

1 DAVID SHONKA
Acting General Counsel

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

9 Attorneys for Plaintiff Federal Trade Commission

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

13 **Federal Trade Commission,**

14 **Plaintiff,**

15 **v.**

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

20 **Defendant.**

Case No. _____

**MEMORANDUM OF POINTS
AND AUTHORITIES IN
SUPPORT OF PLAINTIFF'S
MOTION FOR AN *EX PARTE*
TEMPORARY RESTRAINING
ORDER AND ORDER TO SHOW
CAUSE**

TABLE OF CONTENTS

1

2 I. SUMMARY 1

3 II. THE PARTIES 2

4 A. Plaintiff 2

5 B. Defendant 2

6 III. THE DEFENDANT’S BUSINESS PRACTICES 3

7 A. Special Agent Sean Zadig, NASA Office of Inspector General, Computer Crime

8 Division 3

9 1. The Discovery of the ICQ Logs 4

10 2. Botnet and Click Fraud Basics 5

11 3. The Translated ICQ Logs 6

12 4. Zadig’s Analysis of the Content Hosted by 3FN 8

13 5. Attacks on NASA Originating From 3FN 9

14 B. Gary Warner, Director of Research in Computer Forensics, University of

15 Alabama at Birmingham 9

16 1. The Illegal, Harmful and Malicious Content Hosted by 3FN 10

17 a. Malicious Botnet Software 10

18 b. Child Pornography 10

19 c. Fake Anti-Virus Products 11

20 d. Illegal Online Pharmacies 11

21 e. Pirated Music and Software 11

22 2. 3FN Actively Recruits Criminals 12

23 C. Sarah Ohlsen, Supervisor, Exploited Children Division, The National Center for

24 Missing and Exploited Children 12

25 D. Steve Linford, Founder, The Spamhaus Project 13

26 E. Andre’ DiMino, Co-Founder and Director, The Shadowserver Foundation 15

27 F. Dean Turner, Director of the Global Intelligence Network, Symantec

28 Corporation 16

G. Sheryl Drexler, Investigator, Federal Trade Commission 17

1. Aliases Used by Pricewert 17

2. Pricewert’s Extensive Overseas Ties 17

3. Pricewert’s Marketing Efforts 18

4. Consumer Complaints Regarding 3FN 18

5. Malicious Activity Originating from 3FN’s Servers 18

IV. ARGUMENT

A. The FTC Act Authorizes the Requested Relief 19

B. The Commission Has Established a Likelihood of Succeeding on the Merits of its

Section 5 Claims that Pricewert Has Engaged in Unfair Acts or Practices 10

1. Defendant’s Conduct Causes or is Likely to Cause Substantial Injury to

Consumers 22

2. The Harm Pricewert Inflicts Upon Consumers Is Not Outweighed by any

Countervailing Benefits 23

3. The Harm Inflicted Upon Consumers Is Not Reasonably Avoidable ... 23

4. Pricewert’s Unfair Conduct Is Not Protected By Section 230 of the

Communications Decency Act 24

C. The Balance of Equities Tips Decidedly In the Commission’s Favor and Supports

Awarding the Requested Injunctive Relief 24

V. AN *EX PARTE* TEMPORARY RESTRAINING ORDER DISCONNECTING

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

DEFENDANT’S SERVERS FROM THE INTERNET, FREEZING ASSETS AND ORDERING THE TURNOVER OF DOCUMENTS, AN ACCOUNTING, AND THE PRESERVATION OF RECORDS SHOULD BE GRANTED 26

VI. CONCLUSION 28

1 **TABLE OF AUTHORITIES**

2 **Federal Statutes**

3 15 U.S.C. § 45(a) (2006) 2, 20
4 15 U.S.C. § 45(n) (2006) 20, 22
5 15 U.S.C. § 53(b) (2006) 2
6 15 U.S.C. §§ 41-58 (2006) 2
7 18 U.S.C. § 1030 (2006) 6
8 47 U.S.C. § 230 (2006). 24

9 **State Statutes**

10 Cal. Penal Code § 502 (2008) 6

11 **Cases**

12
13 *Doe v. United States*, 487 U.S. 201 (1988) 28
14 *Fair Housing Council of San Fernando Valley v. Roomates.com LLC*, 521 F.3d 1157 (9th Cir.
15 2008) 24
16 *FSLIC v. Sahni*, 868 F.2d 1096 (9th Cir. 1989) 27
17 *FTC v. Accusearch, Inc.*, 2007 U.S. Dist. LEXIS 74905 (D. Wyo. 2007) 21, 22
18 *FTC v. Affordable Media*, 179 F.3d 1228 (9th Cir. 1999) 27, 28
19 *FTC v. American National Cellular, Inc.*, 810 F.2d 1511 (9th Cir. 1987) 19
20 *FTC v. Amy Travel Serv., Inc.*, 875 F.2d 654 (7th Cir. 1989) 19
21 *FTC v. Crescent Publ'g Group, Inc.*, 129 F. Supp. 2d 311 (S.D.N.Y. 1991) 21
22 *FTC v. Dugger*, Civ. No. CV-06-0078-PHX-ROS (D. Ariz., Jan. 10, 2006) 19, 22, 26
23 *FTC v. Enternet Media*, CV-05-7777 CAS-AJWx (C.D. Cal. 2005) 20
24 *FTC v. ERG Ventures, LLC*, CV-06-00578 LRH-VCP (D. Nev. 2006) 20
25 *FTC v. Gem Merchandising Corp.*, 87 F.3d 466 (11th Cir. 1996) 27
26 *FTC v. H.N. Singer, Inc.*, 668 F.2d 1107 (9th Cir. 1982) 19, 27
27 *FTC v. Innovative Marketing*, Civ. No. RDB-08-CV-3233 (D. Md. Dec. 2, 2008) 11

1 *FTC v. J.K. Pubs. Inc.*, 99 F. Supp. 2d 1176 (C.D. Cal. 2000) 21, 23, 27

2 *FTC v. MaxTheater, Inc.*, No. 05-CV-0069 (E.D. Wa. Dec. 6, 2005) 11

3 *FTC v. National Vending Consultants, Inc.*, CV-S-05-0160-RCJ-PAL (D. Nev. 2005) 20

4 *FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104 (S.D. Cal. 2008) 20, 22

5 *FTC v. Pantron I Corp.*, 33 F.3d 1088 (9th Cir. 1994) 21

6 *FTC v. Sage Seminars, Inc.*, 1995 U.S. Dist. LEXIS 21043 (N.D. Cal. 1995) 20, 25

7 *FTC v. Seismic Entertainment Productions*, No. 04-377-JD (D.N.H. Oct. 12, 2004) 11, 21

8 *FTC v. Silueta Distributors, Inc.*, 1994 U.S. Dist. LEXIS 10095 (N.D. Cal. 1994) 20, 25

9 *FTC v. Trustsoft, Inc.*, No. H-05-1905 (S.D. Tex. Nov. 30, 2005) 11

10 *FTC v. U.S. Oil & Gas Corp.*, 748 F.2d 1431 (11th Cir. 1984) 19, 26, 27

11 *FTC v. Windward Marketing, Ltd.*, 1997 U.S. Dist. LEXIS 17114, at *32 (N.D. Ga., Sept. 30
1997) 21, 22, 23

12 *FTC v. World Wide Factors, Ltd.*, 882 F.2d 344 (9th Cir. 1989) 19, 24, 27

13 *HUD v. Cost Control Mktg. & Sales Mgmt. of Va.*, 64 F.3d 920 (4th Cir. 1995) 31

14 *In re Vuitton et Fils*, 606 F.2d 1 (2d Cir. 1979) 28

15 *Kemp v. Peterson*, 940 F.2d 110 (4th Cir. 1991) 28

16 *Nat'l Org. for Reform of Marijuana Laws v. Mullen*, 828 F.2d 536 (9th Cir. 1987) 28

17 *Orkin Exterminating Co., Inc. v. FTC*, 849 F.2d 1354 (11th Cir. 1988) 23

18 *SEC v. International Swiss Inv. Corp.*, 895 F.2d 1272 (9th Cir. 1990) 27

19 *SEC v. R.J. Allen & Assoc., Inc.*, 386 F. Supp. 866 (S.D. Fla. 1974) 25

20 *U.S. v. First Nat'l City Bank*, 379 U.S. 378 (1965) 27

21 *United States v. Diapulse Corp. of Am.*, 457 F.2d 25 (2d Cir. 1972) 25

22

23

24 **Other Authority**

25 Brian Krebs, *Host of Internet Spam Groups Is Cut Off*, available online at
26 [http://www.washingtonpost.com/wp-dyn/content/
27 article/2008/11/12/AR2008111200658.html](http://www.washingtonpost.com/wp-dyn/content/article/2008/11/12/AR2008111200658.html) (last visited May 28, 2009) 4

28 CERT Coordination Center, *Botnets as a Vehicle for Online Crime*,
<http://www.certorg/archive/pdf/Botnets.pdf> (last visited May 28, 2009) 5, 6

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Fed. R. Civ. P. 65(b) 26, 27

Fed. R. Civ. P. 65(c) 19

Fed. R. Civ. Pro. 65(d)(2) 28

<http://samspace.org/d/ipdns.html> (last visited May 29, 2009) 3

ICQ Company, <http://www.icq.com/products/whatisicq.html> (last visited May 28, 2009) 4

Letter from the FTC to Hon. Wendell Ford and Hon. John Danforth, Committee on Commerce, Science, and Transportation, United States Senate, Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction, appended to *International Harvester Co.*, 104 F.T.C. 949, 1064 (1984) (“Unfairness Statement”) 20, 22

Marshall8e6, *Are Bots About to Bring Down Your Business?*, http://www.marshall8e6.com/documents/pdfs/white_papers/business/WP_BotsBringDownBusiness.pdf (last visited May 28, 2009) 6

Stefanie Olsen, Exposing Click Fraud, available online at http://news.cnet.com/Exposing-click-fraud/2100-1024_3-5273078.html (last visited May 29, 2009) 6

Tim Ferguson, *Security Experts: Botnets Biggest Threat on Net*, ZDNet UK, Apr. 11, 2008, <http://news.zdnet.co.uk/security/0,1000000189,39384066,00.htm> (last visited on May 28, 2009) 6

Wikipedia, <http://en.wikipedia.org/wiki/ICQ> (last visited May 28, 2009) 4

Wikipedia, http://en.wikipedia.org/wiki/Click_fraud (last visited May 29, 2009) 6

1 **I. SUMMARY**

2 Plaintiff Federal Trade Commission (“FTC” or “Commission”) seeks an *ex parte*
3 temporary restraining order (“TRO”) to stop a rogue Internet Service Provider controlled by
4 overseas criminals from continuing to harm U.S. consumers. As described in depth below,
5 defendant Pricewert LLC (“Defendant,” “Pricewert,” or “3FN”) operates Triple Fiber Network,
6 an Internet hosting provider that recruits, knowingly hosts, and actively participates in the
7 distribution of, illegal, malicious, and harmful electronic content, including child pornography,
8 malicious software, and the servers used to control networks of compromised computers known
9 as botnets.

