingly cause the transmission of a program, information, code and command, and as a result of such conduct, intentionally cause damage without authorization to a computer involved in interstate and foreign commerce and communication, and cause loss aggregating more than \$5,000 in a one-year period, and damage affecting a computer system used by and for a government entity in furtherance of the administration of justice, national defense, and national security, all in violation of 18 U.S.C. §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), 1030(a)(5)(B)(v), and 1030(b); and

b. To knowingly and with intent to defraud, access a computer used in interstate and foreign commerce and communication without authorization, and by means of such conduct, further the intended fraud and obtain something of value, in violation of 18 U.S.C. §§ 1030(a)(4) and 1030(b).

//

1 MEANS BY WHICH THE CONSPIRACY WAS TO BE ACCOMPLISHED

2 147. The objects of the conspiracy were to be accomplished as  
3 follows:

4 148. ANCHETA and an unindicted co-conspirator using the  
5 nickname "SoBe" would obtain access to servers from Internet  
6 hosting companies.

7 149. ANCHETA and SoBe would use servers to which they had  
8 access as IRC servers by running IRCDs.

9 150. ANCHETA and SoBe would create channels in IRC which they  
10 controlled.

11 151. ANCHETA and SoBe would enroll as affiliates of  
12 advertising service companies and obtain affiliate identification  
13 numbers for the purpose of receiving compensation for adware  
14 installations.

15 152. ANCHETA and SoBe would create clickers; namely, they  
16 would modify without permission the adware they obtained from the  
17 advertising service companies to enable the adware to be  
18 surreptitiously installed without notifying, or requiring any  
19 action from, a computer's user, but nonetheless appear to the  
20 advertising service companies as legitimately installed.

21 153. ANCHETA and SoBe would use other servers to which they  
22 had access as servers hosting malicious adware or clickers.

23 154. ANCHETA and SoBe would cause the transmission of  
24 malicious code to computers connected to the Internet, causing the  
25 infected computers to report to an IRC channel controlled by  
26 ANCHETA and SoBe, thereby creating a botnet.

27 155. ANCHETA and SoBe would cause infected computers in the  
28 botnet to be redirected to one of their adware servers, where files

1 containing components of a Trojan horse program would download onto  
2 the infected computers, causing the surreptitious installation of  
3 adware.

4 156. ANCHETA and SoBe would cause the advertising affiliate  
5 companies whose adware would be surreptitiously installed on an  
6 infected computer to be notified of that instance of installation,  
7 and to credit one of their affiliate identification numbers for  
8 that installation.

9 157. ANCHETA and SoBe would receive periodic payments from  
10 advertising service companies based upon the number of  
11 installations of adware that were credited to them.

12 158. To avoid detection by network administrators, security  
13 analysts, or law enforcement, and thereby maintain the integrity of  
14 the scheme, ANCHETA and SoBe would use IRC channel topic commands  
15 to vary the download times and rates of adware installations so  
16 that the installations would appear to be legitimate web traffic to  
17 anyone that may be watching.

18 159. When a company hosting a particular adware server grew  
19 suspicious of or discovered the malicious activity, ANCHETA and  
20 SoBe would cause infected computers residing on IRC servers they  
21 controlled, or to which they had access, to be redirected to  
22 another adware server they controlled, or to which they had access,  
23 so as to further maintain the integrity and success of the scheme.

24 160. ANCHETA would transfer a portion of the payments he  
25 received from advertising service companies to SoBe as a fee for  
26 maintaining the botnet and adware servers.

27 //

28 //

1 OVERT ACTS

2 161. In furtherance of the conspiracy, and to accomplish the  
3 objects of the conspiracy, defendant JEANSON JAMES ANCHETA and  
4 others known and unknown to the Grand Jury, committed various overt  
5 acts in Los Angeles County, within the Central District of  
6 California, and elsewhere, including the following:

7 162. On or about August 13, 2004, ANCHETA transferred \$114.00  
8 to Sago Networks through Paypal as payment for access to a server.

9 163. On or about September 3, 2004, ANCHETA transferred  
10 \$100.00 to Sago Networks through Paypal as payment for access to a  
11 server.

12 164. On or about September 21, 2004, during a chat on AIM,  
13 ANCHETA told another AIM user who had offered to install ANCHETA's  
14 clickers on bots in exchange for a percentage of any advertising  
15 affiliate payment generated, "i pay sherby \$500 month to do my  
16 clicker everyday as topic for 30 min but he has a lot of bots ... i  
17 mean SOBE."

18 165. On or about September 27, 2004, ANCHETA transferred  
19 \$200.09 from his Wells Fargo Bank account to The Planet as payment  
20 for access to a server.

21 166. On or about October 8, 2004, ANCHETA received \$2,305.89  
22 from LOUDcash through Paypal.

23 167. On the same day, on or about October 8, 2004, ANCHETA  
24 transferred \$120 to SoBe through Paypal.

25 168. On or about October 5, 2004, during a chat on AIM,  
26 ANCHETA educated SoBe about how to avoid detection by network  
27 administrators, security analysts, or law enforcement, explaining,  
28 among other things, "try and limit yourself from logging into your

1 bots unless its very important because that's how it gets sniffed,"  
2 "if you do login into your bots don't ever [use] your real handle,"  
3 and if "authorities or anything" find "the box," "just ignore and  
4 notify me."

5 169. On or about October 5, 2004, during a chat on AIM,  
6 ANCHETA gave SoBe the operator password to the IRC channel  
7 #syzt3m#.

8 170. On or about October 5, 2004, during a chat on AIM,  
9 ANCHETA asked SoBe, "when do you want to start doing the lc  
10 [LOUDcash] stuff again. . .i'm still waiting for lc [LOUDcash] to  
11 fucking pay. . .tomorrow they should pay since its the 6<sup>th</sup>."

12 171. On or about October 17, 2004, during a chat on AIM, while  
13 discussing with SoBe clicker install statistics, ANCHETA stated  
14 that he was receiving affiliate credit for at least 1,000 clickers  
15 per day, commenting, "i'm averaging an extra 2-3 buffalo.edu per 30  
16 minutes with this forbot hehe."

17 172. On or about October 17, 2004, during a chat on AIM, after  
18 learning from SoBe that a server they controlled, or to which they  
19 had access, "hit new high max this morning," that SoBe believed  
20 they would need access to another server soon, and that SoBe would  
21 need help in moving some of the botnet to a new server, ANCHETA  
22 replied, "i dont care ur helping me im helping you its all good."

23 173. On or about October 17, 2004, during a chat on AIM,  
24 ANCHETA reassured SoBe, explaining "fbi dont bust ya for having  
25 bots. . .its how you use them. . .i mean think about it, a company  
26 that makes thousands a day and you crippled it just for a day they  
27 lose lots and not just affecting that site your affecting many  
28 others on that box . . .haha many ways of killing a box without



1 ddos ==)." "

2 174. On or about October 17, 2004, during a chat on AIM,  
3 ANCHETA instructed SoBe to "switch to lc [LOUDcash]," to which SoBe  
4 responded, "i forgot actually . . .damn, that was almost an hour. .  
5 .the reason why i dont like to do both [affiliate programs] . . .is  
6 than [sic] i would be paying them so much."

7 175. On or about October 18, 2004, ANCHETA transferred \$65.00  
8 to Sago Networks through Paypal as payment for access to a server.

9 176. On or about October 20, 2004, ANCHETA deposited a  
10 \$3,034.61 check from Gammacash into his Wells Fargo Bank account.

11 177. On or about October 21, 2004, during a chat on AIM, when  
12 SoBe complained that "there werent a lot of bots," ANCHETA told  
13 SoBe to "stay in the server" and that ANCHETA would "restart the  
14 box first thing tomorrow."

15 178. On or about October 21, 2004, during a chat on AIM,  
16 ANCHETA discussed with SoBe how to change the topic in the IRC  
17 channel to maximize the number of bots successfully redirected to  
18 the adware servers without detection.

19 179. On or about October 24, 2004, during a chat on AIM,  
20 ANCHETA told SoBe, "if you wanna keep seeing the money coming lets  
21 keep the bot talking to nothing," explaining, "there are tons of  
22 admins [network administrators] out there, thats why i tell  
23 everyone i have no bots."

24 180. On or about October 24, 2004, during a chat on AIM,  
25 ANCHETA and SoBe discussed their affiliate earnings, ANCHETA  
26 predicted that SoBe would make "2.2gs" by the end of the month, and  
27 when SoBe asked, "I wonder how long itll last," ANCHETA responded,  
28 "as long as everything is [on the "down low" or undiscovered] im

1 estimating 6 more months to 8 months, hopefully a year."

2 181. On or about October 30, 2004, during a chat on AIM,  
3 ANCHETA told SoBe he was setting the topic in IRC to LOUDcash,  
4 namely, that ANCHETA would redirect the bots in the IRC channel to  
5 navigate to the adware server where LOUDcash clickers would  
6 surreptitiously install onto the bots.

7 182. On or about October 30, 2004, during a chat on AIM,  
8 ANCHETA discussed with SoBe the money they were making, commenting  
9 "its easy like slicing cheese," to which SoBe later responded, "I  
10 just hope this lc [LOUDcash] stuff lasts a while so I don't have to  
11 get a job right away."

12 183. On or about October 31, 2004, during a chat on AIM,  
13 ANCHETA mentioned to SoBe, "you did good this month," predicted  
14 that SoBe would make over \$1,000 for the month, and instructed SoBe  
15 to upgrade his Paypal account so that he could receive a payment in  
16 an amount over \$1,000.

17 184. On or about October 31, 2004, during a chat on AIM, SoBe  
18 told ANCHETA, "hey btw [by the way] there are gov/mil on the box if  
19 you want to get rid of them," to which ANCHETA responded "rofl  
20 [rolling on the floor laughing]."

21 185. In or about November 2004, ANCHETA leased a server  
22 located at FDCServers.

23 186. On or about November 2, 2004, ANCHETA transferred \$187.00  
24 from his Wells Fargo Bank account to The Planet as payment for  
25 access to a server.

26 187. On or about November 5, 2004, ANCHETA deposited a  
27 \$3,970.91 check from Gammacash into his Wells Fargo Bank account.

28 //

1 188. On or about November 9, 2004, ANCHETA obtained access to  
2 a server located at EasyDedicated.

3 189. On or about November 10, 2004, during a chat on AIM, when  
4 SoBe told ANCHETA that a large number of bots from uncc.edu were  
5 reporting to an IRC channel they controlled, or to which they had  
6 access, ANCHETA warned SoBe "if you do it too much you will get  
7 caught up one time or another."

8 190. On or about November 12, 2004, during a chat on AIM, SoBe  
9 told ANCHETA, "we hit 49.990k this morning, usually the box peaks  
10 at 50000," to which ANCHETA responded, "im getting another box. .  
11 .i suggest u do too."

12 191. On or about November 12, 2004, during a chat on AIM,  
13 ANCHETA asked SoBe to remind him which email account SoBe was using  
14 at Paypal so that ANCHETA could pay him from the affiliate proceeds  
15 ANCHETA was expecting to receive shortly.

16 192. On or about November 16, 2004, ANCHETA received \$1,263.73  
17 from LOUDcash through Paypal.

18 193. On the same day, or about November 16, 2004, ANCHETA  
19 transferred \$1,100 to SoBe through Paypal.

20 194. On or about November 19, 2004, ANCHETA deposited a  
21 \$4,044.26 check from Gammacash into his Wells Fargo Bank account.

22 195. Or about November 19, 2004, during a chat on AIM, ANCHETA  
23 told SoBe that he had set up a server "just as a distraction for  
24 the fbi to see that im running legal network."

25 196. On or about November 20, 2004, during a chat on AIM,  
26 ANCHETA told SoBe, "hey bro try to find me a west coast datacenter  
27 that allows ircd."

28 //

1 197. On or about November 20, 2004, during a chat on AIM,  
2 ANCHETA told SoBe "i hope the box dont get reported again, I ddosed  
3 with my bots on there, i needed the extra power, it wont get  
4 reported though since its a new .exe."

5 198. On or about November 20, 2004, during a chat on AIM,  
6 ANCHETA told SoBe that he would change the topic in the IRC channel  
7 to redirect the bots to a different adware server and monitor the  
8 channel for an hour or so while SoBe was unavailable to do so.

9 199. On or about November 20, 2004, during a chat on AIM,  
10 while discussing their affiliate earnings, ANCHETA told SoBe, "my  
11 average spending is \$600 a week, every friday I buy new clothes and  
12 every week I buy new parts for my car."

13 200. On or about November 23, 2004, ANCHETA transferred  
14 \$149.00 from his Wells Fargo Bank account to FDCServers as payment  
15 for access to a server.

16 201. On or about November 24, 2004, ANCHETA caused SoBe to  
17 obtain access for them to a server from Sago Networks.

18 202. On or about November 27, 2004, during a chat on AIM,  
19 ANCHETA taught SoBe how to run IRCD, configure, and set  
20 root/administrator privileges and passwords on the new server SoBe  
21 had leased from Sago Networks.

22 203. On or about November 28, 2004, during a chat on AIM,  
23 ANCHETA told SoBe that one of their adware servers was flooded and  
24 instructed SoBe to set more than one topic in IRC for a few hours  
25 to simultaneously direct the bots to multiple adware servers to  
26 correct the problem.

27 204. On or about December 7, 2004, during a chat on AIM,  
28 ANCHETA agreed with SoBe that he should log into the IRC channel

1 and improve the "scanners."

2 205. On or about December 7, 2004, during a chat on AIM,  
3 ANCHETA warned SoBe to use more innocuous, common sounding names  
4 like "imports" or "honda" as the domains for the botnet and adware  
5 servers, explaining, "that lessens the suspicious activity . . .  
6 only dumbasses buy domains for there [sic] botnets and call it  
7 1337-botnet.com."

8 206. On or about December 7, 2004, during a chat on AIM,  
9 ANCHETA explained to SoBe, "most ppl dont know that bnets how they  
10 spread all depends on what kind of bots your starting with, if you  
11 have a wide range of different isp bots you will spread a lot  
12 faster, thats why nets stop at a certain point its because theres  
13 nothing else to scan."

14 207. On or about December 7, 2004, during a chat on AIM,  
15 ANCHETA posted to SoBe a complaint message he had received from an  
16 internet hosting company that read "the IRC server controlling the  
17 bot drones is on port >6667, and the IRC channel is #syzt3m,"  
18 commented to SoBe, "they forgot the # rofl so we are cool," told  
19 SoBe "I'm gonna msg them saying 'this irc network was investigated  
20 by my staff and we have removed the suspicious channel related to  
21 this'" and concluded, "haha always works."

22 208. On or about December 7, 2004, during a chat on AIM,  
23 ANCHETA told SoBe, "a tip to you is after setting up a bnet or irc  
24 or something illegal, do history -c, it will clear ur [your]  
25 history cmd's [commands]."

26 209. On or about December 7, 2004, ANCHETA received \$1,306.52  
27 from LOUDcash through Paypal.

28 //



1       210. On or about December 7, 2004, ANCHETA transferred \$1,200  
2 to SoBe through Paypal.

3       211. On or about December 7, 2004, ANCHETA discussed with SoBe  
4 over AIM the various advertising service companies for which they  
5 could serve as affiliates by using their botnets to install  
6 malicious code and make money, concluding "its immoral but the  
7 money makes it right."

8       212. On or about December 7, 2004, during a chat on AIM,  
9 ANCHETA and SoBe tested and modified the malicious code they were  
10 using to improve the efficiency and performance of the botnet and  
11 clickers.

