

1 DAVID SHONKA
2 Acting General Counsel
3 Ethan Arenson, DC # 473296
4 Carl Settlemyer, DC # 454272
5 Philip Tumminio, DC # 985624
6 Federal Trade Commission
7 600 Pennsylvania Avenue, N.W.
8 Washington, DC 20580
9 (202) 326-2204 (Arenson)
10 (202) 326-2019 (Settlemyer)
11 (202) 326-2204 (Tumminio)
12 (202) 326-3395 *facsimile*
13 earenson@ftc.gov
14 csettlemyer@ftc.gov
15 ptumminio@ftc.gov

16 Attorneys for Plaintiff Federal Trade Commission

17
18
19
20
21
22
23
24
25
26
27
28

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
San Jose Division**

Federal Trade Commission,

Plaintiff,

v.

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

Defendant.

Case No. C-09-2407 RMW

**[PROPOSED] Order Appointing
Temporary Receiver**

By Order dated June 5, 2009 (D.E. 13), this Court directed the Plaintiff Federal Trade Commission (“FTC” or “Commission”) to submit a proposal for expeditiously addressing concerns raised by third parties whose websites were hosted by Defendant and minimizing any undue harm such third parties suffered as a result of the Temporary Restraining Order of June 2, 2009 (D.E.12). Having reviewed the FTC’s proposal, this Court finds that good cause exists to

Proposed Order Appointing Temp.
Receiver - C-09-2407 RMW

1 appoint a temporary receiver who can evaluate the claims of third parties whose data is stored on
2 Defendant Data Servers and coordinate the release of copies of such data to third parties whose
3 data does not appear to relate to the conduct prohibited by the Temporary Restraining Order. The
4 Court further finds that the costs associated with providing third parties with copies of their data
5 should be borne by the Defendant.

6 **DEFINITIONS**

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

- 8 1. **“Assets”** means any legal or equitable interest in, right to, or claim to, any real,
9 personal, or intellectual property of Defendant or held for the benefit of Defendant
10 wherever located, including, but not limited to, chattel, goods, instruments,
11 equipment, fixtures, general intangibles, effects, leaseholds, contracts, mail or
12 other deliveries, shares of stock, inventory, checks, notes, accounts, credits,
13 receivables (as those terms are defined in the Uniform Commercial Code), cash,
14 and trusts, including but not limited to any other trust held for the benefit of
15 Defendant.
- 16 2. **“Botnet”** means a network of computers that have been compromised by
17 malicious code and surreptitiously programmed to follow instructions issued by a
18 Botnet Command and Control Server.
- 19 3. **“Botnet Command and Control Server”** means a computer or computers used to
20 issue instructions to, or otherwise control, a Botnet.
- 21 4. The term **“Child Pornography”** shall have the same meaning as provided in 18
22 U.S.C. § 2256.
- 23 5. **“Data Center”** means any person or entity that contracts with third parties to
24 house computer servers and associated equipment, and provides the infrastructure
25 to support such equipment, such as power or environmental controls.
- 26 6. **“Day”** shall have the meaning prescribed by and time periods in this Order shall be
27 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. **“Defendant Data Servers”** means computer servers and associated equipment
7 owned, leased, or controlled by the Defendant stored in a Data Center subject to
8 the Temporary Restraining Order, and any data stored on such computer servers or
9 associated equipment.
- 10 9. **“Document”** is synonymous in meaning and equal in scope to the usage of the
11 term in the Federal Rules of Civil Procedure 34(a), and includes writing, drawings,
12 graphs, charts, Internet sites, Web pages, Web sites, electronic correspondence,
13 including e-mail and instant messages, photographs, audio and video recordings,
14 contracts, accounting data, advertisements (including, but not limited to,
15 advertisements placed on the World Wide Web), FTP Logs, Server Access Logs,
16 USENET Newsgroup postings, World Wide Web pages, books, written or printed
17 records, handwritten notes, telephone logs, telephone scripts, receipt books,
18 ledgers, personal and business canceled checks and check registers, bank
19 statements, appointment books, computer records, and other data compilations
20 from which information can be obtained and translated. A draft or non-identical
21 copy is a separate document within the meaning of the term.
- 22 10. **“Harmful Data”** means Child Pornography, botnet command and control servers
23 or software, spyware, viruses, trojan horses, phishing-related data or software, or
24 similar electronic code or content that inflicts harm upon consumers.
- 25 11. **“Phishing”** means the use of email, Internet web sites, or other means to mimic or
26 copy the appearance of a trustworthy entity for the purpose of duping consumers
27 into disclosing personal information, such as account numbers and passwords.
28

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

12. **“Receiver”** means the temporary receiver appointed in this Order and any deputy receivers that may be named by the temporary receiver;

13. **“Representatives”** means the following persons or entities who receive actual notice of the Temporary Restraining Order by personal service or otherwise:
(1) the Defendant’s officers, agents, servants, employees, and attorneys; and (2) all other persons who are in active concert or participation with Defendant or its officers, agents, servants, employees, or attorneys.