10 Because the Defendant has gone to considerable lengths to hide from law enforcement,
11 and is engaged in outright criminal activity that is causing massive consumer injury, the
12 Commission seeks an *ex parte* temporary restraining order that would, *inter alia*, immediately
13 disconnect the Defendant’s servers from the Internet, impose an asset freeze, and order the
14 preservation of evidence. Defendant’s history of criminal conduct,¹ extensive efforts to hide
15 from law enforcement, and refusal to cease its injurious activity despite calls from consumers
16 and the Internet security community, demonstrates its propensity to violate the law and to
17 disregard any order to refrain from dissipating or concealing assets or destroying documents if
18 given advance notice of this lawsuit. Moreover, advance notice to the Defendant prior to the
19 disconnection of its servers would likely result in the Defendant and its criminal clientele
20 transferring their illegal, malicious and harmful electronic content to other Internet providers,
21 which would render much of the relief requested in the Temporary Restraining Order moot and
22 would cause significant harm to consumers. Accordingly, immediate, *ex parte* relief is critical to
23

24 ¹It is the Commission’s understanding that a parallel criminal investigation of the
25 Defendant is underway. Although the Commission is not privy to the details of that
26 investigation, the Commission is informed that a search warrant will be executed at the
27 Defendant’s data center on or about Wednesday, June 3, 2009. The Commission respectfully
28 requests that this Court rule on the Commission’s *Ex Parte* Motion for Temporary Restraining
Order prior to June 3, 2009, so that – if the Commission’s Motion is granted – service of the
TRO can be effected at the same time the search warrant is executed.

1 bringing a halt to Defendant's conduct, and to protect Defendant's assets for possible consumer
2 redress or disgorgement pending final resolution of this matter.

3 **II. THE PARTIES**

4 **A. Plaintiff**

5 Plaintiff, FTC, is an independent agency of the United States government created by the
6 FTC Act, 15 U.S.C. §§ 41-58 (2006). The FTC is charged with, among other things,
7 enforcement of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or
8 deceptive acts or practices in or affecting commerce. The FTC is authorized to initiate federal
9 district court proceedings, by its own attorneys, to enjoin violations of the FTC Act, and to
10 secure such equitable relief as may be appropriate in each case, including restitution and
11 disgorgement. 15 U.S.C. § 53(b) (2006).

12 **B. Defendant**

13 Defendant Pricewert is a shell company created by the overseas criminals that operate the
14 Internet Service Provider known as "Triple Fiber Network" or "3FN." Pricewert is an Oregon
15 limited liability company, which reports its principal place of business as 35 Barrack Road,
16 Belize City, Belize, in corporate filings with the State of Oregon. Drexler Decl., Ex. 7, ¶ 23. In
17 its filings, Pricewert states that its only members are two Belizean companies, both of which
18 share the same Barrack Road address in Belize as Pricewert. *Id.* No individuals, other than an
19 employee of "Registered Agents Ltd.," appear in Pricewert's filings. *Id.*

20 Pricewert is the owner and registrant of the 3FN.net domain name. Drexler Decl., Ex. 7,
21 ¶ 5. Visitors to pricewert.com, moreover, are redirected to the 3FN.net website. Drexler Decl.,
22 Ex. 7, ¶ 12. Pricewert also operates under a series of aliases, including Triple Fiber Network,
23 APS Telecom, APX Telecom, APS Communications, and APS Communication, all of which
24 have been linked to Pricewert by the FTC. *See* Drexler Decl., Ex. 7, ¶¶ 3-20, 23-25; *See also*
25 Linford Decl., Ex. 4, ¶¶ 7-12.

26 A significant number of Pricewert's computer servers are located at Data Pipe, a third-
27 party data center located in San Jose. Zadig Decl., Ex. 1, ¶ 9. In addition, Pricewert lists a series
28

1 of addresses in the San Jose area in its registration information for its various websites and
2 Internet Protocol (“IP”) ranges.² See Drexler Decl., Ex. 7, ¶¶ 5, 7, 8, 9, 11, 13-14, 17, and 24.
3 Pricewert also lists a San Jose area code (408) as the phone number on its website, and boasts on
4 its webpage that its servers are located in the “heart of the Silicon Valley.” Drexler Decl., Ex. 7,
5 ¶¶ 24, 25.

6 **III. THE DEFENDANT’S BUSINESS PRACTICES**

7 Pricewert recruits and colludes with criminals seeking to distribute illegal, malicious and
8 harmful electronic content via the Internet. Pricewert offers these criminals a full service
9 Internet hosting facility that welcomes content no legitimate Internet Service Provider would
10 ever willingly host. This content includes a witches’ brew of child pornography, botnet
11 command and control servers, spyware, viruses, trojans, phishing-related sites, and pornography
12 featuring violence, bestiality, and incest. In addition to recruiting and willingly distributing this
13 illegal, malicious and harmful content, Pricewert actively colludes with its criminal clientele in
14 several areas, including the maintenance and deployment of networks of compromised
15 computers known as botnets.

16 In order to provide this Court with a full picture of Pricewert’s harmful activities, the
17 FTC has recruited a distinguished panel of Internet security experts, who have submitted
18 declarations in support of the FTC’s suit. The evidence assembled by these experts, combined
19 with evidence collected during the FTC’s investigation of Pricewert, provides overwhelming
20 proof that Pricewert is engaged in conduct that violates Section 5 of the FTC Act.

21 **A. Special Agent Sean Zadig, NASA Office of Inspector General, Computer 22 Crime Division**

23 Special Agent Sean Zadig works in the Computer Crime Division of the National
24 Aeronautics and Space Administration’s (“NASA”) Office of Inspector General. Zadig Decl.,

25
26 ²An IP address is a unique, 32 bit number assigned to every computer connected to the
27 Internet, and expressed as four eight bit numbers, written in decimal and separated by periods.
28 For example 151.196.75.10. See <http://samspade.org/d/ipdns.html> (last visited May 29, 2009). A
IP range or block is a collection of many IP addresses. *Id.*

1 Ex. 1, ¶ 1. Zadig first encountered 3FN as part of an investigation into a series of computer
2 intrusions at NASA. Zadig Decl., Ex. 1, ¶ 5. Zadig traced those intrusions to a number of
3 computer servers hosted by a now defunct ISP by the name of McColo. *Id.* McColo was a
4 notorious haven for criminal activity that was shut down after its upstream Internet providers
5 were approached by a Washington Post reporter and provided with evidence of the volume of
6 malicious content McColo was hosting. *Id.* See also Brian Krebs, *Host of Internet Spam Groups*
7 *Is Cut Off*, Wash. Post, [http://www.washingtonpost.com/wp-dyn/content/article/2008/11/12/](http://www.washingtonpost.com/wp-dyn/content/article/2008/11/12/AR2008111200658.html)
8 [AR2008111200658.html](http://www.washingtonpost.com/wp-dyn/content/article/2008/11/12/AR2008111200658.html) (last visited May 28, 2009).

9 1. The Discovery of the ICQ Logs

10 Pursuant to a federal search warrant, Zadig copied the contents of several McColo servers
11 connected to the computer intrusions at NASA, and proceeded to analyze the data recovered.
12 Zadig Decl., Ex. 1, ¶¶ 5-6. In analyzing the data, Zadig discovered a series of connections
13 between McColo and 3FN, including malicious software located on McColo servers
14 communicating with 3FN servers. Zadig Decl., Ex. 1, ¶ 8.

15 One of the McColo servers Zadig analyzed contained a number of ICQ instant message
16 logs -- transcripts of instant message conversations between various parties that were relayed
17 through the McColo server. Zadig Decl., Ex. 1, ¶ 6. These logs contain, *inter alia*, the unique
18 ICQ number of each participant in the chat, the time and date of each message, and the content
19 of the messages. Zadig Decl., Ex. 1, ¶¶ 6, 10. Although the messages were in Russian, Zadig
20 was able to connect two of the chat participants to 3FN through their unique ICQ identifiers. *Id.*

21 Each user of ICQ is assigned a unique identifier or “handle” upon first registering to use
22 the program.³ Zadig connected two of the ICQ handles that appeared in the chat logs to 3FN:
23 331226 and 126254. Zadig Decl., Ex. 1, ¶ 10. Zadig learned from 3FN’s website that 331226 is
24 the unique ICQ handle assigned to 3FN’s “Head of Programming Department.” *Id.* On its
25 website, 3FN advertises “24h[our] ICQ Support” and encourages users to contact its Head of
26

27 ³ See ICQ Company, <http://www.icq.com/products/whatisicq.html> (last visited May 28,
28 2009); ICQ, available online at <http://en.wikipedia.org/wiki/ICQ> (last visited May 28, 2009).