12       213. On or about December 10, 2004, ANCHETA deposited a  
13 \$2,732.96 check from Gammacash into his Wells Fargo Bank account.

14       214. On or about December 14, 2004, ANCHETA caused a computer  
15 on the computer network of the China Lake Naval Air Facility to  
16 attempt to connect to #syzt3m#, an IRC channel he controlled,  
17 located on an IRC server at Sago Networks leased by SoBe.

18       215. On or about December 20, 2004, ANCHETA transferred  
19 \$149.00 from his Wells Fargo Bank account to FDCServers as payment  
20 for access to a server.

21       216. On or about December 24, 2004, ANCHETA deposited a  
22 \$2,352.86 check from Gammacash into his Wells Fargo Bank account.

23       217. On or about January 5, 2005, ANCHETA caused a computer on  
24 the computer network of the China Lake Naval Air Facility to  
25 attempt to connect to #syzt3m#, an IRC channel he controlled,  
26 located on an IRC server at Sago Networks leased by SoBe.

27       218. On or about January 7, 2005, ANCHETA received \$450.63  
28 from LOUDcash through Paypal.

1       219. On or about January 8, 2005, ANCHETA transferred \$425 to  
2       SoBe through Paypal.

3       220. On or about January 9, 2005, ANCHETA caused a computer on  
4       the computer network of the Defense Information Security Agency to  
5       attempt to connect to #syzt3m#, an IRC channel he controlled,  
6       located on an IRC server at Sago Networks leased be SoBe.

7       221. On or about January 10, 2005, ANCHETA deposited a  
8       \$2,139.86 check from Gammacash into his Wells Fargo Bank account.

9       222. On or about January 21, 2005, ANCHETA deposited a  
10       \$2,429.81 check from Gammacash into his Wells Fargo Bank account.

11       223. On or about February 6, 2005, ANCHETA caused a computer  
12       on the computer network of the Defense Information Security Agency  
13       to attempt to connect to #syzt3m#, an IRC channel he controlled,  
14       located on an IRC server at Sago Networks leased by SoBe.

15       224. On or about February 7, 2005, ANCHETA deposited a  
16       \$2,988.11 check from Gammacash into his Wells Fargo Bank account.

17       225. On or about February 16, 2005, ANCHETA transferred \$1,100  
18       to SoBe through Paypal.

19       226. On or about February 16, 2005, ANCHETA caused the  
20       approximately 18,540 bots that had joined the IRC channel #syzt3m#  
21       to be redirected to navigate to an adware server located at  
22       FDCServers which he controlled, or to which he had access, and  
23       receive additional malicious code, namely, clickers.

24       227. On or about February 16, 2005, after FDCServers  
25       terminated ANCHETA's lease "for hosting malicious botnets," ANCHETA  
26       caused the topic in the IRC channel #syzt3m# to change to redirect  
27       the bots in that channel to navigate to a different adware server,  
28       one at EasyDedicated that he controlled, or to which he had access.

1       228. On or about February 17, 2005, ANCHETA caused the  
2 approximately 19,901 bots that had joined the IRC channel #syzt3m#  
3 to be redirected to navigate to an adware server located at  
4 EasyDedicated which he controlled, or to which he had access, and  
5 attempt to receive additional malicious code, namely, clickers.

6       229. On or about February 18, 2005, ANCHETA caused the  
7 approximately 21,973 bots that had joined the IRC channel #syzt3m#  
8 to be redirected to navigate to an adware server located at  
9 EasyDedicated which he controlled, or to which he had access, and  
10 attempt to receive additional malicious code, namely, clickers.

11       230. On or about February 22, 2005, ANCHETA or SoBe caused the  
12 approximately 19,148 bots that had joined the IRC channel #syzt3m#  
13 to be redirected to navigate to an adware server located at  
14 EasyDedicated which ANCHETA controlled, or to which ANCHETA had  
15 access, and attempt to receive additional malicious code, namely,  
16 clickers.

17       231. On or about February 24, 2005, ANCHETA or SoBe caused the  
18 approximately 23,410 bots that had joined the IRC channel #syzt3m#  
19 to be redirected to navigate to an adware server located at  
20 EasyDedicated which ANCHETA controlled, or to which ANCHETA had  
21 access, and attempt to receive additional malicious code, namely,  
22 clickers.

23       232. On or about February 25, 2005, ANCHETA or SoBe caused the  
24 approximately 19,205 bots that had joined the IRC channel #syzt3m#  
25 to be redirected to navigate to an adware server located at  
26 EasyDedicated which ANCHETA controlled, or to which ANCHETA had  
27 access, and attempt to receive additional malicious code, namely,  
28 clickers.

1           233. On or about February 25, 2005, ANCHETA deposited a  
2     \$3,541.31 check from Gammacash into his Wells Fargo Bank account.

3           234. On or about February 27, 2005, ANCHETA caused the  
4     approximately 23,879 bots that had joined the IRC channel #syzt3m#  
5     to be redirected to navigate to an adware server located at  
6     EasyDedicated which ANCHETA controlled, or to which ANCHETA had  
7     access, and attempt to receive additional malicious code, namely,  
8     clickers.

9           235. On or about February 28, 2005, ANCHETA leased a server  
10    from Sago Networks.

11          236. On or about February 28, 2005, ANCHETA transferred  
12    \$156.14 to Sago Networks through Paypal as payment for access to a  
13    server.

14          237. On or about February 28, 2005, ANCHETA caused the topic  
15    in the IRC channel #syzt3m# to change to redirect the  
16    approximately 27,494 bots that had joined the channel to navigate  
17    to a different adware server, namely to the one at Sago Networks he  
18    had just leased, and attempt to receive additional malicious code,  
19    namely, clickers.

20          238. On or about March 1, 2005, ANCHETA caused the  
21    approximately 23,879 bots that had joined the IRC channel #syzt3m#  
22    to be redirected to navigate to an adware server located at Sago  
23    Networks which he controlled, or to which he had access, and  
24    attempt to receive additional malicious code, namely, clickers.

25          239. On or about March 8, 2005, ANCHETA deposited a \$3,188.21  
26    check from Gammacash into his Wells Fargo Bank account.

27          240. On or about March 20, 2005, ANCHETA caused the  
28    approximately 17,957 bots that had joined the IRC channel #syzt3m#

1 to be redirected to navigate to an adware server located at Sago  
2 Networks which he controlled, or to which he had access, and  
3 attempt to receive additional malicious code, namely, clickers.

4 241. On or about March 22, 2005, ANCHETA deposited a \$7,996.10  
5 check from Gammacash into his Wells Fargo Bank account.

6 242. On or about March 23, 2005, ANCHETA caused the  
7 approximately 19,365 bots that had joined the IRC channel #syzt3m#  
8 to be redirected to navigate to an adware server located at Sago  
9 Networks which he controlled, or to which he had access, and  
10 attempt to receive additional malicious code, namely, clickers.

11 243. On or about April 3, 2005, ANCHETA transferred \$185.50 to  
12 Sago Networks through Paypal as payment for access to a server.

13 244. On or about April 5, 2005, ANCHETA deposited a \$6,336.86  
14 check from Gammacash into his Wells Fargo Bank account.

15 245. On or about April 7, 2005, SoBe caused the approximately  
16 14,244 bots that had joined the IRC channel #syzt3m# to be  
17 redirected to navigate to an adware server located at Sago Networks  
18 which ANCHETA controlled, or to which ANCHETA had access, and  
19 attempt to receive additional malicious code, namely, clickers.

20 246. On or about April 16, 2005, ANCHETA or SoBe caused the  
21 approximately 3,636 bots that had joined the IRC channel #syzt3m#  
22 to be redirected to navigate to an adware server located at Sago  
23 Networks which ANCHETA controlled, or to which ANCHETA had access,  
24 and attempt to receive additional malicious code, namely, clickers.

25 247. On or about April 22, 2005, ANCHETA deposited a \$4,010.81  
26 check from Gammacash into his Wells Fargo Bank account.

27 //

28 //



1       248. On or about April 27, 2005, ANCHETA or SoBe caused the  
2 approximately 7,779 bots that had joined the IRC channel #syzt3m#  
3 to be redirected to navigate to an adware server located at Sago  
4 Networks which ANCHETA controlled, or to which ANCHETA had access,  
5 and attempt to receive additional malicious code, namely, clickers.

6       249. On or about May 3, 2005, ANCHETA transferred \$204.00 from  
7 his Wells Fargo Bank account to Sago Networks as payment for access  
8 to a server.

9       250. On or about May 20, 2005, ANCHETA deposited a \$2,750.96  
10 check from Gammacash into his Wells Fargo Bank account.

11       251. On or about June 9, 2005, ANCHETA deposited a \$1,513.46  
12 check from Gammacash into his Wells Fargo Bank account.

13 //

14 //

15 //

16 //

17 //

18 //

19 //

20 //

21 //

22 //

23 //

24 //

25 //

26 //

27 //

28 //

## COUNT FIVE

[18 U.S.C. §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(v), and 1030(b)]

252. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64, as well as paragraphs 98, 113, 114, 144 through 251 of this Indictment.

253. Beginning at least as early as December 13, 2004, and continuing through at least as late as January 26, 2005, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA knowingly caused the transmission of a program, information, code and command, and as a result of such conduct, intentionally caused damage without authorization to a protected computer used in interstate and foreign commerce and communication, namely, defendant JEANSON JAMES ANCHETA knowingly caused the transmission of malicious code to protected computers belonging to the China Lake Naval Air Facility that directed those computers to attempt to connect and connect to an IRC server outside the China Lake Naval Air Facility computer network to await further instructions, which, as a result of such conduct, caused damage affecting a computer system used by and for a government entity in furtherance of the administration of justice, national defense, and national security.

//

//

//

//

//

//

## COUNT SIX

[18 U.S.C. §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(v), and 1030(b)]

254. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64, as well as paragraphs 98, 113, 114, 144 through 251 of this Indictment.

255. Beginning at least as early as January 9, 2005, and continuing through at least as late as February 6, 2005, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA knowingly caused the transmission of a program, information, code and command, and as a result of such conduct, intentionally caused damage without authorization to a computer used in interstate and foreign commerce and communication, namely, defendant JEANSON JAMES ANCHETA knowingly caused the transmission of malicious code to protected computers belonging to the Defense Information Security Agency that directed those computers to attempt to connect and connect to an IRC server outside the Defense Information Security Agency computer network to await further instructions, which, as a result of such conduct, caused damage affecting a computer system used by and for a government entity in furtherance of the administration of justice, national defense, and national security.

//

//

//

//

//

//

**COUNTS SEVEN THROUGH ELEVEN**

[18 U.S.C. §§ 1030(a)(4) and 1030(b)]

256. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64, as well as all of the allegations pertaining to the scheme to defraud set forth in paragraphs 98, 113, 114, 144 through 251 of this Indictment.

257. During on or about the following dates, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA knowingly and with intent to defraud accessed without authorization the following approximate numbers of computers involved in interstate and foreign commerce and communication, and furthered the intended fraud by installing adware on those computers without notice to or consent from the users of those computers, and by means of such conduct, obtained the following approximate monies from the following advertising service companies:

<u>COUNT</u>	<u>APPROXIMATE DATES</u>	<u>APPROXIMATE NUMBER OF PROTECTED COMPUTERS ACCESSED WITHOUT AUTHORIZATION</u>	<u>APPROXIMATE PAYMENT</u>
SEVEN	November 1, 2004 through November 19, 2004	26,975	\$4,044.26 from Gammacash
EIGHT	November 16, 2004 through December 7, 2004	8,744	\$1,306.52 from LOUDcash
NINE	January 15, 2005 through February 7, 2005	19,934	\$2,988.11 from Gammacash

<u>COUNT</u>	<u>APPROXIMATE DATES</u>	<u>APPROXIMATE NUMBER OF PROTECTED COMPUTERS ACCESSED WITHOUT AUTHORIZATION</u>	<u>APPROXIMATE PAYMENT</u>
TEN	March 1, 2005 through March 22, 2005	53,321	\$7,996.10 from Gammacash
ELEVEN	April 1, 2005 through April 22, 2005	28,066	\$4,010.81 from Gammacash

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//



**COUNTS TWELVE THROUGH SIXTEEN**

[18 U.S.C. § 1956(a) (1) (A) (i)]

258. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64, as well as all of the allegations set forth in paragraphs 98, 113, 114, 144 through 258.

259. On or about the following dates, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA knowingly conducted the following financial transactions that involved the transfer of proceeds of specified unlawful activity, namely accessing protected computers to conduct fraud in violation of 18 U.S.C. §§ 1030(a) (4) and 1030(b), as alleged in Counts Seven through Eleven of this Indictment, which financial transactions affected interstate and foreign commerce, knowing that the property involved in each of the financial transactions represented the proceeds of some form, though not necessarily which form, of unlawful activity constituting a felony under federal, state, or foreign law, and with the intent to promote the carrying on of specified unlawful activity, namely, the transfer of payments to Internet hosting companies for access to the servers used to commit the intended fraud, as follows:

<u>COUNT</u>	<u>APPROXIMATE DATE</u>	<u>APPROXIMATE AMOUNT</u>	<u>FINANCIAL TRANSACTION</u>
TWELVE	November 23, 2004	\$149.00	Transfer of funds from Wells Fargo Bank to FDCServers

<u>COUNT</u>	<u>APPROXIMATE DATE</u>	<u>APPROXIMATE AMOUNT</u>	<u>FINANCIAL TRANSACTION</u>
THIRTEEN	December 20, 2004	\$149.00	Transfer of funds from Wells Fargo Bank to FDCServers
FOURTEEN	February 28, 2005	\$157.14	Transfer of funds from Wells Fargo Bank to Sago Networks
FIFTEEN	April 3, 2005	\$185.50	Transfer of funds from Wells Fargo Bank to Sago Networks
SIXTEEN	May 3, 2005	\$204.00	Transfer of funds from Wells Fargo Bank to Sago Networks

//

//

//

//

//

//

//

//

//

//

//

//

//

//

**COUNT SEVENTEEN**

[18 U.S.C. § 982 and 21 U.S.C. § 853]

260. For the purpose of alleging forfeiture pursuant to Title 18, United States Code, Section 982, and Title 21, United States Code, Section 853, the Grand Jury hereby repeats and re-alleges each and every allegation of Counts One through Sixteen of this Indictment.

261. Pursuant to Title 18, United States Code, Section 982(a), defendant JEANSON JAMES ANCHETA, if convicted of one or more of the offenses alleged in Counts One through Sixteen, shall forfeit to the United States the following property:

a. All right, title, and interest in any and all property involved in each offense, or conspiracy to commit such offense, for which the defendant is convicted, and all property traceable to such property, including the following:

(1) the approximately \$2,989.81 in proceeds generated from the sale of bots and proxies, as alleged in Counts One through Three of the Indictment, and deposited into Wells Fargo Bank accounts ending in the numbers 8032 and 7644 and linked to Paypal account resjames@sbcglobal.net;

(2) the approximately \$58,357.86 in proceeds generated from the surreptitious install of adware on protected computers accessed without authorization, as alleged in Counts Four through Eleven of the Indictment, and deposited into a Wells Fargo Bank account ending in the numbers 8032 and 7644 and linked to Paypal account resjames@sbcglobal.net;

(3) a 1993 BMW 325is, Vehicle Identification Number WBABF4318PEK09502, California license plate number j4m3zzz, which

1 defendant JEANSON JAMES ANCHETA purchased on or about October 25,  
2 2004 and improved thereafter with proceeds generated from the  
3 offenses alleged in Counts One through Eleven of the Indictment;

4 b. all money or other property that was the subject of  
5 each transaction, transportation, transmission or transfer in  
6 violation of Title 18, United States Code, Section  
7 1956(a) (1) (A) (i), as alleged in Counts Twelve through Sixteen;  
8 and

9 c. all property used in any manner or part to commit or  
10 to facilitate the commission of those violations, including the  
11 following:

12 (1) one generic tower desktop computer containing a  
13 single internal hard disk, seized from the residence of defendant  
14 JEANSON JAMES ANCHETA on or about December 10, 2004;

15 (2) one IBM 2628 laptop computer, serial number 78-  
16 FFT63, seized from the residence of defendant JEANSON JAMES ANCHETA  
17 on or about December 10, 2004; and

18 (3) one Toshiba laptop computer, model number  
19 A7552212, serial number 35239783K seized from the residence of  
20 defendant JEANSON JAMES ANCHETA on or about May 26, 2005.