1 Programming Department using ICQ identifier 331226. Zadig Decl., Ex. 1, ¶ 10, Drexler Decl.,
2 Ex. 7, ¶ 21. Zadig also queried the official website of the ICQ network for information about the
3 user assigned the ICQ identifier 331226. Zadig Decl., Ex. 1, ¶ 10. This query returned a profile
4 describing the user as “TAiNT, Ukraine, 35yo male.” *Id.*

5 Zadig also connected a second ICQ identifier found in the chats, 126254, to 3FN. Zadig
6 Decl., Ex. 1, ¶ 10. This identifier was used by an individual promoting 3FN’s services in an
7 online spam forum⁴ located at the website *crutop.nu*. *Id.* This individual identified himself as
8 3FN’s “Senior Project Manager” and utilized the ICQ identifier 126254. Zadig Decl., Ex. 1, ¶¶
9 6-7, 10.

10 Although the chats found by Zadig appeared to be in Russian, Zadig was able to use a
11 free translation service offered by Google to get a rough idea of the contents of the messages.
12 Zadig Decl., Ex. 1, ¶ 6. Although the translation was imperfect, Zadig was able to discern that
13 the logs contained a series of discussions between the above-referenced 3FN employees and
14 individuals seeking 3FN’s assistance in configuring and deploying networks of compromised
15 computers, known as botnets. Zadig Decl., Ex. 1, ¶¶ 6-7, 10.

16 2. Botnet and Click Fraud Basics

17 A botnet is a network of computers, which have been compromised with malicious code
18 and enslaved by the originator of the botnet, known as the bot herder. Zadig Decl., Ex. 1, ¶ 7;
19 CERT Coordination Center, *Botnets as a Vehicle for Online Crime*, at 11,
20 <http://www.cert.org/archive/pdf/Botnets.pdf> (last visited May 28, 2009). Typically, users whose
21 computers have been conscripted into a botnet are unaware that their computers have been
22 compromised. Zadig Decl., Ex. 1, ¶ 7.

23 In order to command his army of compromised computers, the bot herder utilizes a
24 computer server known as a “command and control” server or “C&C.” *Id.* Upon being
25 compromised by malicious code, infected computers are instructed to communicate with the

26
27 ⁴ See Warner Decl., Ex. 2 ¶ 11 (discussing spam section of *crutop.nu*); see also Drexler
28 Decl., Ex. 7, ¶ 30.

1 command and control server and follow whatever instructions are received. *Id.*; Turner Decl.,
2 Ex. 6, ¶ 25. By relaying commands through the C&C, the bot herder is able to remotely control
3 a vast network of compromised computers, and use those computers for a variety of nefarious
4 purposes, including the sending of spam, the distribution of malicious software, click fraud, and
5 denial of service attacks. *Id.*; CERT Coordination Center, *Botnets as a Vehicle for Online*
6 *Crime*, at 7-16, <http://www.cert.org/archive/pdf/Botnets.pdf> (last visited May 28, 2009)

7 The rise of botnets has been recognized as the most serious security threat facing the
8 Internet. *See, e.g.*, Tim Ferguson, *Security Experts: Botnets Biggest Threat on Net*, ZDNet UK,
9 Apr. 11, 2008, <http://news.zdnet.co.uk/security/0,1000000189,39384066,00.htm> (last visited on
10 May 28, 2009). Among other harms, experts estimate that botnets are responsible for
11 approximately 85% of spam sent worldwide. *See, e.g.*, Marshall8e6, *Are Bots About to Bring*
12 *Down Your Business?* at 2, [http://www.marshal8e6.com/documents/pdfs/](http://www.marshal8e6.com/documents/pdfs/white_papers/business/WP_BotsBringDownBusiness.pdf)
13 [white_papers/business/WP_BotsBringDownBusiness.pdf](http://www.marshal8e6.com/documents/pdfs/white_papers/business/WP_BotsBringDownBusiness.pdf) (last visited May 28, 2009). Operating
14 a botnet is illegal, and in many cases, punishable as felony. *See* 18 U.S.C. § 1030 (2006).

15 Click fraud, one of the many uses for a botnet, is a type of Internet crime that occurs in
16 connection with pay per click online advertising when an automated script or computer program
17 imitates a legitimate user of a web browser clicking on an ad, for the sole purpose of generating
18 a charge per click without having actual interest in the target of the ad's link. *See, e.g.*, Stefanie
19 Olsen, *Exposing Click Fraud*, CNET News, [http://news.cnet.com/Exposing-click-fraud](http://news.cnet.com/Exposing-click-fraud/2100-1024_3-5273078.html)
20 [/2100-1024_3-5273078.html](http://news.cnet.com/Exposing-click-fraud/2100-1024_3-5273078.html) (last visited May 29, 2009); "Click Fraud," Wikipedia,
21 http://en.wikipedia.org/wiki/Click_fraud (last visited May 29, 2009). Click fraud is a crime in
22 many jurisdictions, including California, where it is a felony. *See* Cal. Penal Code § 502 (2008).

23 3. The Translated ICQ Logs

24 The ICQ logs located by Agent Zadig were provided to the FTC and submitted to a
25 translator, who translated the logs from Russian to English. Zadig Decl., Ex. 1, ¶¶ 10-11,
26 Drexler Decl., Ex. 7, ¶ 27. The translated ICQ logs contain a series of admissions by 3FN's
27 senior staff that definitively link 3FN to illegal and injurious botnet and click fraud activity.

1 In one of the ICQ chats dated July 15, 2008, 3FN's Head of Programming engages in a
 2 conversation with a customer regarding the number of compromised computers the customer
 3 controls. Drexler Decl., Ex 7 at p. 361-362. The customer informs 3FN that he controls a total
 4 of 200,000 compromised computers, with 20,000 online and available for use at the time of the
 5 chat. Id. The customer then offers this massive network of bots to 3FN. The head of 3FN's
 6 Programming Department agrees to work with the customer, but complains upon learning of the
 7 size of the botnet that it will require a lot of effort. Id. at p. 361. The substance of the chat
 8 between 3FN and its customer is reproduced below:

FROM	TO	
Head of 3FN Programming Department	Customer	Bro, I am on my way home Shall we put off till tomorrow?
Customer	Head of 3FN Programming Department	lets do tomorrow, we have not configured it today yet
Head of 3FN Programming Department	Customer	I see Do you have big botnet?
Customer	Head of 3FN Programming Department	can reach 20k online sometimes even more
Head of 3FN Programming Department	Customer	what about geography?
Customer	Head of 3FN Programming Department	will tell you for sure 200k bots reached today, 15% of them are USA - Europe-Australia
Head of 3FN Programming Department	Customer	I got it, that's somewhere normal
Customer	Head of 3FN Programming Department	yep, bots are waiting for you)
Head of 3FN Programming Department	Customer	It's a lot of fucking work

26 In another chat, dated June 17, 2008, a Senior Project Manager for 3FN is approached by
 27 a customer seeking to work with 3FN on "botnet and clicker" – the use of a botnet to commit
 28

1 click fraud. Drexler Decl., Ex. 7 at pg. 365-366. 3FN’s Senior Project Manager inquires about
 2 the size of the botnet and asks if 3FN will need to write the software to control it. Id. at p. 366.
 3 Upon learning these details, 3FN’s Senior Project Manager reassures the customer that “we can
 4 manage it” and then proceeds to explain to the customer that 20,000 active bots are needed in
 5 order to generate \$500/day through click fraud. The substance of the chat is reproduced below:

FROM	TO	
Customer	3FN’s Senior Project Manager	Do you want to work with me at clicker [software]?)
3FN’s Senior Project Manager	Customer	If you have something to offer me . . .
Customer	3FN’s Senior Project Manager	botnet and clicker
3FN’s Senior Project Manager	Customer	what is the size of botnet? do we have to write software from the beginning?
Customer	3FN’s Senior Project Manager	Software remains version for beginning of this year botnet is approx. 20 000 clicks now and keeps on growing
3FN’s Senior Project Manager	Customer	Well, we can manage it To earn 500 USD per day you need to have 20 000 clicks approx.

18 4. Zadig’s Analysis of the Content Hosted by 3FN

19 In an effort to quantify the scope of illegal, malicious, and harmful content currently and
 20 historically hosted by 3FN, Agent Zadig prepared an analysis of the websites and other content
 21 hosted at the various Internet Protocol ranges assigned to 3FN. Zadig Decl., Ex. 1, ¶¶ 12-19.
 22 Agent Zadig conducted his analysis by entering each IP address controlled by 3FN into several
 23 databases, as well as a network mapping tool, and the Google search engine. Zadig Decl., Ex. 1,
 24 ¶¶ 12-13. Agent Zadig then recorded any reports of illegal, malicious or harmful content into a
 25 spreadsheet. Zadig Decl., Ex. 1, ¶ 13. The completed spreadsheet, which is attached to Zadig’s
 26 declaration as Exhibit 1, establishes that 3FN hosts a massive amount of content that harms
 27 consumers. Among other harmful content, Zadig found: botnet command and control servers,
 28

1 websites engaged in the hijacking of users' web browsers; websites engaged in search engine
2 optimization (SEO) ploys (spamming and other techniques used to artificially inflate the ranking
3 of a website); illegal online pharmacies; malware distribution sites; intellectual property theft
4 (MP3 and movie filesharing and downloads); sites featuring investment and currency trading
5 scams; hacking-related sites; rogue anti-virus products; and sites distributing trojan horses.

6 Zadig Decl., Ex. 1, at Att. A.

7 Indeed, 3FN's network is so full of malicious content that, while mapping the content
8 that 3FN hosts, Zadig's own computer was repeatedly infected with malicious software
9 originating from sites hosted by 3FN. Zadig Decl., Ex. 1, ¶ 16. One of the resulting infections
10 forced Zadig to completely rebuild his computer. *Id.*

11 5. Attacks on NASA Originating From 3FN

12 In another effort to quantify the harm originating from 3FN, Agent Zadig searched
13 NASA's agency-wide database of incidents of computer intrusions and infections impacting
14 NASA computers. Zadig Decl., Ex. 1, ¶¶ 20-22. Zadig searched the database for any incidents
15 traceable to IP addresses controlled by 3FN. Zadig Decl., Ex. 1, ¶ 20. The query found 22
16 separate attacks on NASA computers originating from IP addresses controlled by 3FN, including
17 five attacks in 2009, one as recently as April of 2009. Zadig Decl., Ex. 1, ¶¶ 20-21. Several of
18 these attacks involved efforts to conscript NASA computers into a botnet. Zadig Decl., Ex. 1, ¶
19 21. Zadig estimates that NASA has spent more than \$14,000 to repair the damage to NASA's
20 systems that originated from servers hosted by 3FN. Zadig Decl., Ex. 1, ¶ 22.

21 **B. Gary Warner, Director of Research in Computer Forensics, University of 22 Alabama at Birmingham**

23 Gary Warner is the Director of Research in Computer Forensics at the University of
24 Alabama at Birmingham. Warner Decl., Ex. 2, ¶ 1. Warner has substantial expertise in the
25 fields of computer forensics, computer security, and cybercrime, and is the recipient of
26 numerous awards and other recognitions for his work, including his designation as a Microsoft
27 MVP in Enterprise Security – one of only 57 individuals in the world to be so designated. *Id.*

1 As part of his job responsibilities at the University of Alabama, Warner and his staff of
2 researchers track and analyze spam for evidence of criminal activity. Warner Decl., Ex. 2, ¶ 2.
3 Based on this work, Warner has become familiar with a number of Internet Service Providers
4 (“ISPs”) that host unusually high concentrations of criminal activity. *Id.* Two of these ISPs –
5 McColo and InterCage – were shut down after their upstream providers learned of the amount of
6 criminal activity they were hosting. *Id.* In the wake of these shutdowns, Warner believes that
7 3FN (known to him as APS Telecom) is now the worst ISP located in the United States in terms
8 of hosting malicious content. *Id.*

9 1. The Illegal, Harmful and Malicious Content Hosted by 3FN

10 To support his conclusion that 3FN is the worst domestic ISP in terms of hosting criminal
11 activity, Warner analyzed the various websites and other content 3FN hosts. *Id.* As described in
12 great depth in his declaration, and summarized below, Warner located a remarkably wide range
13 of illegal, harmful and malicious content hosted by 3FN.

14 a. Malicious Botnet Software

15 As part of his spam analysis work, Warner tracked a cluster of spam messages that
16 invited users to visit a series of webpages offering pornographic content. Warner Decl., Ex. 2, ¶
17 3. Warner determined that users who visited these pages were instructed to download a video
18 player, which was actually malicious software hosted by 3FN. *Id.* Users who agreed to
19 download the software unwittingly exposed their computers to malicious code that compromised
20 their computers and conscripted them into a botnet. *Id.*

21 By studying this malicious code, Warner was able to determine how to access the 3FN-
22 hosted website associated with the code, and view the tracking statistics maintained by the
23 criminals controlling the botnet. *Id.* These statistics showed that thousands of computers had
24 been compromised by the malicious code located by Warner. *Id.*

25 b. Child Pornography

26 Warner located more than 40 websites hosted by 3FN that are possible hosts of child
27 pornography, including several with domain names designed to appeal to those seeking such
28

1 content, including: *young-girl-sex.net*, *little-beauty.com*, *little-lady.info*, *little-incest.com*, *littles-*
2 *raped.com*, and *DrIncest.com*. Warner Decl., Ex. 2, ¶ 4. Although Warner did not visit these
3 sites due to their content, he did perform traffic analysis on several of the sites, and viewed one
4 of the sites with a text-only browser. Warner Decl., Ex. 2, ¶¶ 5-7. This analysis revealed a
5 strong correlation between visits to “*little-lady.info*” and the search term “nude little preteen
6 angels.” Warner Decl., Ex. 2, ¶¶ 5-6. Moreover, by viewing *little-incest.com* with a text-based
7 browser, Warner was able to confirm that the 3FN-hosted site contains the following text
8 “ILLEGAL PHOTOS OF LITTLE GIRLS - just 3 steps,” “VERY LITTLE SCHOOLGIRLS
9 RAPED,” and “more than 10 free samples of tiny schoolgirls being forced...”. Warner Decl., Ex.
10 2, ¶ 7.

11 c. Fake Anti-Virus Products

12 Warner uncovered several 3FN-hosted websites engaged in the selling of fake or “rogue”
13 antivirus: software that falsely informs consumers that their computers are infected with
14 malicious software and urges them to purchase the rogue anti-virus product in order to eliminate
15 the infection. Warner Decl., Ex. 2, ¶ 8. The FTC is currently litigating a suit against one of the
16 major purveyors of such software, and has a long history with this type of deceptive software.
17 *See, e.g., FTC v. Innovative Marketing*, Civ. No. RDB-08-CV-3233 (D. Md. Dec. 2, 2008); *FTC*
18 *v. MaxTheater, Inc.*, No. 05-CV-0069 (E.D. Wa. Dec. 6, 2005); *FTC v. Trustsoft, Inc.*, No. H-05-
19 1905 (S.D. Tex. Nov. 30, 2005); *FTC v. Seismic Entertainment Productions*, No. 04-377-JD
20 (D.N.H. Oct. 12, 2004).

21 d. Illegal Online Pharmacies

22 Warned discovered numerous online pharmacies hosted at 3FN, all of which appear to be
23 illegal, including *BuyCialisWithoutAPrescription.net*, *BuyValiumNoRX.com*, and
24 *BuyDrugsOnlineNoPrescriptionNecessary.net*. Warner Decl., Ex. 2, ¶ 13.

25 e. Pirated Music and Software

26 Warner lists in his declaration a variety of sites hosted by 3FN that are distributing
27 pirated software and music. Warner Decl., Ex. 2, ¶¶ 10, 12. These sites include *mp3-mass.com*,

1 which sells current music by popular artists such as Kanye West, Britney Spears, and Fergie for
2 20 cents per song, and \$3 per album – far below what legitimate websites charge. Warner Decl.,
3 Ex. 2, ¶ 10. Similarly, software sites like 3FN-hosted *cheapoemstore.com* sell popular software,
4 including products from Adobe and Microsoft, at 10 to 20 percent of their retail value. Warner
5 Decl., Ex. 2, ¶ 12.

6 2. 3FN Actively Recruits Criminals

7 In an effort to understand how so much illegal content could exist at one ISP, Warner
8 began visiting websites where criminals share techniques and strategies with one another.
9 Warner Decl., Ex. 2, ¶ 11. One of the websites Warner visited is *crutop.nu*, which is itself
10 hosted by 3FN. *Id.* *Crutop.nu* is a Russian language website that features a variety of discussion
11 forums that focus on making money from spam. *Id.*

12 Warner discovered that representatives of 3FN are active participants in the *crutop.nu*
13 forums, and that 3FN advertises its services in banner ads placed on *crutop.nu*. *Id.* An
14 individual who identifies himself as 3FN’s “Senior Project Manager” has posted 3,440 messages
15 in the *crutop* forums. *Id.* In one exchange between 3FN’s Senior Project Manager and a user
16 identified as “Rett,” Rett asks if he can host “Rape and Incest sites on 3FN.” The response from
17 3FN: “Yes of course.” *Id.*

18 C. Sarah Ohlsen, Supervisor, Exploited Children Division, 19 The National Center for Missing and Exploited Children

20 Sarah Ohlsen is a Supervisor in the Exploited Children Division of the The National
21 Center for Missing and Exploited Children (“NCMEC”). Ohlsen Decl., Ex. 3, ¶ 1. NCMEC
22 serves as a clearinghouse for reports of child exploitation, including reports of child
23 pornography. Through its “CyberTipline” and “CyberTipline II” – which Ohlsen supervises –
24 NCMEC enables members of the public, electronic service providers, and law enforcement to
25 report, *inter alia*, images containing child pornography found online. Ohlsen Decl., Ex. 3, ¶¶ 2 -
26 4.

1 All reports to NCMEC's CyberTiplines are assigned to a NCMEC analyst, who reviews
2 the material alleged to be child pornography and makes a determination whether the specified
3 image is indeed "apparent child pornography." Ohlsen Decl., Ex. 3, ¶¶ 3 - 5. Although NCMEC
4 is not a law enforcement organization, NCMEC's reports are routinely shared with criminal law
5 enforcement, and NCMEC is often called upon by criminal law enforcement to analyze images
6 of suspected child pornography. Ohlsen Decl., Ex. 3, ¶¶ 2 - 3

7 At the FTC's request, NCMEC searched its database for CyberTipline reports associated
8 with IP ranges controlled by 3FN and a series of websites hosted by 3FN. Ohlsen Decl., Ex. 3, ¶
9 6. In those cases where NCMEC located a CyberTipline report, NCMEC consulted the
10 associated NCMEC analyst report to determine if the NCMEC analyst was able to confirm the
11 report. Ohlsen Decl., Ex. 3, ¶¶ 6 - 7.