21 262. If, as a result of any act or omission by  
22 defendant JEANSON JAMES ANCHETA any of the foregoing money and  
23 property (a) cannot be located by the exercise of due diligence;  
24 (b) has been transferred, or sold to, or deposited with, a third  
25 party; (c) has been placed beyond the jurisdiction of the Court;  
26 (d) has been substantially diminished in value; or (e) has been  
27 commingled with other property that cannot be subdivided without  
28 difficulty, then any other property or interests of defendant

1 JEANSON JAMES ANCHETA, up to the value of the money and property  
2 described in the preceding paragraph of this Indictment, shall be  
3 subject to forfeiture to the United States.

4 A TRUE BILL

5  
6  
7 Foreperson

8  
9 DEBRA WONG YANG  
United States Attorney

10  
11 THOMAS P. O'BRIEN  
Assistant United States Attorney  
12 Chief, Criminal Division

13  
14 JAMES M. AQUILINA  
Assistant United States Attorney  
15 Cyber and Intellectual Property Crimes Section  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28





P-SEND

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

CRIMINAL MINUTES - GENERAL

SCANNED

Case No. CR 05-1060-RGK Date May 8, 2006

Present: The Honorable R. GARY KLAUSNER, UNITED STATES DISTRICT JUDGE

Interpreter None

Sharon L. Williams

Deputy Clerk

Margaret Babykin

Court Reporter/Recorder, Tape No.

James Aquilina

Assistant U.S. Attorney

<u>U.S.A. v. Defendant(s):</u>	<u>Present</u>	<u>Cust.</u>	<u>Bond</u>	<u>Attorneys for Defendants:</u>	<u>Present</u>	<u>App.</u>	<u>Ret.</u>
JEANSON JAMES ANCHETA	X	X		Greg Wesley, DFPD	X	X	

**Proceedings: SENTENCING**

Court and counsel confer. Counsel present argument. Defendant addresses the Court. The Court proceeds with sentencing.

It is ordered that the defendant shall pay to the United States a special assessment of \$400, which is due immediately.

The defendant shall comply with General Order 01-05.

Pursuant to U.S.S.G. Section 5E1.2(e) of the Guidelines, all fines are waived as it is found that the defendant does not have the ability to pay a fine.

It is ordered that the defendant shall pay restitution in the total amount of \$14,611.54 pursuant to 18 USC 3663A.

The amount of restitution ordered shall be paid as follows:

Victim	Amount
Defense Information System Agency	\$4,337.94

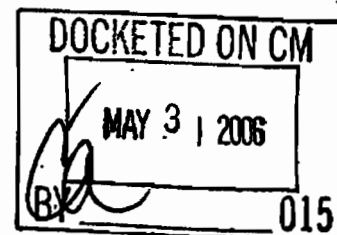
Western Field Office

26722 Plaza Street, Suite 130

Mission Viejo, CA 92691

Attn: Robert Young, Defense Criminal Investigative Service, Computer Crimes Coordinator

AND



P-SEND

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

CRIMINAL MINUTES - GENERAL

China Lake \$10,273.60  
Information Assurance Division  
NAVARWD, China Lake, CA  
Code 7266000D  
Attn: Juanita Martin, Incident Response Handler

23  
11  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30

Restitution shall be paid as ordered by the U.S. Probation Office.

Pursuant to the Sentencing Reform Act of 1984, it is the judgment of the Court that the defendant, Jeanson James Ancheta, is hereby committed on Counts One, Four, Five and 10 of the Indictment to the custody of the Bureau of Prisons to be imprisoned for a term of FIFTY-SEVEN (57) months. This term consists of 57 months on each of Counts One, Four, Five, and Ten of the Indictment to be served concurrently.

Upon release from imprisonment, the defendant shall be placed on supervised release for a term of THREE (3) years under the following terms and conditions. This term consists of three years on each of Counts One, Four, Five and Ten, all such terms to run concurrently.

1. The defendant shall comply with the rules and regulations of the U.S. Probation Office and General Order 318;
2. The defendant shall refrain from any unlawful use of a controlled substance. The defendant shall submit to one drug test within 15 days of release from imprisonment/placement on probation and at least two periodic drug tests thereafter, not to exceed eight tests per month, as directed by the Probation Officer;
3. During the period of community supervision the defendant shall pay the special assessment and restitution in accordance with this judgment's orders pertaining to such payment;
4. The defendant shall cooperate in the collection of a DNA sample from the defendant.
5. The defendant shall use only those computers and computer-related devices, screen user names, passwords, email accounts, and internet service providers (ISPs), as approved by the Probation Officer. Computers and computer-related devices include, but are not limited to, personal computers, personal data assistants (PDAs), internet appliances, electronic games, and cellular telephones, as well as their peripheral equipment, that can access, or can be modified to access, the internet, electronic bulletin boards, and other computers, or similar media;
6. All computers, computer-related devices, and their peripheral equipment, used by the defendant, shall be subject to search and seizure and the installation of search and/or monitoring software and/or hardware, including unannounced seizure for the purpose of search. The defendant shall not add, remove, upgrade, update, reinstall, repair, or otherwise modify the hardware or software on the computers, computer-related devices, or their peripheral equipment, nor shall he/she hide

P-SEND

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

CRIMINAL MINUTES - GENERAL

or encrypt files or data without prior approval of the Probation Officer. Further, the defendant shall provide all billing records, including telephone, cable, internet, satellite, and the like, as requested by the Probation Officer; and

7. The defendant shall not possess or use a computer with access to any online service at any location (including his/her place of employment), without the prior approval of the Probation Officer. This includes access through any internet service provider, bulletin board system, or any public or private computer network system. The defendant shall not have another individual access the internet on his/her behalf to obtain files or information which he/she has been restricted from accessing himself/herself, or accept restricted files or information from another person.

All remaining counts are dismissed.

The Court recommends designation to a Bureau of Prisons facility in Southern California.

**IT IS SO ORDERED.**

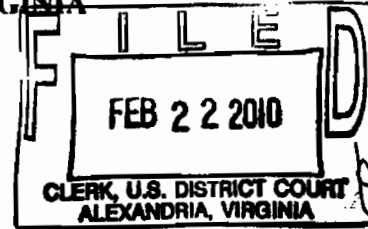
\_\_\_\_\_ : 20  
Initials of Deputy slw  
Clerk \_\_\_\_\_

cc: FISCAL ✓  
USPO ✓  
PSA - LA ✓  
USM - LA ✓





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



MICROSOFT CORPORATION, a  
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-27, CONTROLLING A  
COMPUTER BOTNET THEREBY  
INJURING MICROSOFT AND ITS  
CUSTOMERS

Defendants.

Civil Action No: 1:10 cv 156 (LMB/JFA)

**EX PARTE TEMPORARY RESTRAINING ORDER AND  
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiff Microsoft Corp. ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030), (2) the CAN-SPAM Act (15 U.S.C. § 7704), (3) the Electronic Communications Privacy Act (18 U.S.C. § 2701), (4) the Lanham Act (15 U.S.C. §§ 1125(a), (c)), and (5) the common law of trespass, unjust enrichment and conversion. Microsoft has moved *ex parte* for an emergency temporary restraining order and for 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.

**FINDINGS**

The Court has considered the pleadings, declarations, exhibits, and memoranda filed in support of Microsoft's motion and finds that:

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 relief may be granted against the Defendants under the 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 Lanham Act (15 U.S.C. § 1125) and the common law of trespass to chattels, unjust enrichment and conversion;

2. 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), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125) and the common law of trespass to chattels, unjust enrichment and conversion, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. There is good cause to believe that, unless the Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations of the 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 Lanham Act (15 U.S.C. § 1125) and the common law of trespass to chattels, unjust enrichment and conversion. The evidence set forth in Microsoft's Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Motion"), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing laws by: intentionally accessing and sending malicious code to Microsoft's and its customers' protected computers and operating systems, without authorization, in order to infect those computers and make them part of the botnet, sending malicious code to configure, deploy and operate a botnet, sending unsolicited spam email to Microsoft's Hotmail accounts, sending unsolicited spam email that falsely indicate that they are from Microsoft's Hotmail accounts, collecting personal information including personal email addresses, and delivering malicious code including fake and misleading antivirus software. There is good cause to believe that such if such conduct continues, irreparable harm will occur to Microsoft, its customers 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;

4. 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 domains at issue in Microsoft's TRO Motion and other discoverable evidence of Defendants' misconduct available through such domains if the Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Motion and accompanying declarations and exhibits, Microsoft is likely to be able to prove that: (1) the Defendants are engaged in activities that directly violate U.S. law and harms Microsoft, its customers and the public; (2) the Defendants have continued their unlawful conduct despite the clear injury to Microsoft, its customers and the public; (3) the Defendants are likely to relocate the domains at issue in Microsoft's TRO Motion and the harmful and malicious code disseminated through these domains and to warn its associates engaged in such activities if informed of Microsoft's action. Microsoft's request for this emergency *ex parte* relief is not the result of any lack of diligence on Microsoft's part, but instead is based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b) and Civil L.R. 65-1, good cause and the interests of justice require that this Order be Granted without prior notice to the Defendants, and, accordingly, Microsoft is relieved of the duty to provide the Defendants with prior notice of Microsoft's motion;

5. There is good cause to believe that the Defendants have engaged in illegal activity using .com Domains which are maintained by the top level domain registry Verisign, located in the United States and the Eastern District of Virginia.

6. There is good cause to believe that to immediately halt the injury caused by Defendants, Verisign must be ordered:

a. to immediately take all steps necessary to lock at the registry level the domains at

issue in the TRO Motion, and which are set forth at Appendix A hereto, to ensure that changes to the domain names cannot be made absent a court order;

- b. to immediately take all steps required to propagate to the foregoing domain registry changes to domain name registrars; and
- c. to hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.

7. 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 circumstance 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 contact information in the U.S., (2) personal delivery through the Hague Convention on Service Abroad upon defendants who provided contact information in China, (3) transmission by e-mail, facsimile and mail to the contact information provided by defendants to their domain name registrars and as agreed to by defendants in their domain name registration agreements, (4) publishing notice on a publicly available Internet website.

**TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE**

**IT IS THEREFORE ORDERED** that, Defendants and its representatives are temporarily restrained and enjoined from intentionally accessing and sending malicious code to Microsoft's and its customers' protected computers and operating systems, without authorization, in order to infect those computers and make them part of the botnet, sending malicious code to configure, deploy and operate a botnet, sending unsolicited spam email to Microsoft's Hotmail accounts, sending unsolicited spam email that falsely indicate that they are from Microsoft's Hotmail accounts, collecting personal information



including personal email addresses, and delivering malicious code including fake antivirus software, or undertaking any similar activity that inflicts harm on Microsoft, its customers or the public.

**IT IS FURTHER ORDERED** that, Defendants and its representatives are temporarily restrained and enjoined from configuring, deploying, operating or otherwise participating in or otherwise facilitating the botnet described in the TRO Motion, including but not limited to the domains at issue in the TRO motion and any other component or element of the botnet.

**IT IS FURTHER ORDERED** that Verisign must:

- a. immediately take all steps necessary to lock at the registry level the domains at issue in the TRO Motion, and which are set forth at Appendix A hereto, to ensure that changes to the domain names cannot be made absent a court order;
- b. immediately take all steps required to propagate to the foregoing domain registry changes to domain name registrars; and
- c. hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.

**IT IS FURTHER ORDERED** 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 in China, (3) by transmission by e-mail, facsimile and mail to the contact information provided by defendants to their domain name registrars and as agreed to by defendants in their domain name registration agreements, (4) by publishing notice on a publicly available Internet website.

**IT IS FURTHER ORDERED** that the Temporary Restraining Order granted herein shall expire on March 8, 2010 at 9:00 a.m., unless within such time, the Order, for good cause shown, is extended for an additional period not to exceed fourteen (14) days, or unless it is further extended pursuant to Federal



Rule of Civil Procedure 65.

**IT IS FURTHER ORDERED**, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on March 8, 2010, at 9:00 a.m., to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this order.

**IT IS FURTHER ORDERED** that the Defendants shall file with the Court and serve on Microsoft's 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 Microsoft's request for a preliminary injunction. Microsoft may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the 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. (Eastern Standard Time) on the appropriate dates listed in this paragraph.

**IT IS FURTHER ORDERED** that Microsoft shall maintain its bond in the amount of \$ \$54,600.<sup>00</sup>, as payment of damages to which Defendants may be entitled for a wrongful injunction or restraint, during the pendency of this Action, or until further Order of the Court.

**IT IS SO ORDERED**

*/s/ LMB*  
\_\_\_\_\_  
Leonie M. Brinkema  
United States District Judge

Entered this 22<sup>ND</sup> day of February, 2010.

**Appendix A**

1. bestchristmascard.com
2. bestmirabella.com
3. bestyearcard.com
4. blackchristmascard.com
5. cardnewyear.com
6. cheapdecember.com
7. christmaslightsnow.com
8. decemberchristmas.com
9. directchristmasgift.com
10. eternalgreetingcard.com
11. freechristmassite.com
12. freechristmasworld.com
13. freedecember.com
14. funnychristmasguide.com
15. greatmirabellasite.com
16. greetingcardcalendar.com
17. greetingcardgarb.com
18. greetingguide.com
19. greetingsupersite.com
20. holidayxmas.com
21. itsfatherchristmas.com
22. justchristmasgift.com
23. lifegreetingcard.com
24. livechristmascard.com
25. livechristmasgift.com
26. mirabellaclub.com
27. mirabellamotors.com
28. mirabellanews.com
29. mirabellaonline.com
30. newlifeyearsite.com
31. newmediayearguide.com
32. newyearcardcompany.com
33. newyearcardfree.com
34. newyearcardonline.com
35. newyearcardservice.com
36. smartcardgreeting.com
37. superchristmasday.com
38. superchristmaslights.com
39. superyearcard.com
40. themirabelladirect.com
41. themirabellaguide.com
42. themirabellahome.com
43. topgreetingsite.com
44. whitewhitechristmas.com
45. worldgreetingcard.com
46. yourchristmaslights.com
47. yourdecember.com
48. yourmirabelladirect.com
49. yourregards.com
50. youryearcard.com
51. bestbarack.com
52. bestbaracksite.com
53. bestobamadirect.com
54. expowale.com
55. greatbarackguide.com
56. greatobamaguide.com
57. greatobamaonline.com
58. jobarack.com
59. superobamadirect.com
60. superobamaonline.com
61. thebaracksite.com
62. topwale.com
63. waledirekt.com
64. waleonline.com
65. waleprojekt.com
66. goodnewsdigital.com
67. goodnewsreview.com
68. linkworldnews.com
69. reportradio.com
70. spacemynews.com
71. wapcitynews.com
72. worldnewsdot.com
73. worldnewseye.com
74. worldtracknews.com
75. bestgoodnews.com
76. adorelyric.com
77. adorepoem.com
78. adoresongs.com

- |                              |                               |
|------------------------------|-------------------------------|
| 79. bestadore.com            | 120. greatvalentine.com       |
| 80. bestlovelong.com         | 121. greatvalentinepoems.com  |
| 81. funloveonline.com        | 122. macride.com              |
| 82. youradore.com            | 123. mazdaautomotiveparts.com |
| 83. yourgreatlove.com        | 124. mazdacarclub.com         |
| 84. orldlovelife.com         | 125. mazdaspeedzone.com       |
| 85. romanticsloving.com      | 126. netcitycab.com           |
| 86. adoresong.com            | 127. petcabtaxi.com           |
| 87. bestlovehelp.com         | 128. smartsalesgroup.com      |
| 88. chatloveonline.com       | 129. superpartycab.com        |
| 89. cherishletter.com        | 130. supersalesonline.com     |
| 90. cherishpoems.com         | 131. thecoupondiscount.com    |
| 91. lovecentralonline.com    | 132. themazdacar.com          |
| 92. lovelifeportal.com       | 133. themazdaspeed.com        |
| 93. whocherish.com           | 134. thevalentine lovers.com  |
| 94. worldlovelife.com        | 135. thevalentineparty.com    |
| 95. worshiplove.com          | 136. wirelessvalentineday.com |
| 96. yourteamdoc.com          | 137. workcaredirect.com       |
| 97. yourdatabank.com         | 138. workhomegold.com         |
| 98. alldatanow.com           | 139. worklifedata.com         |
| 99. alldataworld.com         | 140. yourcountycoupon.com     |
| 100. cantiosedata.com        | 141. yourmazdacar.com         |
| 101. freedoconline.com       | 142. yourmazdatribute.com     |
| 102. losenowfast.com         | 143. yourvalentineday.com     |
| 103. mingwater.com           | 144. yourvalentinepoems.com   |
| 104. theworldpool.com        | 145. againstfear.com          |
| 105. wagerpond.com           | 146. antiterroralliance.com   |
| 106. beadcareer.com          | 147. antiterroris.com         |
| 107. beadworkdirect.com      | 148. antiterrornetwork.com    |
| 108. bestcouponfree.com      | 149. bayhousehotel.com        |
| 109. bestmazdadealer.com     | 150. bestblogdirect.com       |
| 110. bluevalentineonline.com | 151. bestbreakingfree.com     |
| 111. buymazdacars.com        | 152. bestjournalguide.com     |
| 112. codecouponsite.com      | 153. bestlifeblog.com         |
| 113. deathtaxi.com           | 154. bestusablog.com          |
| 114. funnyvalentinessite.com | 155. blogginghell.com         |
| 115. greatcouponclub.com     | 156. blogsitedirect.com       |
| 116. greatmazdacars.com      | 157. boarddiary.com           |
| 117. greatsalesavailable.com | 158. breakingfreemichigan.com |
| 118. greatsalesgroup.com     | 159. breakinggoodnews.com     |
| 119. greatsalestax.com       | 160. breakingkingnews.com     |

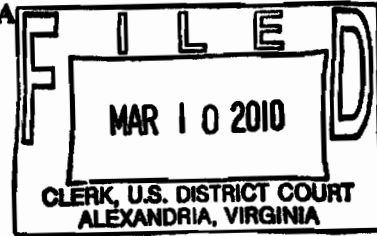
161.	breakingnewsfm.com	202.	virtualesms.com
162.	breakingnewsfild.com	203.	wealthleaf.com
163.	debtbgonesite.com	204.	yourbarrier.com
164.	easyworldnews.com	205.	discountfreesms.com
165.	extendedman.com	206.	eccellentesms.com
166.	farboards.com	207.	freesmsorange.com
167.	fearalert.com	208.	ipersmstext.com
168.	globalantiterror.com	209.	morefreesms.com
169.	gonessite.com	210.	nuovosmsclub.com
170.	longballonline.com	211.	primosmsfree.com
171.	mobilephotoblog.com	212.	smsinlinea.com
172.	photoblogsite.com	213.	smsluogo.com
173.	residencehunter.com	214.	superioresms.com
174.	terroralertstatus.com	215.	4thfirework.com
175.	terrorfear.com	216.	biumer.com
176.	terrorismfree.com	217.	entrunk.com
177.	themostrateblog.com	218.	fireholiday.com
178.	tntbreakingnews.com	219.	fireworksholiday.com
179.	urbanfear.com	220.	fireworksnetwork.com
180.	usabreakingnews.com	221.	fireworkspoint.com
181.	yourbreakingnew.com	222.	freeindependence.com
182.	yourlength.com	223.	gemells.com
183.	yourlol.com	224.	handyphoneworld.com
184.	yourwent.com	225.	happyindependence.com
185.	bakeloaf.com	226.	holidayfirework.com
186.	chinamobilesms.com	227.	holidaysfirework.com
187.	coralarm.com	228.	holifireworks.com
188.	downloadfreesms.com	229.	interactiveindependence.com
189.	freecolorsms.com		
190.	freeservesms.com	230.	miosmschat.com
191.	fryroll.com	231.	movie4thjuly.com
192.	goldfixonline.com	232.	moviefireworks.com
193.	lastlabel.com	233.	movieindependence.com
194.	miosmsclub.com	234.	movies4thjuly.com
195.	moneymedal.com	235.	moviesfireworks.com
196.	nuovosms.com	236.	moviesindependence.com
197.	screenalias.com	237.	outdoorindependence.com
198.	smsclubnet.com	238.	smophi.com
199.	smsdiretto.com	239.	superhandycap.com
200.	smspianeta.com	240.	thehandygal.com
201.	tagdebt.com	241.	video4thjuly.com

- 242. videoindependence.com
- 243. yourhandyhome.com
- 244. yusitymp.com
- 245. aweleon.com
- 246. bedioger.com
- 247. bicodehl.com
- 248. birdab.com
- 249. cismosis.com
- 250. crucism.com
- 251. cyclozo.com
- 252. encybest.com
- 253. favolu.com
- 254. framtr.com
- 255. frostep.com
- 256. gumentha.com
- 257. hindger.com
- 258. hornalfa.com
- 259. noloid.com
- 260. nonprobs.com
- 261. oughwa.com
- 262. painkee.com
- 263. pantali.com
- 264. pathoph.com
- 265. prerre.com
- 266. purgand.com
- 267. rascop.com
- 268. sodanthu.com
- 269. specipa.com
- 270. tabatti.com
- 271. tatumen.com
- 272. thingre.com
- 273. tobeyew.com





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



MICROSOFT CORPORATION, a  
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-27, CONTROLLING A  
COMPUTER BOTNET THEREBY  
INJURING MICROSOFT AND ITS  
CUSTOMERS

Defendants.

Civil Action No: 1:10 CV 156 (LMB/JFA)

**ORDER GRANTING PRELIMINARY INJUNCTION**

Plaintiff Microsoft Corp. ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030), (2) the CAN-SPAM Act (15 U.S.C. § 7704), (3) the Electronic Communications Privacy Act (18 U.S.C. § 2701), (4) the Lanham Act (15 U.S.C. §§ 1125(a), (c)), and (5) the common law of trespass, unjust enrichment and conversion. Microsoft has moved for a preliminary injunction pursuant to Rule 65 of the Federal Rules of Civil Procedure.

**FINDINGS**

The Court has considered the pleadings, declarations, exhibits, and memoranda filed in support of Microsoft's motion and finds that:

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 the Defendants under the 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 Lanham Act (15 U.S.C. § 1125) and the common law of trespass to chattels, unjust enrichment and conversion;

2. 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), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125) and the common law of trespass to chattels, unjust enrichment and conversion, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. There is good cause to believe that, unless the Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations of the 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 Lanham Act (15 U.S.C. § 1125) and the common law of trespass to chattels, unjust enrichment and conversion. The evidence set forth in Microsoft's Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Motion"), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing laws by: intentionally accessing and sending malicious code to Microsoft's and its customers' protected computers and operating systems, without authorization, in order to infect those computers and make them part of the botnet, sending malicious code to configure, deploy and operate a botnet, sending unsolicited spam email to Microsoft's Hotmail accounts, sending unsolicited spam email that falsely indicate that they are from Microsoft's Hotmail accounts, collecting personal information including personal email addresses, and delivering malicious code including fake

and misleading antivirus software. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, its customers 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;

4. 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 domains at issue in Microsoft's TRO Motion and other discoverable evidence of Defendants' misconduct available through such domains if Defendants are not restrained by Order of this Court. Based on the evidence cited in Microsoft's TRO Motion and accompanying declarations and exhibits, Microsoft is likely to be able to prove that: (1) Defendants have operated through businesses and principals located outside of the United States; (2) the Defendants are engaged in activities that directly violate U.S. law and harms Microsoft, its customers and the public; (3) the Defendants have continued their unlawful conduct despite the clear injury to Microsoft, its customers and the public; (4) the Defendants are likely to relocate the domains at issue in Microsoft's TRO Motion and the harmful and malicious code disseminated through these domains if not restrained from doing so by Order of this Court. Therefore, in accordance with Fed. R. Civ. P. 65 and Civil L.R. 65-1, good cause and the interests of justice require that this Order be Granted;

5. There is good cause to believe that the Defendants, which are primarily individuals outside of the United States, have engaged in illegal activity using .com Domains which are maintained by the top level domain registry Verisign, located in the United States and the Eastern District of Virginia.

6. There is good cause to believe that to immediately prevent the injury caused by

Defendants, Verisign must be ordered:

- a. to immediately take all steps necessary to lock at the registry level the domains at issue in the TRO Motion and to remove all such domains from the zone file and to ensure that changes to the domain names cannot be made by Defendants absent a court order;
- b. to immediately take all steps required to propagate the foregoing domain registry changes to domain name registrars; and
- c. to hold the domains in escrow and take all steps necessary to ensure that the evidence of Defendants' misconduct available through the domains be preserved.

7. There is good cause to permit notice of the instant order and service of the Complaint by formal and alternative means, given the exigency of the circumstance 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 U.S. defendants, (2) personal delivery through the Hague Convention on Service Abroad upon Chinese defendants, (3) transmission by e-mail, facsimile and mail to the contact information provided by defendants to their domain name registrars and as agreed to by defendants in their domain name registration agreements, and (4) publication, including publishing notice on a publicly available Internet website.

**PRELIMINARY INJUNCTION**

**IT IS THEREFORE ORDERED** that, Defendants and its representatives are restrained and enjoined during the pendency of this action from intentionally accessing and sending



malicious code to Microsoft's and its customers' protected computers and operating systems, without authorization, in order to infect those computers and make them part of the botnet, sending malicious code to configure, deploy and operate a botnet, sending unsolicited spam email to Microsoft's Hotmail accounts, sending unsolicited spam email that falsely indicate that they are from Microsoft's Hotmail accounts, collecting personal information including personal email addresses, and delivering malicious code including fake antivirus software, or undertaking any similar activity that inflicts harm on Microsoft, its customers or the public.

**IT IS FURTHER ORDERED** that, Defendants and its representatives are restrained and enjoined during the pendency of this action from configuring, deploying, operating or otherwise participating in or otherwise facilitating the botnet described in the TRO Motion, including but not limited to the domains set forth at Appendix A hereto and any other component or element of the botnet.

**IT IS FURTHER ORDERED** that during the pendency of this action Verisign must:

- a. take all steps necessary to lock at the registry level the domains at issue in the TRO Motion and to remove all such domains from the zone file and to ensure that changes to the domain names cannot be made by Defendants absent a court order;
- b. take all steps required to propagate the foregoing domain registry changes to domain name registrars; and
- c. hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.


**IT IS FURTHER ORDERED** that copies of this Order and service of the Complaint may be carried out 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 in China, (3) by transmission by e-mail, facsimile and mail to the contact information provided by defendants to their domain name registrars and as agreed to by defendants in their domain name registration agreements, and (4) publication, including publishing notice on a publicly available Internet website.

**IT IS FURTHER ORDERED** that Microsoft shall maintain during the pendency of this action the bond it has posted in the amount of \$55,400, as payment of damages to which Defendants may be entitled for a wrongful injunction or restraint, during the pendency of this Action, or until further Order of the Court.

**IT IS SO ORDERED**

Entered this <sup>th</sup>10 day of March, 2010.

  
\_\_\_\_\_  
Leonie M. Brinkema  
United States District Judge

Appendix A

1. bestchristmascard.com
2. bestmirabella.com
3. bestyearcard.com
4. blackchristmascard.com
5. cardnewyear.com
6. cheapdecember.com
7. christmaslightsnow.com
8. decemberchristmas.com
9. directchristmasgift.com
10. eternalgreetingcard.com
11. freechristmassite.com
12. freechristmasworld.com
13. freedecember.com
14. funnychristmasguide.com
15. greatmirabellasite.com
16. greetingcardcalendar.com
17. greetingcardgarb.com
18. greetingguide.com
19. greetingsupersite.com
20. holidayxmas.com
21. itsfatherchristmas.com
22. justchristmasgift.com
23. lifegreetingcard.com
24. livechristmascard.com
25. livechristmasgift.com
26. mirabellaclub.com
27. mirabellamotors.com
28. mirabellaneews.com
29. mirabellaonline.com
30. newlifeyearsite.com
31. newmediayearguide.com
32. newyearcardcompany.com
33. newyearcardfree.com
34. newyearcardonline.com
35. newyearcardservice.com
36. smartcardgreeting.com
37. superchristmasday.com
38. superchristmaslights.com
39. superyearcard.com
40. themirabelladirect.com
41. themirabellaguide.com
42. themirabellahome.com
43. topgreetingsite.com
44. whitewhltechristmas.com
45. worldgreetingcard.com
46. yourchristmaslights.com
47. yourdecember.com
48. yourmirabelladirect.com
49. yourregards.com
50. youryearcard.com
51. bestbarack.com
52. bestbaracksite.com
53. bestobamadirect.com
54. expowale.com
55. greatbarackguide.com
56. greatobamaguide.com
57. greatobamaonline.com
58. jobarack.com
59. superobamadirect.com
60. superobamaonline.com
61. thebaracksite.com
62. topwale.com
63. waledirekt.com
64. waleonline.com
65. waleprojekt.com
66. goodnewsdigital.com
67. goodnewsreview.com
68. linkworldnews.com
69. reportradio.com
70. spacemynews.com
71. wapcitynews.com
72. worldnewsdot.com
73. worldnewseye.com
74. worldtracknews.com
75. bestgoodnews.com
76. adorelyric.com