12 Ohlsen's declaration paints a highly disturbing picture. In response to the FTC's query,
13 Ohlsen found that NCMEC's CyberTiplines received more than 700 reports of child
14 pornography hosted at 3FN. Ohlsen Decl., Ex. 3, ¶ 7. In more than 500 different cases,
15 NCMEC's analysts were able to confirm that the reported website did indeed contain apparent
16 child pornography. *Id.*

17 Moreover, a review of the reports attached to Ohlsen's declaration shows that 3FN has
18 consistently hosted child pornography over a long period of time. The earliest CyberTipline
19 reports concerning 3FN's hosting of child pornography date back to 2004; the most recent to
20 May 21, 2009. Ohlsen Decl., Ex. 3, ¶ 7 and Appendix B to Ohlsen Decl. at line "# 1" (Ex. pg.
21 183) and line "# 329" (Ex. 3 pg. 201).

22 **D. Steve Linford, Founder, The Spamhaus Project**

23 Steve Linford is the founder of the Spamhaus Project, one of the world's preeminent anti-
24 spam organizations. Linford Decl., Ex. 4, ¶¶ 2-3. Spamhaus fights spam by tracking spam
25 activity via its own network of sensors and data sources and then compiling lists of Internet
26 Protocol addresses associated with spam activity. Linford Decl., Ex. 4, ¶ 4. These IP addresses
27 are added to the Spamhaus Blocklist ("SBL"), which is widely used by ISPs around the world.

1 Linford Decl., Ex. 4, ¶¶ 4-5. ISPs use the SBL, along with other data, to determine which IP
2 ranges to block from their network. Linford Decl., Ex. 4, ¶ 4.

3 At the time an IP address is added to the SBL, Spamhaus generates and transmits an
4 abuse complaint to the network responsible for the cited IP. Linford Decl., Ex. 4, ¶ 6. If the
5 network responsible for the IP address takes action to remove the offending content hosted at the
6 cited IP, Spamhaus will remove the IP address from the SBL. *Id.* In virtually every case, ISPs
7 respond to Spamhaus abuse complaints and take action to remove the spam-related content from
8 their network. *Id.*

9 Spamhaus has a long history with 3FN, and has sent 3FN more than 70 abuse reports
10 since 2005. Linford Decl., Ex. 4, ¶ 7. Spamhaus's abuse complaints to 3FN have been answered
11 by two individuals since 2007: "Sergey Dubenco" and "Nick Tooms." Linford Decl., Ex. 4, ¶ 8.
12 Both of these individuals appear to be located outside of the United States, possibly in Ukraine
13 or Estonia. Linford Decl., Ex. 4, ¶¶ 9-12.

14 Based on Spamhaus's interactions with 3FN, it is Linford's view that 3FN is actively
15 collaborating with and protecting its clients who are engaged in spam and botnet-related activity.
16 Linford Decl., Ex. 4, ¶¶ 13-20. Linford bases this conclusion on 3FN's interactions with
17 Spamhaus since 2007. Linford Decl., Ex. 4, ¶ 14. During that period, 3FN has demonstrated a
18 consistent "push a pawn" strategy, whereby 3FN feigns cooperation with Spamhaus by
19 temporarily removing offending websites and servers, only to reinstate them shortly after
20 Spamhaus has withdrawn the IP address from the SBL. *Id.* In several cases, 3FN has moved
21 offending websites to other IP addresses controlled by 3FN, in what Linford believes to be an
22 effort to evade detection by Spamhaus. *Id.*

23 Linford includes several examples of 3FN's suspect behavior in his declaration,
24 including an incident involving botnet command and control servers hosted by 3FN. Linford
25 Decl., Ex. 4, ¶¶ 15-19. Between November 2008 and March 2009, Spamhaus reported 17
26 different IP addresses controlled by 3FN that were home to botnet command and control servers.
27 Linford Decl., Ex. 4, ¶ 19. In Linford's view, this is a huge number of command and control
28

1 servers to be located on any one network in the same time frame, and puts 3FN in the same
2 category as McColo and Atrivo/Interage – two notorious rogue ISPs that were taken offline by
3 their upstream providers. *Id.*

4 In response to Spamhaus’s abuse complaints regarding the botnet command and control
5 servers, 3FN assured Spamhaus that the command and control servers located by Spamhaus had
6 been taken down. Linford Decl., Ex. 4, ¶¶ 17-18, 20. This assertion proved to be false. Data
7 collected by Andre’ DiMino (discussed below) establishes that at least five of the command and
8 control servers reported by Spamhaus – and purportedly taken down by 3FN – were not in fact
9 removed.

10 **E. Andre’ DiMino, Co-Founder and Director, The Shadowserver Foundation**

11 Andre’ DiMino is the Co-Founder and Director of The Shadowserver Foundation, a
12 group of security researchers that gather information on malicious software, botnet activity, and
13 compromised servers. DiMino Decl., Ex. 5, ¶ 2. As described in depth in DiMino’s declaration,
14 Shadowserver employs a comprehensive and regularly validated method of capturing and
15 logging information related to Internet-based malicious activity. DiMino Decl., Ex. 5, ¶¶ 3-10.

16 At the FTC’s request, DiMino queried the Shadowserver database for reports of
17 malicious activity originating from IP addresses controlled by 3FN. DiMino Decl., Ex. 5, ¶¶ 11-
18 12. DiMino’s query covered the time period January 1, 2008 through May 7, 2009. DiMino
19 Decl., Ex. 5, ¶ 13. During that period, DiMino found 311 unique IP addresses controlled by 3FN
20 that were found to be participating in, or facilitating, malicious activity. DiMino Decl., Ex. 5,
21 ¶¶ 14-15.

22 DiMino’s database search also revealed 4,576 unique malicious software programs
23 (“malware”) that use 3FN’s servers as a botnet command and control server. DiMino Decl., Ex.
24 5, ¶ 21. DiMino’s analysis of this malware found a range of malicious behavior, including
25 programs capable of keystroke logging, password stealing, data stealing, programs with hidden
26 backdoor remote control activity, and programs involved in spam distribution. DiMino Decl.,
27 Ex. 5, ¶ 22.

1 At the FTC's request, DiMino searched the Shadowserver database for evidence of
2 botnet command and control servers at a series of IP addresses provided by the FTC. DiMino
3 Decl., Ex. 5, ¶¶ 24-25. The FTC obtained these IP addresses from Spamhaus, which connected
4 them to botnet command and control activity, and reported them to 3FN in late 2008 and, in one
5 case, early 2009. As detailed in Steve Linford's declaration, 3FN responded to Spamhaus's
6 complaint and reported that these command and control servers were taken offline. DiMino's
7 data confirms that 3FN's representations to Spamhaus were false. In fact, the botnet command
8 and control servers purportedly taken down by 3FN continued to operate after the date 3FN told
9 Spamhaus they had been taken offline. DiMino Decl., Ex. 5, ¶¶ 26-30; Linford Decl., Ex. 4, ¶
10 19.

11 **F. Dean Turner, Director of the Global Intelligence Network, Symantec**
12 **Corporation**

13 Dean Turner is the Director of the Symantec Corporation's Global Intelligence Network.
14 Turner Decl., Ex. 6, ¶ 2. Among other responsibilities, Turner manages and co-authors
15 Symantec's annual Internet Threat Report, coordinates the research and analysis conducted on
16 attack data gathered from Symantec's network of Internet sensors, and manages Symantec's
17 DeepSight Analyst teams, which study cyber attacks and the vulnerability of systems to cyber
18 attacks. Turner Decl., Ex. 6, ¶¶ 2, 4.

19 Symantec's Global Intelligence Network database consists of information gathered by
20 Symantec's network of "infield sensors" – software and hardware managed by Symantec that
21 report Internet threat data back to Symantec as well as sensors in the control of third parties (for
22 example, users of Symantec's anti-virus software who have agreed to share data with Symantec.)
23 Turner Decl., Ex. 6, ¶ 2. At the FTC's request, Turner queried the Global Intelligence Network
24 databases by searching for cyber intrusions or attacks originating from IP addresses belonging to
25 3FN⁵ in the past six months. Turner Decl., Ex. 6, ¶ 9.

27 ⁵ A comparison of the IP ranges analyzed by Mr. Turner (*See* Turner Decl., Ex. 6, ¶ 9
28 (listing IP ranges)) with the IP ranges linked by FTC Investigator Drexler (*See* Drexler Decl., Ex.

1 Turner's query found more than 600 IP addresses controlled by 3FN launching a variety
2 of attacks, including a number of attacks capable of taking control of a user's computer. Turner
3 Decl., Ex. 6, ¶ 11 and Ex A to Turner Decl. Turner's query also revealed phishing⁶ and spam
4 activity originating from 3FN IP addresses (Turner Decl., Ex. 6, ¶¶ 29-32 and Exs. D and E. to
5 Turner Decl.), and 17 different 3FN IP addresses that housed botnet command and control
6 servers. Turner Decl., Ex. 6, ¶ 27 and Ex. C to Turner Decl.

7 **G. Sheryl Drexler, Investigator, Federal Trade Commission**

8 Sheryl Drexler is an investigator for the Federal Trade Commission. Drexler has more
9 than six years of experience investigating unfair and deceptive practices involving the Internet.
10 Drexler ¶ 1.

11 1. Aliases Used by Pricewert

12 By reviewing the defendant's domain and IP registration information, visting the
13 defendant's websites, and reviewing the defendant's corporate filings with the state of Oregon,
14 Drexler was able to link defendant's various aliases, including Triple Fiber Network, 3FN, APS
15 Telecom, APS Communication(s), and APX Telecom. Drexler Decl., Ex. 7, ¶¶ 3-20, 23-25.