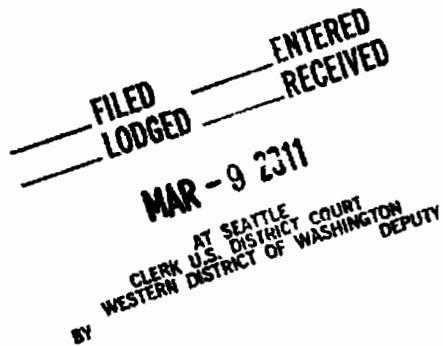
- |                              |                               |
|------------------------------|-------------------------------|
| 77. adorepoem.com            | 118. greatsalesgroup.com      |
| 78. adoresongs.com           | 119. greatsalestax.com        |
| 79. bestadore.com            | 120. greatsvalentine.com      |
| 80. bestlovelong.com         | 121. greatvalentinepoems.com  |
| 81. funloveonline.com        | 122. macride.com              |
| 82. youradore.com            | 123. mazdaautomotiveparts.com |
| 83. yourgreatlove.com        | 124. mazdacarclub.com         |
| 84. orldlovelife.com         | 125. mazdaspeedzone.com       |
| 85. romanticsloving.com      | 126. netcitycab.com           |
| 86. adoresong.com            | 127. petcabtaxi.com           |
| 87. bestlovehelp.com         | 128. smartsalesgroup.com      |
| 88. chatloveonline.com       | 129. superpartycab.com        |
| 89. cherishletter.com        | 130. supersalesonline.com     |
| 90. cherishpoems.com         | 131. thecoupondiscount.com    |
| 91. lovecentralonline.com    | 132. themazdacar.com          |
| 92. lovelifeportal.com       | 133. themazdaspeed.com        |
| 93. whocherish.com           | 134. thevalentineovers.com    |
| 94. worldlovelife.com        | 135. thevalentineparty.com    |
| 95. worshiplove.com          | 136. wirelessvalentineday.com |
| 96. yourteamdoc.com          | 137. workcaredirect.com       |
| 97. yourdatabank.com         | 138. workhometogold.com       |
| 98. alldatanow.com           | 139. worklifedata.com         |
| 99. alldataworld.com         | 140. yourcountycoupon.com     |
| 100. cantlosedata.com        | 141. yourmazdacar.com         |
| 101. freedoconline.com       | 142. yourmazdatribute.com     |
| 102. losenowfast.com         | 143. yourvalentineday.com     |
| 103. mingwater.com           | 144. yourvalentinepoems.com   |
| 104. theworldpool.com        | 145. againstfear.com          |
| 105. wagerpond.com           | 146. antiterroralliance.com   |
| 106. beadcareer.com          | 147. antiterroris.com         |
| 107. beadworkdirect.com      | 148. antiterrornetwork.com    |
| 108. bestcouponfree.com      | 149. bayhousehotel.com        |
| 109. bestmazdadealer.com     | 150. bestblogdirect.com       |
| 110. bluevalentineonline.com | 151. bestbreakingfree.com     |
| 111. buymazdacars.com        | 152. bestjournalguides.com    |
| 112. codecouponsite.com      | 153. bestlifeblog.com         |
| 113. deathtaxi.com           | 154. bestusablog.com          |
| 114. funnyvalentinessite.com | 155. blogginhell.com          |
| 115. greatcouponclub.com     | 156. blogsiteidirect.com      |
| 116. greatmazdacars.com      | 157. boarddiary.com           |
| 117. greatsalesavailable.com | 158. breakingfreemichigan.com |

- |      |                       |      |                             |
|------|-----------------------|------|-----------------------------|
| 159. | breakinggoodnews.com  | 200. | smspaneta.com               |
| 160. | breakingkingnews.com  | 201. | tagdebt.com                 |
| 161. | breakingnewsfm.com    | 202. | virtualesms.com             |
| 162. | breakingnewsitd.com   | 203. | wealthleaf.com              |
| 163. | debtbgonesite.com     | 204. | yourbarrier.com             |
| 164. | easyworldnews.com     | 205. | discountfreesms.com         |
| 165. | extendedman.com       | 206. | eccellentesms.com           |
| 166. | farboards.com         | 207. | freesmsorange.com           |
| 167. | fearalert.com         | 208. | ipersmstext.com             |
| 168. | globalantiterror.com  | 209. | morefreesms.com             |
| 169. | gonesite.com          | 210. | nuovosmsclub.com            |
| 170. | longballonline.com    | 211. | primosmsfree.com            |
| 171. | mobilephotoblog.com   | 212. | smsinlinea.com              |
| 172. | photoblogsite.com     | 213. | smsluogo.com                |
| 173. | residencehunter.com   | 214. | superloresms.com            |
| 174. | terroralertstatus.com | 215. | 4thfirework.com             |
| 175. | terrorfear.com        | 216. | blumer.com                  |
| 176. | terrorismfree.com     | 217. | entranc.com                 |
| 177. | themostrateblog.com   | 218. | fireholiday.com             |
| 178. | tntbreakingnews.com   | 219. | fireworksholiday.com        |
| 179. | urbanfear.com         | 220. | fireworksnetwork.com        |
| 180. | usabreakingnews.com   | 221. | fireworkspoint.com          |
| 181. | yourbreakingnew.com   | 222. | freeindependence.com        |
| 182. | yourlength.com        | 223. | gemells.com                 |
| 183. | yourlol.com           | 224. | handyphoneworld.com         |
| 184. | yourwent.com          | 225. | happyindependence.com       |
| 185. | bakeloaf.com          | 226. | holidayfirework.com         |
| 186. | chinamobilesms.com    | 227. | holidaysfirework.com        |
| 187. | coralarm.com          | 228. | holifireworks.com           |
| 188. | downloadfreesms.com   | 229. | interactiveindependence.com |
| 189. | freecolorsms.com      | 230. | miosmschat.com              |
| 190. | freeservesms.com      | 231. | movie4thjuly.com            |
| 191. | fryroll.com           | 232. | moviefireworks.com          |
| 192. | goldfixonline.com     | 233. | movieindependence.com       |
| 193. | lastlabel.com         | 234. | movies4thjuly.com           |
| 194. | miosmsclub.com        | 235. | moviesfireworks.com         |
| 195. | moneymedal.com        | 236. | moviesindependence.com      |
| 196. | nuovosms.com          | 237. | outdoorindependence.com     |
| 197. | screenalias.com       | 238. | smophi.com                  |
| 198. | smsclubnet.com        | 239. | superhandycap.com           |
| 199. | smsdiretto.com        | 240. | thehandygai.com             |



- 241. video4thjuly.com
- 242. videoindependence.com
- 243. yourhandyhome.com
- 244. yusltymp.com
- 245. aweleon.com
- 246. bedioger.com
- 247. bicodehl.com
- 248. blrdab.com
- 249. clsmosis.com
- 250. crucism.com
- 251. cycloro.com
- 252. encybest.com
- 253. favolu.com
- 254. framtr.com
- 255. frostep.com
- 256. gumentha.com
- 257. hindger.com
- 258. homalfa.com
- 259. nolold.com
- 260. nonprobs.com
- 261. oughwa.com
- 262. painkee.com
- 263. pantall.com
- 264. pathoph.com
- 265. prerre.com
- 266. purgand.com
- 267. rascop.com
- 268. sodanthu.com
- 269. specipa.com
- 270. tabatti.com
- 271. tatumen.com
- 272. thingre.com
- 273. tobeyew.com
- 274. broadwo.com
- 275. houreena.com
- 276. cyanian.com





The Honorable James L. Robart

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

MICROSOFT CORPORATION,

Plaintiff,

v.

JOHN DOES 1-11 CONTROLLING A  
COMPUTER BOTNET THEREBY  
INJURING MICROSOFT AND ITS  
CUSTOMERS,

Defendants.

Case No. 2:11-cv-00222

**SECOND AMENDED [PROPOSED]  
EX PARTE TEMPORARY  
RESTRAINING ORDER, SEIZURE  
ORDER AND ORDER TO SHOW  
CAUSE RE PRELIMINARY  
INJUNCTION**

**\*\*FILED UNDER SEAL\*\***

Plaintiff Microsoft Corporation ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the CAN-SPAM Act (15 U.S.C. § 7704); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (4) the common law of trespass, conversion and unjust enrichment. Microsoft has 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 Microsoft's Application for *Ex Parte* Temporary Restraining Order, *Ex Parte* Seizure and Order

SECOND AMENDED [PROPOSED] EX PARTE  
TEMPORARY RESTRAINING ORDER, SEIZURE  
ORDER AND ORDER TO SHOW CAUSE RE  
PRELIMINARY INJUNCTION

Orrick Herrington & Sutcliffe LLP  
701 5th Avenue, Suite 5500  
Seattle, Washington 98104-7097  
tel+1-206-839-4300

1 to Show Cause Re Preliminary Injunction ("TRO Application"), the Court hereby makes the  
2 following findings of fact and conclusions of law:

3 1. This Court has jurisdiction over the subject matter of this case and there is good  
4 cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim  
5 upon which relief may be granted against the Defendants under the Computer Fraud and Abuse  
6 Act (18 U.S.C. § 1030); CAN-SPAM Act (15 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§  
7 1114, 1125); and the common law of trespass to chattels, conversion and unjust enrichment.

8 2. Microsoft owns the registered trademarks "Microsoft," "Windows," and "Hotmail"  
9 used in connection with its services, software, and products.

10 3. There is good cause to believe that Defendants have engaged in and are likely to  
11 engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030);  
12 CAN-SPAM Act (15 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§ 1114, 1125); and the  
13 common law of trespass to chattels, conversion and unjust enrichment, and that Microsoft is,  
14 therefore, likely to prevail on the merits of this action.

15 4. There is good cause to believe that, unless the Defendants are restrained and  
16 enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants'  
17 ongoing violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030); CAN-SPAM Act  
18 (15 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§ 1114, 1125); and the common law of trespass  
19 to chattels, conversion and unjust enrichment. The evidence set forth in Microsoft's Application  
20 for an Emergency Temporary Restraining Order, Seizure Order and Order to Show Cause Re  
21 Preliminary Injunction ("TRO Motion"), and the accompanying declarations and exhibits,  
22 demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in  
23 violations of the foregoing laws by: (1) intentionally accessing and sending malicious software to  
24 Microsoft's and its customers' protected computers and operating systems, without authorization,  
25 in order to infect those computers and make them part of the botnet; (2) sending malicious  
26 software to configure, deploy and operate a botnet; (3) sending unsolicited spam e-mail to  
27 Microsoft's Hotmail accounts; and (4) sending unsolicited spam e-mails that falsely indicate that  
28 they are from or approved by Microsoft and that promote counterfeit pharmaceuticals and other

1 fraudulent schemes. There is good cause to believe that if such conduct continues, irreparable  
2 harm will occur to Microsoft and the public, including Microsoft's customers. There is good  
3 cause to believe that the Defendants will continue to engage in such unlawful actions if not  
4 immediately restrained from doing so by Order of this Court.

5         5. There is good cause to believe that immediate and irreparable damage to this  
6 Court's ability to grant effective final relief will result from the sale, transfer, or other disposition  
7 or concealment by Defendants of the botnet command and control software that is hosted at and  
8 otherwise operates through the Internet Protocol (IP) addresses listed in Appendix A and the  
9 Internet domains at issue in Microsoft's TRO Application and from the destruction or  
10 concealment of other discoverable evidence of Defendants' misconduct available at those  
11 locations if the Defendants receive advance notice of this action. Based on the evidence cited in  
12 Microsoft's TRO Application and accompanying declarations and exhibits, Microsoft is likely to  
13 be able to prove that: (1) the Defendants are engaged in activities that directly violate U.S. law  
14 and harm Microsoft and the public, including Microsoft's customers; (2) the Defendants have  
15 continued their unlawful conduct despite the clear injury to the foregoing interests; (3) the  
16 Defendants are likely to delete or relocate the botnet command and control software at issue in  
17 Microsoft's TRO Application and the harmful, malicious, and trademark infringing software  
18 disseminated through these IP addresses and domains and to warn their associates engaged in such  
19 activities if informed of Microsoft's action. Microsoft's request for this emergency *ex parte* relief  
20 is not the result of any lack of diligence on Microsoft's part, but instead is based upon the nature  
21 of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b) and 15  
22 U.S.C. § 1116(d), good cause and the interests of justice require that this Order be Granted  
23 without prior notice to the Defendants, and accordingly Microsoft is relieved of the duty to  
24 provide the Defendants with prior notice of Microsoft's motion.

25         6. There is good cause to believe that the Defendants have engaged in illegal activity  
26 using the data centers and/or Internet hosting providers identified in Appendix A to host the  
27 command and control software and the malicious botnet code and content used to maintain and  
28 operate the botnet at computers, servers, electronic data storage devices or media at the IP



1 addresses identified in Appendix A.

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

8 8. There is good cause to believe that to immediately halt the injury caused by  
9 Defendants, and to ensure that future prosecution of this case is not rendered fruitless by attempts  
10 to delete, hide, conceal, or otherwise render inaccessible the software components that distribute  
11 unlicensed copies of Microsoft's registered trademarks and carry out other harmful conduct, with  
12 respect to Defendants' most current, active command and control IP addresses hosted at data  
13 centers operated by ECommerce, Inc.; FDCservers.net, LLC; Wholesale Internet, Inc.; Burstnet  
14 Technologies, Inc. d/b/a Network Operations Center, Inc.; and Softlayer Technologies, Inc., the  
15 United States Marshals Service in the judicial districts where the data centers are located should  
16 be directed to seize, impound and deliver into the custody of third-party escrow service Stroz  
17 Friedberg, 1925 Century Park East, Suite 1350, Los Angeles, CA 90067, all of Defendants'  
18 computers, servers, electronic data storage devices, software, data or media associated with the IP  
19 addresses listed in Appendix A.

20 9. There is good cause to believe that the Defendants have engaged in illegal activity  
21 using the Internet domains identified at Appendix B to this order to host the command and control  
22 software and content used to maintain and operate the botnet. There is good cause to believe that  
23 to immediately halt the injury caused by Defendants, each of Defendants' current and prospective  
24 domains set forth in Appendix B must be immediately made inaccessible, and/or removed from  
25 the Internet zone file.

26 10. There is good cause to direct that third party data centers, hosting providers and  
27 Internet registries/registrars reasonably assist in the implementation of the Order and refrain from  
28 frustrating the implementation and purposes of this Order, pursuant to 28 U.S.C. § 1651(a) (the

1 All Writs Act).

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

8 12. There is good cause to permit notice of the instant order, notice of the Preliminary  
9 Injunction hearing and service of the Complaint by formal and alternative means, given the  
10 exigency of the circumstances and the need for prompt relief. The following means of service are  
11 authorized by law, satisfy Due Process, satisfy Fed. R. Civ. Pro. 4(f)(3), and are reasonably  
12 calculated to notify defendants of the instant order, the Preliminary Injunction hearing and of this  
13 action: (1) personal delivery upon defendants who provided to the data centers and Internet  
14 hosting providers contact information in the U.S.; (2) personal delivery through the Hague  
15 Convention on Service Abroad or other treaties upon defendants who provided contact  
16 information outside the United States; (3) transmission by e-mail, facsimile, and mail to the  
17 contact information provided by defendants to the data centers, Internet hosting providers, and  
18 domain registrars who host the software code associated with the IP addresses in Appendix A, or  
19 through which domains in Appendix B are registered; and (4) publishing notice to the Defendants  
20 on a publicly available Internet website.

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

24 **TEMPORARY RESTRAINING ORDER AND SEIZURE ORDER**

25 **IT IS THEREFORE ORDERED** as follows:

26 A. Defendants, their representatives and persons who are in active concert or  
27 participation with them are temporarily restrained and enjoined from intentionally accessing and  
28 sending malicious software to Microsoft's and its customers' protected computers and operating

1 systems, without authorization, in order to infect those computers and make them part of the  
2 botnet; sending malicious software to configure, deploy and operate a botnet; sending unsolicited  
3 spam e-mail to Microsoft's Hotmail accounts; and sending unsolicited spam e-mail that falsely  
4 indicate that they are from or approved by Microsoft; or undertaking any similar activity that  
5 inflicts harm on Microsoft or the public, including Microsoft's customers.

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

12 C. Defendants, their representatives and persons who are in active concert or  
13 participation with them are temporarily restrained and enjoined from using the trademarks  
14 "Microsoft," "Windows," "Hotmail," and/or other trademarks; trade names; service marks; or  
15 Internet Domain addresses or names; or acting in any other manner which suggests in any way  
16 that Defendants' products or services come from or are somehow sponsored or affiliated with  
17 Microsoft, and from otherwise unfairly competing with Microsoft, misappropriating that which  
18 rightfully belongs to Microsoft, or passing off their goods as Microsoft's.

19 D. Defendants, their representatives and persons who are in active concert or  
20 participation with them are temporarily restrained and enjoined from infringing Microsoft's  
21 registered trademarks, Registration Nos. 1200236, 2165601, 2463510 and others.

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

28 F. Defendants' materials bearing infringing marks, the means of making the



1 counterfeit marks, and records documenting the manufacture, sale, or receipt of things involved in  
2 such violation, in the possession of data centers operated by ECommerce, Inc., FDCServers.net  
3 LLC, Wholesale Internet, Inc., Burstnet Technologies, Inc., and Softlayer Technologies, Inc., all  
4 pursuant to 15 U.S.C. §1116(d), shall be seized:

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

- 15  
16 a. Northern District of Illinois  
U.S. Marshal: Darryl K. McPherson  
219 S. Dearborn Street, Room 2444  
17 Chicago, IL 60604  
(312) 353-5290
- 18  
19 b. District of Colorado  
U.S. Marshal: John Kammerzell  
U.S. Courthouse  
20 901 19th St., 3rd Floor  
Denver, Co 80294  
21 (303) 335-3400
- 22  
23 c. Middle District of Pennsylvania  
U.S. Marshal: Martin J. Pane (Acting)  
Federal Building  
24 Washington Avenue & Linden Street, Room 231  
Scranton, PA 18501  
25 (570) 346-7277
- 26  
27 d. Western District of Missouri  
U.S. Marshal: C. Mauri Sheer  
U.S. Courthouse  
28 400 E. 9th St., Room 3740  
Kansas City, MO 64106  
(816) 512-2000

- 1  
2 e. Eastern District of Virginia  
3 U.S. Marshal: John R. Hackman  
4 401 Courthouse Square  
5 Alexandria, VA 22314  
6 (703) 837-5500  
7  
8 f. Northern District of Texas  
9 U.S. Marshal: Randy Paul Ely  
10 Federal Building  
11 1100 Commerce Street, Room 16F47  
12 Dallas, TX 75242  
13 (214) 767-0836  
14  
15 g. Western District of Washington  
16 U.S. Marshal: Mark L. Ericks  
17 700 Stewart Street, Suite 9000  
18 Seattle, WA 98101-1271  
19 (206) 370-8600  
20  
21 h. Southern District of Ohio  
22 U.S. Marshal: Cathy Jones  
23 U.S. Courthouse  
24 85 Marconi Boulevard, Room 460  
25 Columbus, OH 43215  
26 (614) 469-5540  
27  
28

2. The United States Marshals and their deputies shall be accompanied by Microsoft's 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 in Paragraph F 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.

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 properties seized 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



1 discharged of his or her duties and responsibilities for safekeeping of the seized materials.

2 4. The United States Marshals accomplishing such seizure are permitted to  
3 enter the premises of the data centers operated by ECommerce, Inc., FDCServers.net LLC,  
4 Wholesale Internet, Inc., Burstnet Technologies, Inc., and Softlayer Technologies, Inc., in order to  
5 serve copies of this Order, carry out the terms of this Order and to verify compliance with this  
6 Order. The United States Marshals shall employ whatever reasonable means are necessary to  
7 carry out the terms of this Order and to inspect the contents of any computers, servers, electronic  
8 data storage devices, media, room, closets, cabinets, vehicles, containers or desks or documents  
9 and to dismantle any equipment utilized by Defendants to carry out the activities prohibited by  
10 this Order.

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

14 1. disable Defendants' IP addresses set forth in Appendix A (including  
15 through any backup systems) so that they can no longer be accessed over the Internet, connected  
16 to, or communicated with in any way except as explicitly provided for in this order;

17 2. disable Defendants' domains set forth in Appendix B so that they can no  
18 longer be accessed over the Internet, connected to, or communicated with in any way except as  
19 explicitly provided for in this order by (1) locking the domains and removing such domains from  
20 the zone file and (2) taking all steps required to propagate the foregoing domain registry changes  
21 to domain name registrars;

22 3. transfer any content and software hosted on Defendants' IP addresses listed  
23 in Appendix A to new IP addresses not listed in Appendix A; notify Defendants and any other  
24 owners of such content or software of the new IP addresses, and direct them to contact  
25 Microsoft's Counsel, Gabriel M. Ramsey, Orrick Herrington & Sutcliffe, 1000 Marsh Road,  
26 Menlo Park, CA 90425-1015, (Tel: 650-614-7400), to facilitate any follow-on action;

27 4. preserve and produce to Microsoft documents and information sufficient to  
28 identify and contact Defendants and Defendants' representatives operating or controlling the IP

1 addresses set forth in Appendix A, including any and all individual or entity names, mailing  
2 addresses, e-mail addresses, facsimile numbers and telephone numbers or similar contact  
3 information, including but not limited to such contact information reflected in billing, usage and  
4 contact records;

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

10 6. refrain from publishing or providing notice or warning of this Order to  
11 Defendants, their representatives or persons who are in active concert or participation with them,  
12 until this Order is fully executed, except as explicitly provided for in this Order.

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

15 **IT IS FURTHER ORDERED** that copies of this Order, notice of the Preliminary  
16 Injunction hearing and service of the Complaint may be served by any means authorized by law,  
17 including (1) by personal delivery upon defendants who provided contact information in the U.S.;  
18 (2) personal delivery through the Hague Convention on Service Abroad upon defendants who  
19 provided contact information outside the U.S.; (3) by transmission by e-mail, facsimile and mail  
20 to the contact information provided by defendants to the data centers, Internet hosting providers  
21 and domain registrars who hosted the software code associated with the IP addresses set forth at  
22 Appendix A or through which domains in Appendix B are registered; and (4) by publishing notice  
23 to Defendants on a publicly available Internet website.

24 **IT IS FURTHER ORDERED**, pursuant to Federal Rule of Civil Procedure 65(b), 15  
25 U.S.C. §1116(d)(10) and 28 U.S.C. § 1651(a) (the All Writs Act) that the Defendants shall appear  
26 before this Court within 28 days from the date of this order, to show cause, if there is any, why  
27 this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against  
28 the Defendants, enjoining them from the conduct temporarily restrained by the preceding

provisions of this Order.

**IT IS FURTHER ORDERED** that Microsoft shall post bond in the amount of \$173,000 as cash to be paid into the Court registry.

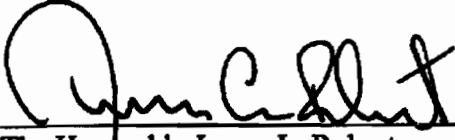
**IT IS FURTHER ORDERED** that Microsoft shall compensate the data centers, Internet hosting providers and/or domain registries identified in Appendices A and B at prevailing rates for technical assistance rendered in implementing the Order.

**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 identified in Appendices A and B consistent with thorough and prompt implementation of this Order. *All actions undertaken under the authority of this Order shall be in strict compliance with 15 U.S.C. § 1116.*

**IT IS FURTHER ORDERED** that the Defendants shall file with the Court and serve on Microsoft's 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 Microsoft's request for a preliminary injunction. Microsoft may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the 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 9<sup>th</sup> day of March, 2011.  
at 9:00 a.m.

  
The Honorable James L. Robart  
United States District Judge





FILED  
LODGED  
ENTERED  
RECEIVED

APR - 6 2011

AT SEATTLE  
CLERK U.S. DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
DEPUTY

The Honorable James L. Robart

11-CV-00222-ORD

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

MICROSOFT CORPORATION,

Plaintiff,

v.

JOHN DOES 1-11 CONTROLLING A  
COMPUTER BOTNET THEREBY  
INJURING MICROSOFT AND ITS  
CUSTOMERS,

Defendants.

Case No. 2:11-cv-00222

~~PROPOSED~~ ORDER FOR  
PRELIMINARY INJUNCTION

*JLR*

Plaintiff Microsoft Corporation ("Microsoft") filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the CAN-SPAM Act (15 U.S.C. § 7704); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (4) the common law of trespass, conversion and unjust enrichment. On March 9, 2011, the Court granted Microsoft's Application for an Emergency Temporary Restraining Order, Seizure Order and Order to Show Cause Re Preliminary Injunction. Microsoft now moves for an Order for Preliminary Injunction seeking to keep in place the relief granted by the March 9<sup>th</sup> order.

**FINDINGS OF FACT AND CONCLUSIONS OF LAW**

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Microsoft's Application for *Ex Parte* Temporary Restraining Order, *Ex Parte* Seizure and Order to Show Cause Re Preliminary Injunction ("TRO Application"), as well as supplemental

[PROPOSED] ORDER FOR PRELIMINARY  
INJUNCTION

Case No. 2:11-cv-00222

Orrick Herrington & Sutcliffe LLP  
701 5th Avenue, Suite 3600  
Seattle, Washington 98104-7097  
tel+1-206-839-4300



1 declarations and a status report regarding notice and service of process submitted by Microsoft  
2 on April 4, 2011, the Court hereby makes the following findings of fact and conclusions of law:

3 1. This Court has jurisdiction over the subject matter of this case and there is good  
4 cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim  
5 upon which relief may be granted against the Defendants under the Computer Fraud and Abuse  
6 Act (18 U.S.C. § 1030); CAN-SPAM Act (15 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§  
7 1114, 1125); and the common law of trespass to chattels, conversion and unjust enrichment.

8 2. Microsoft owns the registered trademarks "Microsoft," "Windows," and  
9 "Hotmail," used in connection with its services, software, and products.

10 3. There is good cause to believe that Defendants have engaged in and are likely to  
11 engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030);  
12 CAN-SPAM Act (15 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§ 1114, 1125); and the  
13 common law of trespass to chattels, conversion and unjust enrichment. The evidence set forth in  
14 Microsoft's Application for an Emergency Temporary Restraining Order, Seizure Order and  
15 Order to Show Cause Re Preliminary Injunction ("TRO Motion"), and the accompanying  
16 declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that  
17 Defendants have engaged in violations of the foregoing laws by: (1) intentionally accessing and  
18 sending malicious software to Microsoft's and its customers' protected computers and operating  
19 systems, without authorization, in order to infect those computers and make them part of the  
20 botnet; (2) sending malicious software to configure, deploy and operate a botnet; (3) sending  
21 unsolicited spam e-mail to Microsoft's Hotmail accounts; and (4) sending unsolicited spam e-  
22 mails that falsely indicate that they are from or approved by Microsoft and that promote  
23 counterfeit pharmaceuticals and other fraudulent schemes. Therefore, Microsoft is likely to  
24 prevail on the merits of this action.

25 4. There is good cause to believe that unless they are preliminarily enjoined by  
26 Order of this Court, immediate and irreparable harm will result from the Defendants' further  
27 violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030); CAN-SPAM Act (15  
28 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§ 1114, 1125); and the common law of trespass to

1 chattels, conversion and unjust enrichment. There is good cause to believe that if such conduct  
2 continues, irreparable harm will occur to Microsoft and the public, including Microsoft's  
3 customers. There is good cause to believe that the Defendants will continue to engage in such  
4 unlawful actions if not preliminarily enjoined from doing so by Order of this Court.

5 5. There is good cause to believe that the hardship to Microsoft, its customers, and  
6 the public resulting from denying this Motion for Preliminary Injunction far outweighs the  
7 hardship that will be suffered by Defendants if the Preliminary Injunction issues. Defendants are  
8 accused of illegally infecting end-user computers to enlist them into Rustock, a network of  
9 infected end-user computers operated over the Internet and used for illegal purposes. Microsoft,  
10 its customers, and the public are harmed by this activity through the high-volume of spam e-mail  
11 generated by Rustock, the various schemes promoted by Rustock e-mail such as the sale of  
12 counterfeit pharmaceuticals, and the ongoing infection of end-user computers and their use in  
13 illegal purposes. Therefore, the balance of hardships tips in favor of granting a Preliminary  
14 Injunction.

15 6. There is good cause to believe that the preliminary injunction will benefit the  
16 public. Maintaining the relief put in place under the Court's TRO will keep the operators of  
17 Rustock from reconstituting its Command and Control Infrastructure, will sharply curtail its  
18 ability to propagate spam e-mail, will reduce its involvement in promoting illegal schemes  
19 including infringement of Microsoft's trademarks and the sale of counterfeit pharmaceuticals,  
20 and will keep it from using the current tier of Rustock-infected end-user computers in illegal  
21 activity without their owner's permission or knowledge. Therefore, a Preliminary Injunction will  
22 have a favorable impact on the public interest.

23 7. There is good cause to believe that the Defendants have engaged in illegal activity  
24 using the data centers and/or Internet hosting providers identified in Appendix A to host the  
25 command and control software and the malicious botnet code and content used to maintain and  
26 operate the botnet at computers, servers, electronic data storage devices or media at the IP  
27 addresses identified in Appendix A.

28 8. There is good cause to believe that to keep Defendants from resuming actions

1 injurious to Microsoft and others, Defendants' IP addresses identified in Appendix A must  
2 remain in a disabled state; Defendants' computing resources related to such IP addresses must  
3 remain disconnected from the Internet; and Defendants must be prohibited from accessing  
4 Defendants' computer resources related to such IP addresses.

5 9. There is good cause to believe that the Defendants have engaged in illegal activity  
6 using the Internet domains identified at Appendix B to this order to host the command and  
7 control software and content used to maintain and operate the botnet. There is good cause to  
8 believe that to immediately halt the injury caused by Defendants, each of Defendants' current  
9 and prospective domains set forth in Appendix B must be maintained in an inaccessible state,  
10 and/or removed from the Internet zone file.

11 10. There is good cause to direct that third party data centers, hosting providers and  
12 Internet registries/registrars reasonably assist in the implementation of the Order and refrain from  
13 frustrating the implementation and purposes of this Order, pursuant to 28 U.S.C. § 1651(a) (the  
14 All Writs Act).

15 11. There is good cause to believe that Microsoft has provided adequate notice to  
16 Defendants of the TRO and this Preliminary Injunction. The following means of service  
17 employed by Microsoft are authorized by law, satisfy Due Process, satisfy Fed. R. Civ. Pro.  
18 4(f)(3); and are reasonably calculated to notify defendants of the TRO, the Preliminary  
19 Injunction hearing and of the Complaint: (1) transmission by e-mail, facsimile, and mail to the  
20 contact information provided by defendants to the data centers, Internet hosting providers, and  
21 domain registrars who host the software code associated with the IP addresses in Appendix A, or  
22 through which domains in Appendix B are registered; and (2) publishing notice to the  
23 Defendants on a publicly available Internet website.

24 12. Therefore, in accordance with Fed. R. Civ. P. 65(a) and the All Writs Act, good  
25 cause and the interests of justice require that this Order be Granted.

26 **PRELIMINARY INJUNCTION**

27 **IT IS THEREFORE ORDERED** as follows:

28 A. Defendants, their representatives and persons who are in active concert or  
[PROPOSED] ORDER FOR PRELIMINARY INJUNCTION  
CASE NO. 2:11-CV-00222



1 participation with them are preliminarily enjoined from intentionally accessing and sending  
2 malicious software to Microsoft's and its customers' protected computers and operating systems,  
3 without authorization, in order to infect those computers and make them part of the botnet;  
4 sending malicious software to configure, deploy and operate a botnet; sending unsolicited spam  
5 e-mail to Microsoft's Hotmail accounts; and sending unsolicited spam e-mail that falsely indicate  
6 that they are from or approved by Microsoft; or undertaking any similar activity that inflicts  
7 harm on Microsoft or the public, including Microsoft's customers.