16 2. Pricewert's Extensive Overseas Ties

17 Drexler was also able to confirm that although the defendant claims to be based in the
18 United States, it has extensive ties to eastern Europe, principally the Ukraine. The text on 3FN's
19 website contains awkward phrasing and frequent grammatical errors, which strongly suggests
20 that it was drafted by a non-native English speaker. Drexler Decl., Ex. 7, ¶ 8. Of the employees
21 the FTC has been able to track to a location, all are located in the Ukraine or Estonia. Drexler
22 Decl., Ex. 7, ¶¶ 22 and 26. Moreover, two telephone phone numbers listed on 3FN's website are
23

24 7, ¶ 15 and Attachment A to Drexler Dec. (listing IP ranges)) shows that Mr. Turner's analysis
25 was performed on IP ranges controlled by the Defendant.

26 ⁶Phishing is the use of email, Internet web sites, or other means, to mimic or copy the
27 appearance of a trustworthy entity for the purpose of duping consumers into disclosing personal
28 information, such as account numbers and passwords.

1 answered by individuals with Russian accents, and 3FN advertises in Russian-language forums
2 with ads in Russian. Drexler Decl., Ex. 7, ¶¶ 21-22, 30.

3 3. Pricewert's Marketing Efforts

4 Drexler located a number of 3FN banner advertisements on the website *crutop.nu*, a
5 Russian language site that includes forums for webmasters, including forums devoted to "Casino
6 Money," "Spam" and "Pharmacy." Drexler Decl., Ex. 7, ¶ 30. 3FN's ads appeared along side
7 those of other advertisers of dubious legality, including "IncestMoney.com." Drexler Decl., Ex.
8 7, ¶ 30.

9 4. Consumer Complaints Regarding 3FN

10 Drexler found a number of consumer complaints about 3FN posted in various online
11 forums and websites. Drexler Decl., Ex. 7, ¶ 31. Among other complaints, consumers accused
12 3FN of hosting spam, bots, child pornography, and rogue anti-virus products. *Id.* Moreover,
13 Drexler located a number of complaints about users being redirected to sites on 3FN's servers
14 without their consent, including a report that Oxford University's Department of Education
15 website was hacked to redirect users to graphic images of child pornography hosted by 3FN.
16 Drexler Decl., Ex. 7, ¶ 32.

17 5. Malicious Activity Originating from 3FN's Servers

18 In order to experience first hand the type of malicious activity hosted at 3FN, Drexler
19 visited a series of 3FN-hosted websites that purportedly contained malicious code according to
20 published reports. Drexler Decl., Ex. 7, ¶ 33. In eight different cases, Drexler's computer was
21 attacked by malicious code hosted by 3FN. *Id.* These attacks ranged from programs designed to
22 hijack users to malicious web sites, to a trojan designated as "InfoStealer.Banker.C" – a program
23 created to steal usernames and passwords for online bank accounts and other websites. Drexler
24 Decl., Ex. 7, ¶¶ 33-34.

1 **IV. ARGUMENT**

2 **A. The FTC Act Authorizes the Requested Relief**

3 “Section 13(b) [of the FTC Act] gives the Commission the authority to seek, and gives
4 the district court the authority to grant, permanent injunctions,” and “[i]t is clear that, because
5 the district court has the power to issue a permanent injunction to enjoin acts of practices that
6 violate the law enforced by the Commission, it also has authority to grant whatever preliminary
7 injunctions are justified by the usual equitable standards.” *FTC v. H.N. Singer, Inc.*, 668 F.2d
8 1107, 1111-13 (9th Cir. 1982). This “unqualified grant of statutory authority . . . carries with it
9 the full range of equitable remedies” *Id. Accord FTC v. U.S. Oil & Gas Corp.*, 748 F.2d
10 1431 (11th Cir. 1984) (per curiam); *FTC v. Amy Travel Serv., Inc.*, 875 F.2d 654, 571-72 (7th
11 Cir. 1989). The power of the Court pursuant to Section 13(b) is not limited to injunctive relief;
12 rather, it includes the authority to grant any ancillary relief necessary to accomplish complete
13 justice and preserve assets for rescission and restitution. *Singer*, 668 F.2d at 1112-14. This
14 ancillary relief can include appointment of a receiver, asset freezes, and expedited discovery. *Id.*
15 *Accord FTC v. American National Cellular, Inc.*, 810 F.2d 1511, 1514 (9th Cir. 1987).

16 In determining whether to grant a preliminary injunction under Section 13(b), a court “is
17 required to (i) weigh the equities; and (ii) to consider the FTC’s likelihood of ultimate success
18 before entering a permanent injunction.” *FTC v. World Wide Factors, Ltd.*, 882 F.2d 344, 346
19 (9th Cir. 1989). Unlike private litigants, the Commission need not prove irreparable injury in
20 order to obtain injunctive relief, because “harm to the public interest is presumed.” *Id.*⁷ Other
21 courts in this district and in other districts within the Ninth Circuit have granted similar
22 preliminary relief to the FTC.⁸

23
24 ⁷No security is required for issuance of a temporary restraining order or preliminary
25 injunction in this case because the FTC is an agency of the United States. *See* Fed. R. Civ. P.
26 65(c).

27 ⁸*See, e.g., FTC v. Dugger*, Civ. No. CV-06-0078-PHX-ROS (D. Ariz., Jan. 10, 2006)
28 (granting *ex parte* TRO requiring hosts to disconnect defendants’ computer equipment from
Internet, imposing an asset freeze, requiring records preservation, granting immediate access to

1 In its two-count complaint, the FTC has alleged that Pricewert has engaged and continues
2 to engage in unfair acts or practices that violate Section 5 of the FTC Act. See “Complaint for
3 Permanent Injunction, and Other Equitable Relief,” filed concurrently. As set forth below, in
4 this memorandum and its two attached volume of exhibits, the Commission presents ample
5 evidence that it will ultimately succeed on the merits of its Section 5 claims and that the balance
6 of equities favors the requested injunctive relief.

7 **B. The Commission Has Established a Likelihood of Succeeding on the Merits**
8 **of its Section 5 Claims that Pricewert Has Engaged in Unfair Acts or**
9 **Practices**

10 Counts One and Two of the FTC’s complaint allege that Pricewert has engaged in unfair
11 acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a). An act or practice
12 is unfair under Section 5 if: (1) it causes or is likely to cause substantial injury to consumers;
13 (2) the harm to consumers is not outweighed by any countervailing benefits; and (3) the harm is
14 not reasonably avoidable by consumers. 15 U.S.C. § 45(n).⁹ See, e.g., *FTC v. Neovi, Inc.*, 598 F.
15 Supp. 2d 1104 (S.D. Cal. 2008) (defendant’s creation and delivery of checks without a
16 reasonable level of verification that the customers had authority to draw checks on the specified

17
18 business premises, and requiring foreign asset repatriation) (copies of the complaint, TRO
19 memo, and TRO are included as Exhibits 8,9, and 10, respectively, in the Commission’s
20 accompanying two volumes of exhibits in support of the instant TRO motion); See also *FTC v.*
21 *ERG Ventures, LLC*, CV-06-00578 LRH-VCP (D. Nev. 2006) (granting *ex parte* TRO, asset
22 freeze, financial accounting, preservation of and expedited access to business records); *FTC v.*
23 *National Vending Consultants, Inc.*, CV-S-05-0160-RCJ-PAL (D. Nev. 2005) (granting *ex parte*
24 TRO, immediate access, asset freeze, and receiver); *FTC v. Enternet Media*, CV-05-7777 CAS-
25 AJWx (C.D. Cal. 2005)(granting *ex parte* TRO, immediate access, asset freeze, and financial
26 accounting); see also *FTC v. Sage Seminars, Inc.*, 1995 U.S. Dist. LEXIS 21043 (N.D. Cal.
27 1995) (granting preliminary injunction and asset freeze); *FTC v. Silueta Distributors, Inc.*, 1994
28 U.S. Dist. LEXIS 10095, *1 (N.D. Cal. 1994) (granting preliminary injunction).

⁹See also Letter from the FTC to Hon. Wendell Ford and Hon. John Danforth, Committee
on Commerce, Science, and Transportation, United States Senate, Commission Statement of
Policy on the Scope of Consumer Unfairness Jurisdiction, appended to *International Harvester*
Co., 104 F.T.C. 949, 1064 (1984) (“Unfairness Statement”).

1 bank accounts held unfair), *reh'g denied*, 2009 U.S. Dist. LEXIS 649 (2009), *appeal docketed*,
2 No. 09-55093 (9th Cir. Jan. 16, 2009).¹⁰

3 In satisfying the “substantial injury” prong of the unfairness test, it is well-settled in the
4 Ninth Circuit that “consumer injury is substantial when it is the aggregate of many small
5 individual injuries.” *FTC v. Pantron I Corp.*, 33 F.3d 1088, 1102 (9th Cir. 1994). *Accord FTC*
6 *v. J.K. Pubs. Inc.*, 99 F. Supp. 2d 1176, 1201 (C.D. Cal. 2000) (holding that “[i]njury may be
7 sufficiently substantial if it causes a small harm to a large class of people. *See also FTC v.*
8 *Crescent Publ’g Group, Inc.*, 129 F. Supp. 2d 311, 322 (S.D.N.Y. 1991) (finding that “injury to
9 consumers was substantial in the aggregate”). In addition, the “substantial injury prong can be
10 satisfied if the FTC establishes that consumers were injured by a practice for which they did not
11 bargain.” *J.K. Pubs.*, 99 F. Supp. 2d at 1201. The injury suffered by consumers need not be
12 monetary in nature. *See, e.g., Accusearch*, 2007 U.S. Dist. LEXIS 74905 at *22-23 (resources
13 expended changing phone carriers and upgrading account security held cognizable injury.)