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

14 C. Defendants, their representatives and persons who are in active concert or  
15 participation with them are preliminarily enjoined from using the trademarks "Microsoft,"  
16 "Windows," "Hotmail," and/or other trademarks; trade names; service marks; or Internet Domain  
17 addresses or names; or acting in any other manner which suggests in any way that Defendants'  
18 products or services come from or are somehow sponsored or affiliated with Microsoft, and from  
19 otherwise unfairly competing with Microsoft, misappropriating that which rightfully belongs to  
20 Microsoft, or passing off their goods as Microsoft's.

21 D. Defendants, their representatives and persons who are in active concert or  
22 participation with them are preliminarily enjoined from infringing Microsoft's registered  
23 trademarks, Registration Nos. 1200236, 2165601, 2463510 and others.

24 E. Defendants, their representatives and persons who are in active concert or  
25 participation with them are preliminarily enjoined from using in connection with Defendants'  
26 activities any false or deceptive designation, representation or description of Defendants' or of  
27 their representatives' activities, whether by symbols, words, designs or statements, which would  
28 damage or injure Microsoft or give Defendants an unfair competitive advantage or result in

1 deception of consumers.

2 F. Microsoft shall maintain its bond in the amount of \$173,000 that it has paid into  
3 the Court's Registry.

4 G. Pursuant to the All Writs Act, the data centers and hosting providers identified in  
5 Appendix A and the domain registries identified in Appendix B to this Order, shall, during the  
6 pendency of this action:


7 1. Maintain in a disabled state Defendants' IP addresses set forth in  
8 Appendix A (including through any backup systems) so that they cannot be accessed over the  
9 Internet, connected to, or communicated with in any way except as explicitly provided for in this  
10 order;

11 2. Maintain in a disabled state Defendants' domains set forth in Appendix B  
12 so that they cannot be accessed over the Internet, connected to, or communicated with in any  
13 way except as explicitly provided for in this order by (1) keeping the domains locked and  
14 keeping such domains from being entered into the zone file; and (2) taking all steps required to  
15 propagate the foregoing domain registry changes to domain name registrars;

16 3. provide reasonable assistance in implementing the terms of this Order and  
17 shall take no action to frustrate the implementation of this Order.

18  
19  
20 **IT IS SO ORDERED**

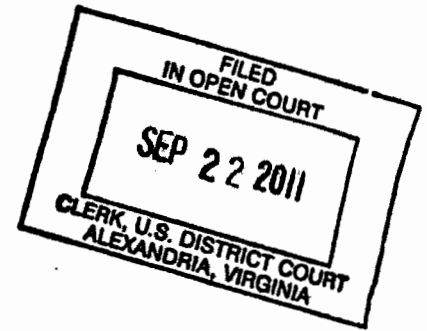
21  
22 Entered this <sup>th</sup>6 day of April, 2011.

  
The Honorable James L. Robart  
United States District Judge





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



MICROSOFT CORPORATION, a  
Washington corporation,

Plaintiff,

v.

DOMINIQUE ALEXANDER PATTI, an  
individual; DOTFREE GROUP S.R.O., a  
Czech limited liability company, JOHN  
DOES 1-22, CONTROLLING A  
COMPUTER BOTNET THEREBY  
INJURING MICROSOFT AND ITS  
CUSTOMERS

Defendants.

Civil Action No: 1:11cv1017

FILED UNDER SEAL

**EX PARTE TEMPORARY RESTRAINING ORDER AND  
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiff Microsoft Corp. ("Microsoft") has file a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the CAN-SPAM Act (15 U.S.C. § 7704); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (4) the common law of trespass, unjust enrichment, conversion, and negligence. Microsoft has 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 and the All-Writs Act, 28 U.S.C. § 1651.

**FINDINGS**

The Court has considered the pleadings, declarations, exhibits, and memorandum filed in support of Microsoft's motion and finds that:

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 thereto; the Complaint states a

claim upon relief may be granted against Defendants under the 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 Lanham Act (15 U.S.C. § 1125), common law trespass to chattels, unjust enrichment, conversion, and negligence.

2. 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), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125), common law trespass to chattels, unjust enrichment, conversion, and negligence, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. There is good cause to believe that, unless the Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations of the 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 Lanham Act (15 U.S.C. § 1125), common law trespass to chattels, unjust enrichment, conversion, and negligence. The evidence set forth in Microsoft's Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Motion"), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing law by:

- a. intentionally accessing and sending malicious code to Microsoft's and its customers' protected computers and operating systems, without authorization, in order to infect those computers and make them part of the botnet;
- b. sending malicious code to configure, deploy and operate a botnet;
- c. sending unsolicited spam email to Microsoft's Hotmail accounts;
- d. collecting personal information, including personal email addresses; and
- e. delivering malicious code.

4. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, its customers, 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;

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 IP addresses and Internet domains at issue in Microsoft's TRO Motion and other discoverable evidence of Defendants' misconduct available through such IP addresses and Internet domains if the Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Motion and accompanying declarations and exhibits, Microsoft is likely to be able to prove that:

- a. Defendants are engaged in activities that directly violate United States law and harms Microsoft, its customers and the public;
- b. Defendants have continued their unlawful conduct despite the clear injury to Microsoft, its customers, and the public;
- c. Defendants are likely to relocate the information and evidence of their misconduct stored at the IP addresses and Internet domains at issue in Microsoft's TRO Motion and the harmful and malicious code disseminated through these IP addresses and Internet domains; and
- d. Defendants are likely to warn its associates engaged in such activities if informed of Microsoft's action.

6. Microsoft's request for this emergency *ex parte* relief is not the result of any lack of diligence on Microsoft's part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), Civil L.R. 65-1 and the All-Writs Act, 28 U.S.C. § 1651, good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and accordingly, Microsoft is relieved of the duty to provide Defendants with prior notice of Microsoft's motion;

7. There is good cause to believe that Defendants have engaged in illegal activity using the IP addresses and the .com and .cc domains that are maintained by the top level domain registry Verisign, located in the United States and the Eastern District of Virginia.

8. There is good cause to believe that to immediately halt the injury caused by Defendants, the hosting companies, IP registries, domain registries and domain registrars set forth in Appendices A and B, must be ordered, at 3:00 a.m. Eastern Daylight Time on September 26, 2011 or such other date and time as requested by Microsoft within seven days of this Order:

- a. to immediately take all steps necessary to lock at the registry level the domains at issue in the TRO Motion, and which are set forth at Appendix A hereto, to ensure that changes to the domain names cannot be made absent a court order;
- b. to immediately take all steps required to propagate the foregoing domain registry changes to domain name registrars; and
- c. to hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.
- d. to immediately take all steps necessary to disable access to the IP addresses at issue in the TRO Motion, and which are set forth at Appendix B hereto, to ensure that access to the IP addresses cannot be made absent a court order;

9. 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 through the Hague Convention on Service Abroad or similar treaties upon defendants who provided contact information in foreign countries that are signatory to such treaties, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain name registrars and as agreed to



by Defendants in their domain name registration agreements, (4) publishing notice on a publically available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

**TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE**

**IT IS THEREFORE ORDERED** that, Defendants and their representatives are temporarily restrained and enjoined from intentionally accessing and sending malicious software or code to Microsoft's and its customers protected computers and operating systems, without authorization, in order to infect those computers and make them part of the Kelihos botnet, sending malicious code to configure, deploy and operate a botnet, sending unsolicited spam email to Microsoft's email and messaging accounts and services, sending unsolicited spam email that falsely indicates that they originated from Microsoft or are approved by Microsoft or are from its email and messaging accounts or services, collecting personal information including personal email addresses, delivering malicious code including fake antivirus software, or undertaking similar activity that inflicts harm on Microsoft, its customers, or the public.

**IT IS FURTHER ORDERED** that, Defendants and their representatives are temporarily restrained and enjoined from configuring, deploying, operating or otherwise participating in or facilitating the botnet described in the TRO Motion, including but not limited to the command and control software hosted at and operating through the IP addresses and domains set forth herein and through any other component or element of the botnet in any location.

**IT IS FURTHER ORDERED** that Defendants and their representatives are temporarily restrained and enjoined from using the "Microsoft," "Windows," "Hotmail," "Windows Live" and "MSN" trade names, trademarks or service marks, in Internet Domain addresses or names, in content or in any other infringing manner or context, 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 Microsoft, and from otherwise unfairly competing with Microsoft, misappropriating that which rightfully belongs to Microsoft, or passing off their goods as Microsoft's.

**IT IS FURTHER ORDERED** that the domain registries and registrars set forth in

Appendix A must:

- a. immediately take all steps necessary to lock at the registry level the domains at issue in the TRO Motion, an which are set forth at Appendix A hereto, to ensure that changes to the domain names cannot be made absent a court order;
- b. immediately take all steps required to propagate to the foregoing domain registry changes to domain name registrars; and
- c. hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.
- d. Shall completely refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and shall refrain from publicizing this Order until this Order is executed in full, except as explicitly provided for in this Order;
- a. Shall save all communications to or from Defendants or Defendants' Representatives and/or related to the domains set forth in Appendix A;
- e. Shall preserve and retain all records and documents associated with Defendants' or Defendants' Representatives' use of or access to the domains set forth in Appendix A, including billing and contact information relating to the Defendants or Defendants' representatives using these servers and all logs associated with these servers.

**IT IS FURTHER ORDERED** that the Internet hosting and service providers identified in Appendix B to this order:

- b. Shall immediately take all reasonable steps necessary to completely block all access by Defendants, Defendants' representatives, resellers, and any other person or computer to the IP addresses set forth in Appendix B, except as explicitly provided for in this Order;

- c. Shall immediately and 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 B 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. Shall immediately, completely, and until further order of this Court, suspend all services associated with the IP addresses set forth in Appendix B;
- e. Shall 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 or any other person;
- f. Shall disable, and shall deny to Defendants and Defendants' representatives, access to any and all "backup" systems, arrangements or services that might otherwise be used to support the IP addresses set forth in Appendix B or that might otherwise be used to circumvent this Order;
- g. Shall log all attempts to connect to or communicate with the IP addresses set forth in Appendix B;
- h. Shall save all communications to or from Defendants or Defendants' Representatives and/or related to the IP addresses set forth in Appendix B;
- i. Shall preserve and retain all records and documents associated with Defendants' or Defendants' Representatives' use of or access to the IP addresses set forth in Appendix B, including billing and contact information relating to the Defendants or Defendants' representatives using these servers and all logs associated with these servers;
- j. Shall completely refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and

shall refrain from publicizing this Order until this Order is executed in full, except as explicitly provided for in this Order;

**IT IS FURTHER ORDERED** that Internet hosting and service providers identified in Appendix B to this Order:

- a. Shall immediately identify and create a written list of domains, if any, hosted at the IP addresses set forth in Appendix B; shall transfer any content and software associated with such domains to IP addresses not listed in Appendix B; and shall notify the domain owners of the new IP addresses, and direct the domain owners 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.
- b. Shall produce to Microsoft 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.

**IT IS FURTHER ORDERED** 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, facsimile and mail to the contact information provided by defendants to the data centers, Internet hosting providers and domain registrars who hosted the software code associated with the domains and IP addresses set forth at Appendices A and B; and (4) by

publishing notice to Defendants on a publicly available Internet website and/or in newspapers in the communities in which Defendants are believed to reside.

**IT IS FURTHER ORDERED**, pursuant to Federal Rule of Civil Procedure 65(b) *on October 5th 2011 at 10:30 AM* that the Defendants shall appear before this Court within 14 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 the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this Order.

**IT IS FURTHER ORDERED** that Microsoft shall post bond in the amount of \$10,000 as cash to be paid into the Court registry.

**IT IS FURTHER ORDERED** that the Defendants shall file with the Court and serve on Microsoft's 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 Microsoft's request for a preliminary injunction. Microsoft may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the 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. (Eastern Standard Time) on the appropriate dates listed in this paragraph.

**IT IS SO ORDERED**

Entered this 22<sup>nd</sup> day of September, 2011.

*10:14 A.M.  
E.D.T.*

*/s/*  
*[Signature]*  
**James C. Cacheris**  
**United States District Judge**  
United States District Judge





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

MICROSOFT CORPORATION, a  
Washington corporation,

Plaintiff,

v.

DOMINIQUE ALEXANDER PIATTI, an  
individual; DOTFREE GROUP S.R.O., a  
Czech limited liability company, JOHN  
DOES 1-22, CONTROLLING A  
COMPUTER BOTNET THEREBY  
INJURING MICROSOFT AND ITS  
CUSTOMERS

Defendants.

Civil Action No: 1:11cv1017 (JCC/IDD)

**CONSENT PRELIMINARY INJUNCTION**

Plaintiff Microsoft Corp. ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the CAN-SPAM Act (15 U.S.C. § 7704); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (4) the common law of trespass, unjust enrichment, conversion, and negligence. Microsoft has moved for a preliminary injunction pursuant to Rule 65(b) of the Federal Rules of Civil Procedure and the All-Writs Act, 28 U.S.C. § 1651.

**FINDINGS**

**Findings Regarding The Domain "CZ.CC"**

With respect to the internet domain name "cz.cc," one of the domains that is the subject of Microsoft's motion for a preliminary injunction, the Court makes the following findings:

1. Plaintiff Microsoft and Defendants Dominique Piatti and dotFree Group s.r.o., have jointly advised the Court that the parties have reached agreement regarding the disposition of the "cz.cc" domain during the pendency of this action. Microsoft, Dominique Piatti and

dotFree Group have specifically advised the Court that such agreement includes provisions to disable malicious subdomains and a process to verify the identities of sub-domain registrants, and that Mr. Piatti and dotFree Group s.r.o. desire to comply with and adhere to the terms of that agreement and this Order.

2. Plaintiff Microsoft and Defendants Dominique Piatti and dotFree Group s.r.o. have jointly advised the Court that the parties stipulate to the Court's jurisdiction and authority to enter the relief set forth herein regarding the domain "cz.cc," without waiver of any of the parties' rights or positions in this action.

**Findings Regarding Domains Registered By John Doe Defendants**

The Court has considered the pleadings, declarations, exhibits, and memorandum filed in support of Microsoft's motion and finds, with respect to Defendants John Does 1-22 that:

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 thereto; the Complaint states a claim upon which relief may be granted against John Doe Defendants under the 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 Lanham Act (15 U.S.C. § 1125), common law trespass to chattels, unjust enrichment, conversion, and negligence;

2. There is good cause to believe that John Doe 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), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125), common law trespass to chattels, unjust enrichment, conversion, and negligence, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. There is good cause to believe that, unless the John Doe Defendants are enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations of the 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 Lanham

Act (15 U.S.C. § 1125), common law trespass to chattels, unjust enrichment, conversion, and negligence. The evidence set forth in Microsoft's Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Motion"), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that John Doe Defendants have engaged in violations of the foregoing law by:

- a. intentionally accessing and sending malicious code to Microsoft's and its customers' protected computers and operating systems, without authorization, in order to infect those computers and make them part of the botnet;
- b. sending malicious code to configure, deploy and operate a botnet;
- c. sending unsolicited spam email to Microsoft's Hotmail accounts;
- d. collecting personal information, including personal email addresses; and
- e. delivering malicious code.

4. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, its customers, and the public. There is good cause to believe that the John Doe Defendants 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 John Doe Defendants of the Internet domains at issue in Microsoft's Motion for Preliminary Injunction and other discoverable evidence of John Doe Defendants' misconduct available through such Internet domains if the John Doe Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's Motion for Preliminary Injunction and accompanying declarations and exhibits, Microsoft is likely to be able to prove that:

- a. John Doe Defendants are engaged in activities that directly violate United States law and harms Microsoft, its customers and the public;

- b. John Doe Defendants have continued their unlawful conduct despite the clear injury to Microsoft, its customers, and the public;
- c. John Doe Defendants are likely to relocate the information and evidence of their misconduct stored at the Internet domains at issue in Microsoft's Motion and the harmful and malicious code disseminated through these Internet domains; and
- d. John Doe Defendants are likely to warn its associates engaged in such activities if informed of Microsoft's action.

6. Microsoft's request for this emergency *ex parte* relief is not the result of any lack of diligence on Microsoft's part, but instead based upon the nature of John Doe Defendants' unlawful conduct.

7. There is good cause to believe that John Doe Defendants have engaged in illegal activity using domains that are maintained by the top level domain registry Verisign, located in the United States and the Eastern District of Virginia.

8. There is good cause to believe that to immediately halt the injury caused by John Doe Defendants, the domain registries and domain registrars set forth in Appendix A in relation to all domains other than cz.cc, must be ordered:

- a. to immediately take all steps necessary to lock at the registry level and to place on registry hold all of the domains set forth at Appendix A hereto (except for "cz.cc"), to ensure that such domains are disabled during the pendency of this action and that changes to the domain names cannot be made absent a court order;
- b. to immediately take all steps required to propagate the foregoing domain registry changes to domain name registrars; and
- c. to hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.

9. There is good cause to permit notice of the instant order 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 and of this action: (1) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided contact information in foreign countries that are signatory to such treaties, (2) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain name registrars and as agreed to by Defendants in their domain name registration agreements, (3) publishing notice on a publically available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

### **PRELIMINARY INJUNCTION**

**IT IS THEREFORE ORDERED** that Plaintiff Microsoft and Defendants Dominique Piatti and dotFree Group s.r.o. are directed to adhere strictly to the terms of the agreement between them regarding disposition of the domain "cz.cc" during the pendency of this action, to prevent the irreparable harm that has been caused by others through the "cz.cc" internet domain name. In particular, Plaintiff Microsoft and Defendants Dominique Piatti and dotFree Group are directed to adhere strictly to the provisions of the agreement regarding disablement of malicious subdomains and provisions concerning a process to verify the identities of sub-domain registrants.

**IT IS THEREFORE ORDERED** that, John Doe Defendants and their representatives are temporarily restrained and enjoined from intentionally accessing and sending malicious software or code to Microsoft's and its customers protected computers and operating systems, without authorization, in order to infect those computers and make them part of the Kelihos botnet, sending malicious code to configure, deploy and operate a botnet, sending unsolicited spam email to Microsoft's email and messaging accounts and services, sending unsolicited spam email that falsely indicates that they originated from Microsoft or are approved by Microsoft or are from its email and messaging accounts or services, collecting personal information including personal email addresses, delivering malicious code including fake antivirus software, or undertaking similar activity that inflicts harm on Microsoft, its customers, or the public.

**IT IS FURTHER ORDERED** that, John Doe Defendants and their representatives are temporarily restrained and enjoined from configuring, deploying, operating or otherwise participating in or facilitating the botnet described in the TRO Motion, including but not limited to the command and control software hosted at and operating through the domains set forth herein and through any other component or element of the botnet in any location.

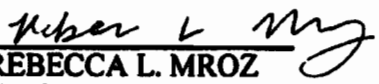
**IT IS FURTHER ORDERED** that John Doe Defendants and their representatives are temporarily restrained and enjoined from using the “Microsoft,” “Windows,” “Hotmail,” “Windows Live” and “MSN” trade names, trademarks or service marks, in Internet Domain addresses or names, in content or in any other infringing manner or context, or acting in any other manner which suggests in any way that John Doe Defendants’ products or services come from or are somehow sponsored or affiliated with Microsoft, and from otherwise unfairly competing with Microsoft, misappropriating that which rightfully belongs to Microsoft, or passing off their goods as Microsoft’s.

**IT IS FURTHER ORDERED** that the domain registries and registrars set forth in Appendix A must:

- a. immediately take all steps necessary to lock at the registry level and to place on registry hold all of the domains set forth at Appendix A hereto (except for “cz.cc”), to ensure that such domains are disabled during the pendency of this action and that changes to the domain names cannot be made absent a court order;
- b. to immediately take all steps required to propagate the foregoing domain registry changes to domain name registrars; and
- c. to hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.
- d. Shall save all communications to or from Defendants or Defendants’ Representatives and/or related to the domains set forth in Appendix A;
- e. Shall preserve and retain all records and documents associated with Defendants’ or Defendants’ Representatives’ use of or access to the domains set forth in

### PRELIMINARY INJUNCTION

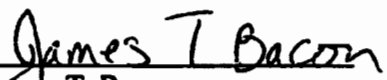
WE ASK FOR THIS:

  
REBECCA L. MROZ  
Va. State Bar No. 77114  
CHRISTOPHER M. O'CONNELL  
Va. State Bar No. 65790  
Attorneys for Plaintiff Microsoft Corp.  
ORRICK, HERRINGTON & SUTCLIFFE LLP  
1152 15th Street, N.W.  
Washington, D.C. 20005-1706  
Telephone: (202) 339-8400  
Facsimile: (202) 339-8500  
[bmroz@orrick.com](mailto:bmroz@orrick.com)  
[coconnell@orrick.com](mailto:coconnell@orrick.com)

Of counsel:

GABRIEL M. RAMSEY (*pro hac vice*)  
JACOB M. HEATH (*pro hac vice*)  
Attorneys for Plaintiff Microsoft Corp.  
ORRICK, HERRINGTON & SUTCLIFFE LLP  
1000 Marsh Road  
Menlo Park, CA 94025  
Telephone: (650) 614-7400  
Facsimile: (650) 614-7401  
[gramsey@orrick.com](mailto:gramsey@orrick.com)  
[jheath@orrick.com](mailto:jheath@orrick.com)

Counsel for Plaintiff Microsoft Corp.

  
James T. Bacon  
Va. Bar No. 22146  
Warner F. Young, III  
Va. Bar No. 24259  
Attorneys for Defendants Dominique A. Piatti and dotFree Group s.r.o.  
Allred, Bacon, Halfhill & Young, PC  
11350 Random Hills Road, Ste. 700  
Fairfax, Virginia 22030  
Tel.: (703) 352-1300  
Fax: (703) 352-1301  
[jbacon@abhylaw.com](mailto:jbacon@abhylaw.com)  
[wyoung@abhylaw.com](mailto:wyoung@abhylaw.com)

Counsel for Defendants Dominique A. Piatti  
and dotFree Group s.r.o.

## APPENDIX A

Domain Names Of Command And Control Servers	Domain Registry And Registrars	Registrant Information
<b>cz.cc</b>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Moniker Online Services, Inc. / Moniker Online Services LLC 20 SW 27<sup>th</sup> Ave, Suite 201 Pompano Beach, Florida 33069</p>	<p>Dominique Alexander Piatti dotFree Group s.r.o. Prazska 636 Dolni Brezany Praha-Zapad 25241 Czech Republic domi@cz.cc</p> <p>Dominique Piatti Postfach 127 Guemligen Bern 3073 Switzerland Dominique_piatti@hotmail.com</p>
<b>bricord.com</b>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois bricord.com c/o bricord.com N4892 Nassau Bahamas flyz0mt4db6aa1b61833@oqijj874d9300d54bd95.privatewhois.net oq9wmmx4db6aa1b6b08e@oqijj874d9300d54bd95.privatewhois.net n8h23tc4db6aa1b675f5@oqijj874d9300d54bd95.privatewhois.net</p>
<b>bevvyky.com</b>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois bevvyky.com c/o bevvyky.com N4892 Nassau Bahamas nomklo44e314f83cfc56@oqijj874d9300d54bd95.privatewhois.net c6e5z0k4e314f83d3306@oqijj874d9300d54bd95.privatewhois.net kh91bdf4e314f83d2364@oqijj874d9300d54bd95.privatewhois.net</p>
<b>carbili.com</b>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois carbili.com c/o carbili.com N4892 Nassau Bahamas Int5fmn4da33006da6ad@oqijj874d9300d54bd95.privatewhois.net hh7429m4da33006dc6f3@oqijj874d9300d54bd95.privatewhois.net e2m0ez64da33006dbb39@oqijj874d9300d54bd95.privatewhois.net</p>



<b>codfirm.com</b>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois codfirm.com c/o codfirm.com N4892 Nassau Bahamas</p> <p>hzteezh4da5e55a43a3f@oqijj874d9300d54bd95.privatewhois.net otqbyon4da5e55a480d4@oqijj874d9300d54bd95.privatewhois.net klwwh2i4da5e55a449e3@oqijj874d9300d54bd95.privatewhois.net</p>
<b>dissump.com</b>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois dissump.com c/o dissump.com N4892 Nassau Bahamas</p> <p>itamzrl4da5e558b33c0@oqijj874d9300d54bd95.privatewhois.net yvamaby4da5e558ba4dc@oqijj874d9300d54bd95.privatewhois.net hwhmpus4da5e558b952a@oqijj874d9300d54bd95.privatewhois.net</p>
<b>doloas.com</b>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois doloas.com c/o doloas.com N4892 Nassau Bahamas</p> <p>sk2xcdp4db6aa1e1a72d@oqijj874d9300d54bd95.privatewhois.net satosfb4db6aa1e1c673@oqijj874d9300d54bd95.privatewhois.net ka94bx44db6aa1e1b6f3@oqijj874d9300d54bd95.privatewhois.net</p>
<b>editial.com</b>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois editial.com c/o editial.com N4892 Nassau Bahamas</p> <p>ugz6k834db6aa1bdf3db@oqijj874d9300d54bd95.privatewhois.net klabbh4db6aa1be12f3@oqijj874d9300d54bd95.privatewhois.net w5n0ngq4db6aa1be078a@oqijj874d9300d54bd95.privatewhois.net</p>
<b>gratima.com</b>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois gratima.com c/o gratima.com N4892 Nassau Bahamas</p> <p>nmpzuvs4db6aa1e9484b@oqijj874d9300d54bd95.privatewhois.net ecvgjy74db6aa1e9a9e9@oqijj874d9300d54bd95.privatewhois.net vmjy2s54db6aa1e99a3f@oqijj874d9300d54bd95.privatewhois.net</p>
<b>hellohello123.com</b>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p>	<p>Verisign Naming Services Attn: VNDS Monitoring-East 21345 Ridgetop Circle 4<sup>th</sup> Floor</p>

	Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Dulles, Virginia 20166
knifell.com	Verisign Naming Services 21345 Ridgeway Circle 4 <sup>th</sup> Floor Dulles, Virginia 20166  Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois knifell.com c/o knifell.com N4892 Nassau Bahamas  nff7lac4db6aalc5f12f@oqijj874d9300d54bd95.privatewhois.net f9rcd314db6aalc61040@oqijj874d9300d54bd95.privatewhois.net xxjkjti4db6aalc60486@oqijj874d9300d54bd95.privatewhois.net
lalare.com	Verisign Naming Services 21345 Ridgeway Circle 4 <sup>th</sup> Floor Dulles, Virginia 20166  Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois lalare.com c/o lalare.com N4892 Nassau Bahamas  q5sgyzz4da5e55aba0cb@oqijj874d9300d54bd95.privatewhois.net gh8xk5h4da5e55abbc1c@oqijj874d9300d54bd95.privatewhois.net fmc13dk4da5e55abb06l@oqijj874d9300d54bd95.privatewhois.net
magdali.com	Verisign Naming Services 21345 Ridgeway Circle 4 <sup>th</sup> Floor Dulles, Virginia 20166  Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois magdali.com c/o magdali.com N4892 Nassau Bahamas  n0vo7qm4da5e55b7a19l@oqijj874d9300d54bd95.privatewhois.net bvdkatd4da5e55b82230@oqijj874d9300d54bd95.privatewhois.net wl505fm4da5e55b80ee3@oqijj874d9300d54bd95.privatewhois.net
partric.com	Verisign Naming Services 21345 Ridgeway Circle 4 <sup>th</sup> Floor Dulles, Virginia 20166  Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois partric.com c/o partric.com N4892 Nassau Bahamas  rsjy9e4db6aalc28df3@oqijj874d9300d54bd95.privatewhois.net t9js2644db6aalc2d019@oqijj874d9300d54bd95.privatewhois.net fv88khq4db6aalc2c0ba@oqijj874d9300d54bd95.privatewhois.net
restonal.com	Verisign Naming Services 21345 Ridgeway Circle 4 <sup>th</sup> Floor Dulles, Virginia 20166  Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois restonal.com c/o restonal.com N4892 Nassau Bahamas  uuyidk54da5e55939e3c@oqijj874d9300d54bd95.privatewhois.net cqvb1nj4da5e5593f00f@oqijj874d9300d54bd95.privatewhois.net ck1u2t54da5e5593e0be@oqijj874d9300d54bd95.privatewhois.net

<b>subcosi.com</b>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois subcosi.com c/o subcosi.com N4892 Nassau Bahamas</p> <p>lz0xca94da5e559c6462@oqijj874d9300d54bd95.privatewhois.net typqrv4da5e559c8f22@oqijj874d9300d54bd95.privatewhois.net zzhu7vv4da5e559c7b9b@oqijj874d9300d54bd95.privatewhois.net</p>
<b>uncter.com</b>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois uncter.com c/o uncter.com N4892 Nassau Bahamas</p> <p>cv47vjf4da5e55be3901@oqijj874d9300d54bd95.privatewhois.net cgvni4da5e55be5bf1@oqijj874d9300d54bd95.privatewhois.net lkvy5fh4da5e55be4c53@oqijj874d9300d54bd95.privatewhois.net</p>
<b>wargalo.com</b>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois wargalo.com c/o wargalo.com N4892 Nassau Bahamas</p> <p>dy0stoh4db6aa1da2eda@oqijj874d9300d54bd95.privatewhois.net o2jtjp64db6aa1da7522@oqijj874d9300d54bd95.privatewhois.net ty3s2ct4db6aa1da6199@oqijj874d9300d54bd95.privatewhois.net</p>
<b>wormetal.com</b>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois wormetal.com c/o wormetal.com N4892 Nassau Bahamas</p> <p>u5248i34db6aa1f24b3c@oqijj874d9300d54bd95.privatewhois.net bjhl1334db6aa1f27244@oqijj874d9300d54bd95.privatewhois.net oykewjr4db6aa1f25ef1@oqijj874d9300d54bd95.privatewhois.net</p>
<b>earplat.com</b>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois earplat.com c/o earplat.com N4892 Nassau Bahamas</p> <p>x1giip14e315630344b@oqijj874d9300d54bd95.privatewhois.net o4yns8o4e315631095bd@oqijj874d9300d54bd95.privatewhois.net sbh8ipe4e31563107e77@oqijj874d9300d54bd95.privatewhois.net</p>
<b>metapli.com</b>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p>	<p>Private Whois metapli.com c/o metapli.com N4892 Nassau Bahamas</p>

	<b>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</b>	<b>pzjjnfc4e3155e157ceb@oqjj874d9300d54bd95.privatewhois.net yeij2yh4e3155e15b733@oqjj874d9300d54bd95.privatewhois.net zv2ea6o4e3155e15a79a@oqjj874d9300d54bd95.privatewhois.net</b>
--	--	--