14 Here, the FTC’s Complaint alleges that Pricewert has violated Section 5 of the FTC Act
15 by: (1) unfairly recruiting and willingly hosting electronic code or content that inflicts harm
16 upon consumers, including but not limited to, child pornography, botnet command and control
17 servers, spyware, viruses, trojans, and phishing-related sites; and (2) colluding with bot herders
18 to configure, deploy, or operate botnets comprised of thousands of compromised computers. As
19
20

21 ¹⁰*See also FTC v. Accusearch, Inc.*, 2007 U.S. Dist. LEXIS 74905 (D. Wyo. 2007)
22 (obtaining and selling of confidential customer phone records without the affected customers’
23 authorization held unfair), *appeal docketed*, No. 08-8003 (10th Cir. Jan. 9, 2008); *FTC v.*
24 *Seismic Entm’t Prods.*, 2004 U.S. Dist. LEXIS 22788 (D. N.H. 2004) (installation of software on
25 computers through web browser exploits without consumers’ knowledge held unfair); *FTC v.*
26 *Windward Marketing Ltd.*, 1997 U.S. Dist. LEXIS 17114 (N.D. Ga. 1997) (unauthorized bank
27 drafts on consumers’ accounts held unfair; company facilitated and provided substantial
28 assistance to co-defendants’ deceptive scheme by depositing unauthorized bank drafts on
consumers’ accounts into bank accounts opened in the names of fictitious magazines; company
knew drafts were not authorized or was on notice of high probability of fraud and consciously
avoided learning the truth).

1 established below, this conduct satisfies all of the elements required in order to establish
2 unfairness under Section 5 of the FTC Act.

3 1. Defendant's Conduct Causes or is Likely to Cause Substantial Injury to
4 Consumers

5 As detailed in the factual recitation above, Pricewert causes massive harm to consumers
6 through the content it recruits and distributes. These harms run the gamut from direct consumer
7 injury – including Pricewert's active participation in botnets that enslave consumers' computers
8 and put them to work for criminal ends, and its distribution of malicious software – to those
9 injuries less easy to quantify, but undoubtedly significant, such as Pricewert's hosting of child
10 pornography, pirated software and music, and participation in click fraud.

11 While the injury suffered by a given consumer as a result of Pricewert's conduct may
12 vary, the aggregate injury resulting from Pricewert's conduct is undoubtedly large. For example,
13 in the two ICQ chats discussed above, Pricewert agrees to manage and configure massive bot
14 networks of hundreds of thousands of enslaved computers. The aggregate injury to the hundreds
15 of thousands of consumers whose computers have been illegally conscripted into these botnets –
16 not to mention the public at large which will be targeted by these botnets – is immense.¹¹ Cf.
17 *FTC v. Dugger*, Civ. No. CV-06-0078-PHX-ROS (D. Ariz., Jan. 10, 2006) (granting FTC *ex*
18 *parte* TRO against individual charged with, *inter alia*, using networks of compromised
19 computers to distribute spam). See also Unfairness Statement, appended to *International*

20
21 ¹¹It is important to note that the Commission seeks to hold Pricewert liable for its *own*
22 unfair acts and practices, not those of third parties who use its services. Many Internet service
23 providers may, unknowingly, host unlawful content or provide services to third-parties who
24 cause consumers harm. Those ISPs do not significantly facilitate, provide substantial assistance
25 to, or materially contribute to the harmful activity. Pricewert, by contrast, does. Courts have
26 held other types of businesses liable under Section 5 when those businesses' own conduct, that
27 significantly facilitated, assisted, or contributed to third party fraudulent activity, met the
28 standard for unfairness under 15 U.S.C. § 45(n). See, e.g., *Neovi*, 598 F. Supp. 2d at *18-24
(rejecting defendants' claim that they "merely offered a 'morally neutral' software program" and
that third-party fraudsters manipulated their services to cause consumer harm; discussing similar
holdings in *Accusearch* and *Windward Marketing* cases), *reh'g denied*, 2009 U.S. Dist. LEXIS
649, *10-12 (same).

1 *Harvester Co.*, 104 F.T.C. 949, 1064 at 4-5 (recognizing that conduct that violates the law is
2 often harmful to consumers and therefore also unfair under the FTC Act.)

3 2. The Harm Pricewert Inflicts Upon Consumers Is Not Outweighed by any
4 Countervailing Benefits

5 The second prong of the unfairness test need not detain the Court long. There is simply
6 no countervailing benefit to either consumers or competition that results from Pricewert's
7 actions. Indeed, the only ones to benefit from Pricewert's activities are the Defendant itself –
8 who is paid by the criminals it caters to and collaborates with – and its criminal clientele, who
9 profit by harming consumers through stealing their account credentials, compromising their
10 computers, and blasting them with huge volumes of spam. *See J.K. Pubs*, 99 F. Supp. 2d at
11 1201; *FTC v. Windward Marketing, Ltd.*, 1997 U.S. Dist. LEXIS 17114, at *32 (N.D. Ga., Sept.
12 30 1997)(countervailing benefits prong of the unfairness test is easily satisfied when a practice
13 disadvantages consumers without an offsetting benefit to consumers or competition.).

14 3. The Harm Inflicted Upon Consumers Is Not Reasonably Avoidable

15 The third prong of the unfairness test requires the Court to consider if the harm caused by
16 the Defendant is reasonably avoidable by consumers. If consumers do not have a “free and
17 informed choice that would have enabled them to avoid the unfair practice, the injury was not
18 reasonably avoidable.” *J.K. Pubs*, 99 F. Supp. 2d at 1201 (*quoting FTC v. Windward Mktg.,*
19 *Ltd.*, 1997 U.S. Dist. LEXIS 17114, at *32 (N.D. Ga. Sept. 30, 1997) *and citing Orkin*
20 *Exterminating Co., Inc. v. FTC*, 849 F.2d 1354, 1365 (11th Cir. 1988)).

21 In this case, consumers not only lack a “free and informed choice” to avoid Pricewert's
22 unfair practices, they have no choice at all. In some cases, consumers are tricked into visiting
23 websites that distribute malicious code hosted by 3FN. Warner Decl., Ex. 2, ¶ 3 . In other cases,
24 consumers are redirected without their consent from legitimate websites to the harmful content
25 hosted by 3FN. Drexler Decl., Ex. 7, ¶ 32 . In still other cases, consumers' computers are
26 conscripted into a 3FN-controlled botnet, which occurs without their knowledge or consent.
27 Zadig Decl., Ex. 1, ¶¶ 7, 21; Drexler Decl., Ex. 7, Att. F at 361. And, consumers that are duped

1 into providing their account information to phishing websites that masquerade as the website of
2 their financial institution do not make a free and informed choice when divulging their personal
3 information. Turner Decl., Ex. 6, ¶¶ 31-32. Moreover, the harm that Pricewert inflicts upon
4 society generally – by, for example, hosting child pornography – cannot be reasonably avoided.
5 No consumer, if given a free choice, would willingly submit to any of these harms.
6 Accordingly, the wide swath of injury caused by Pricewert’s unfair conduct is not reasonably
7 avoidable.

8 4. Pricewert’s Unfair Conduct Is Not Protected By Section 230 of the
9 Communications Decency Act

10 Section 230 of the Communications Decency Act provides, in relevant part, that “no
11 provider or user of an interactive computer service shall be treated as the publisher or speaker of
12 any information provided by another information content provider.” 47 U.S.C. § 230 (2006).
13 This language has been interpreted by courts to protect a number of legitimate ISPs from a range
14 of lawsuits seeking to impose liability for the actions of their customers.

15 However, the protections provided by Section 230 are not limitless, as the Ninth Circuit
16 has made clear. In *Fair Housing Council of San Fernando Valley v. Roomates.com LLC*, 521
17 F.3d 1157 (9th Cir. 2008) (en banc), the Ninth Circuit held that participation by a defendant in
18 the harmful conduct alleged in the complaint vitiates any immunity that Section 230 may
19 otherwise provide. See *Roomates.com*, 521 F.3d at 1167-68. This ruling puts to rest any Section
20 230 defense that Pricewert could otherwise assert. The evidence clearly demonstrates that
21 Pricewert has recruited and actively participated in the harmful code and content it hosts,
22 including its direct role in the operation illegal botnets. As a result, Pricewert cannot hide
23 behind the shield of Section 230.

24 **C. The Balance of Equities Tips Decidedly In the Commission’s Favor and
25 Supports Awarding the Requested Injunctive Relief**

26 The balance of the equities tips decidedly in the Commission’s favor. Where, as here,
27 public and private equities are at issue, public equities far outweigh private equities. *FTC v.*
28 *World Wide Factors, Ltd.*, 882 F.2d 344, 347 (9th Cir. 1989). Pricewert’s past misconduct

1 “gives rise to the inference that there is a reasonable likelihood of future violations.” *SEC v. R.J.*
2 *Allen & Assoc., Inc.*, 386 F. Supp. 866, 877 (S.D. Fla. 1974) (citations omitted). Moreover,
3 Pricewert “can have no vested interest in a business activity found to be illegal.” *United States*
4 *v. Diapulse Corp. of Am.*, 457 F.2d 25, 29 (2d Cir. 1972) (internal quotations and citations
5 omitted). This is especially true when a defendant’s alleged unlawful activities are not “isolated
6 or sporadic,” but constitute a “clear pattern of practices which [are] central to [its] business.”
7 *FTC v. Silueta Distributors, Inc.*, 1994 U.S. Dist. LEXIS 10095, *1 (N.D. Cal. 1994).¹²

8 Here, without the entry of the requested preliminary injunctive relief set forth in the
9 FTC’s proposed TRO filed concurrently, Pricewert will continue to engage in its unfair practices
10 and injure the public during the pendency of the litigation. Pricewert has been in business for
11 several years, and has ignored calls from the Internet security community and affected
12 consumers to halt its harmful practices. Linford Decl., Ex. 4, ¶¶ 13-20. In addition, as
13 described above, in Sections II.B and III.G, Pricewert has engaged in substantial efforts to hide
14 from law enforcement.

15 In summary, Pricewert’s rampant use of unfair practices, particularly in the face of
16 complaints, as well as its efforts to mask its identity, create the inference that Pricewert will
17 continue to engage in its wrongful activities unless a temporary restraining order is issued
18 against it. Pricewert’s unfair practices should be halted immediately to prevent substantial
19 further injury to the public.

20
21
22
23
24 ¹²*See also id.* at *2 (“Although a preliminary injunction may disrupt defendants’ business
25 activities, this court is under no obligation to recognize this equity in the continued operation of
26 the business because the business is permeated with deception designed to harm the public.”);
27 *FTC v. Sage Seminars, Inc.*, 1995 U.S. Dist. LEXIS 21043, *22-23 (N.D. Cal. 1995) (potential
28 hardship to defendants’ business “insignificant” in light of evidence that business was “rooted in
violations of the law”; court of equity under no duty to protect illegitimate profits or advance
business which is conducted illegally) (internal quotations and citations omitted).

1 **V. AN EX PARTE TEMPORARY RESTRAINING ORDER DISCONNECTING**
2 **DEFENDANT'S SERVERS FROM THE INTERNET, FREEZING ASSETS AND**
3 **ORDERING THE TURNOVER OF DOCUMENTS, AN ACCOUNTING, AND**
4 **THE PRESERVATION OF RECORDS SHOULD BE GRANTED**

5 In light of the scope of its criminal activity, its efforts to hide from law enforcement, and
6 its extensive connections to individuals overseas, Defendant is likely to dissipate assets and
7 destroy records if given notice of the relief sought in this suit. The FTC Act authorizes a district
8 court to use its inherent equitable authority to “grant any ancillary relief necessary to accomplish
9 complete justice.” *U.S. Oil & Gas*, 748 F.2d 1431, 1434 (11th Cir. 1984). The Commission
10 asks that the Court employ that authority here to issue an *ex parte* TRO that requires Defendant’s
11 third party data centers and upstream Internet providers to disconnect Defendant’s servers from
12 the Internet, freezes the Defendant’s assets, requires Defendant to turn over business records to
13 the FTC, orders the Defendant to provide the Commission with a financial accounting, and
14 orders Defendant’s assets repatriated to the United States. Courts in this district and throughout
15 the Ninth Circuit have repeatedly issued TROs *ex parte* that contain similar relief. See cases
16 cited in footnote 8, *supra*.

17 An *ex parte* TRO is warranted when the facts show that irreparable injury, loss, or
18 damage will result before the defendants can be heard in opposition. *See In re Vuitton et Fils*,
19 606 F.2d 1, 4-5 (2d Cir. 1979); Fed. R. Civ. P. 65(b). Here, the Commission seeks to halt
20 outright criminal activity by the Defendant that is causing massive consumer harm, and to
21 disgorge Defendant’s ill-gotten gains for possible consumer redress. The TRO requested by the
22 Commission would immediately put a stop to Defendant’s unlawful conduct by ordering its
23 third-party data centers and upstream Internet providers to disconnect its servers from the
24 Internet.¹³ The TRO would also impose an asset freeze and require asset repatriation in order to
25 prevent the Defendant from dissipating the proceeds of its unlawful activities before this Court

26 ¹³ The U.S. District Court for the District of Arizona granted similar relief in *FTC v.*
27 *Dugger*. *See* Ex. 10, at 10-11 (granting *ex parte* TRO that, *inter alia*, required hosts of
28 defendants’ computer equipment to disconnect it from the Internet, deny defendants and others
access to the equipment, and prevent removal of the equipment).

1 has the opportunity to rule on the merits of this case. Given the scope of the Defendant's illegal
2 and harmful conduct, its efforts to hide from law enforcement, and its extensive ties to individuals
3 in eastern Europe, it is likely that advance notice of this suit would cause the Defendant to
4 secrete assets and destroy evidence of their unlawful acts.

5 The FTC's concerns about the destruction of evidence and dissipation of assets absent *ex*
6 *parte* relief are informed by the Agency's experience with others engaged in similar unlawful
7 schemes. As described in depth in the attached Fed. R. Civ. P. 65(b) declaration, *ex parte* relief
8 has proven essential in preserving assets and preventing the destruction of evidence in similar
9 cases. See Certification and Declaration Plaintiff's Counsel of Ethan Arenson in Support of
10 Plaintiff's *ex Parte* Motions For: (1) Temporary Restraining Order and Order to Show Cause; (2)
11 Order Temporarily Sealing Entire File; and (3) Leave to Exceed Page Limit, filed herewith.

12 The asset freeze and asset repatriation requested by the FTC are well within this Court's
13 authority. These provisions are necessary here to preserve the status quo and to preserve the
14 possibility of effective final relief in the form of disgorgement of profits and other consumer
15 redress. A district court's authority to enter orders preserving defendants' assets is ancillary to its
16 equitable authority to order consumer redress. *World Wide Factors*, 882 F.2d at 347; *H.N.*
17 *Singer*, 668 F.2d at 1113; *FTC v. Gem Merchandising Corp.*, 87 F.3d 466, 469 (11th Cir. 1996).
18 Moreover, a court may impose an asset freeze based on the mere possibility of dissipation of
19 assets. See *FSLIC v. Sahni*, 868 F.2d 1096, 1097 (9th Cir. 1989). That possibility certainly
20 is present where, as here, the defendant is engaged in pervasive criminal activity. See, e.g., *J.K.*
21 *Pubs*, 99 F. Supp. 2d at 1176; *H.N. Singer*, 668 F.2d at 1113; *U.S. Oil & Gas*, 748 F.2d 1431.
22 The fact that Defendant's assets may be located overseas is not a bar to the relief sought by the
23 FTC. See *U.S. v. First Nat'l City Bank*, 379 U.S. 378, 384 (1965) ("Once personal jurisdiction
24 of a party is obtained, the District Court has authority to order it to 'freeze' property under its
25 control, whether the property be within or without the United States."); *SEC v. International*
26 *Swiss Inv. Corp.*, 895 F.2d 1272, 1276 (9th Cir. 1990) (upholding district court's injunction
27 freezing and ordering an accounting of foreign assets); *FTC v. Affordable Media, LLC*, 179 F.3d
28

1 1228, 1232, 1238-44 (9th Cir. 1999) (affirming finding of civil contempt for defendants' failure
2 to repatriate assets held for their benefit outside the United States in accordance with TRO and
3 preliminary injunction).

4 Additionally, in order to assist the Commission in locating and securing assets, and to
5 preserve the possibility of consumer redress for victimized consumers and/or the possibility of
6 disgorgement, the FTC requests that the Court order the Defendant to make a full financial
7 accounting.¹⁴ Attached to the proposed Order are copies of proposed financial statements to be
8 completed by the Defendant.¹⁵ Courts have upheld the use of these devices, recognizing that
9 they assist the district court's purpose of monitoring compliance with an asset freeze order and in
10 turn ensure effective final relief. *See Kemp v. Peterson*, 940 F.2d 110, 113 (4th Cir. 1991)
11 (affirming district court's order requiring monthly accounting and financial disclosure
12 statements); *HUD v. Cost Control Mktg. & Sales Mgmt. of Va.*, 64 F.3d 920, 927 (4th Cir. 1995);
13 *Nat'l Org. for Reform of Marijuana Laws v. Mullen*, 828 F.2d 536, 544 (9th Cir. 1987)
14 (approving the appointment of a Special Master to monitor compliance with a preliminary
15 injunction).¹⁶

16 VI. CONCLUSION

17 Defendant recruits, knowingly hosts, and actively participates in the distribution of,
18 illegal, malicious, and harmful electronic content, including child pornography, malicious
19

20 ¹⁴The TRO also includes a provision that restrains Defendant from taking any action that
21 may result in the encumbrance or dissipation of foreign assets, including taking any action that
22 would invoke a duress clause. This provision is important since Defendant may have created
23 asset protection trusts that could frustrate the Court's ability to provide consumer redress. *See*
FTC v. Affordable Media, 179 F.3d 1228, 1239-44 (9th Cir. 1999).

24 ¹⁵The TRO also includes a Consent to Release Financial Records form, which allows the
25 FTC to access records of accounts or assets held by foreign financial institutions. *See Doe v.*
United States, 487 U.S. 201, 215 (1988).

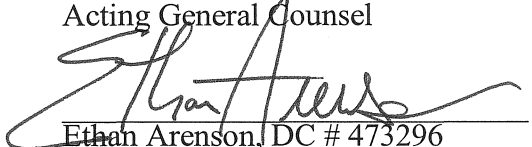
26 ¹⁶The provision in the proposed TRO requiring Defendant's third-party data centers and
27 upstream providers to disconnect its servers from the Internet is also well within this Court's
28 authority pursuant to Fed. R. Civ. Pro. 65(d)(2).

1 software, and the servers used to control botnets. These practices are unfair and cause
2 substantial, unavoidable injuries to massive numbers of consumers throughout the United States
3 who use their computers to access the Internet. In order to put an end to these unlawful
4 practices, the Commission respectfully requests that this Court grant the Commission's motion
5 for an *ex parte* TRO and ancillary equitable relief.

6
7 Dated: June 1, 2009

8 Respectfully submitted:

9 DAVID SHONKA
10 Acting General Counsel

11 

12 Ethan Arenson, DC # 473296
13 Carl Settlemyer, DC # 454272
14 Philip Tumminio, DC # 985624
15 Federal Trade Commission
16 600 Pennsylvania Avenue, N.W.
17 Washington, DC 20580
18 (202) 326-2204 (Arenson)
19 (202) 326-2019 (Settlemyer)
20 (202) 326-2004 (Tumminio)
21 (202) 326-3395 *facsimile*
22 earenson@ftc.gov
23 csettlemyer@ftc.gov
24 ptumminio@ftc.gov

25 Attorneys for Plaintiff