14. **“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.

15. **“Temporary Restraining Order”** means the Temporary Restraining Order issued by this Court on June 2, 2009 in the matter of Federal Trade Commission v. Pricewert, LLC, Case No. C-09-2407 RMW.

16. **“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.

17. **“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.

18. **“Viruses”** means computer programs designed to spread from one computer to another and to interfere with the operation of the computers they infect.

1 Paragraph II of this Order.

2
3 **RECEIVER'S AND DATA CENTERS' DUTIES**

4 **V.**

5 **IT IS FURTHER ORDERED** that, notwithstanding the requirements of the Temporary
6 Restraining Order that prohibit Defendant's and third parties' access to computer resources
7 leased, owned, or operated by Defendant or other enumerated persons, the Receiver is authorized
8 and directed to accomplish, and affected Data Centers are directed to take all reasonable steps to
9 facilitate, the following:

10 A. Take exclusive custody, control, and possession of the Defendant Data Servers.
11 Any Data Center that has secured Defendant Data Servers pursuant to the Temporary Restraining
12 Order shall provide the Receiver and/or his agents with full and immediate access to the
13 Defendant Data Servers and any related data sufficient to enable the Receiver to accomplish his
14 duties under this Order.

15 B. Receive and review requests from third parties who claim they have suffered harm
16 because they own data on Defendant Data Servers rendered inaccessible as a result of the
17 Temporary Restraining Order. Any third party seeking the release of data pursuant to this Order
18 shall provide the Receiver with:

- 19 1. If applicable, the Domain Name(s) and IP Address(es) used to aggregate
20 the data, and any passwords or similar information necessary to enable the
21 Receiver to access the requested data;
- 22 2. Contact information for the third party including a name, address,
23 telephone number, email address, business title, business name, and
24 administrative contact for the domain name in question;
- 25 3. Certification that the third party is the lawful owner of data sought from the
26 Defendant Data Server, or similar certification that the third party may
27 lawfully access such data;

- 1 4. Certification that the third party has no accessible back-up copy or
2 alternative access to the requested data absent the intervention of the
3 Receiver;
- 4 5. Certification that the third party has no knowledge, direct or indirect, that
5 the requested data contains Harmful Data;
- 6 6. Certification that the third party agrees to bear the reasonable costs of
7 copying and transmitting the requested data, and any associated costs; and
- 8 7. Any other information deemed necessary by the Receiver to comply with
9 applicable laws governing disclosure of the requested data to the third
10 party, or to determine: (i) the identity of the third party; (ii) that the third
11 party is lawfully entitled to the possession of the requested data; or (iii) that
12 the data requested by the third party does not contain Harmful Data.

13 C. Determine whether third party requests for data comply with the requirements of
14 Section “B,” above.

15 D. Evaluate the requested third party data to make a reasonable, good faith
16 determination that it does not contain Harmful Data. In making his evaluation, the Receiver shall
17 consider the third party certifications and any other documents or information supplied by the
18 third party and, where appropriate, the documents filed by the Federal Trade Commission in this
19 matter, relevant information that may be readily available from third party sources, and
20 information uncovered through the Receiver’s independent investigation. Provided, that the third
21 party shall have the burden to produce evidence to the Receiver sufficient for the Receiver to
22 make a reasonable, good faith determination that the requested data does not include Harmful
23 Data.

24 E. If the Receiver makes a reasonable, good faith determination that a third party
25 request for data complies with Sections B through D, above, the Receiver shall, while at all times
26 complying with the document preservation and other applicable obligations set out in the
27 Temporary Restraining Order, act expeditiously to obtain a copy of the requested data and
28

1 provide it to the third party.

2 1. The Receiver shall take reasonable steps to minimize disruption and costs
3 to any Data Centers in possession of Defendant Server Data;

4 2. The Receiver is authorized to enter into contracts with technicians,
5 independent contractors, or other parties necessary to obtain copies of third
6 party data pursuant to this Order, or to otherwise deliver requested data to
7 third parties; and

8 3. The Receiver is authorized to purchase insurance as advisable or necessary
9 to accomplish his duties under this Order.

10 F. Notwithstanding the foregoing, if the Receiver determines that a third party's data
11 is located on a server or computer that contains Harmful Data, apparent child pornography, or any
12 other data that is illegal to possess, the Receiver shall immediately cease working on such server
13 or computer and, to the extent required or permitted by applicable law, deliver such server or
14 computer to the appropriate criminal law enforcement authority.

15 G. The Receiver shall deposit all funds and shall make all related payments and
16 disbursements from receivership accounts established pursuant to Paragraph IV of this Order.
17 The Receiver shall serve copies of monthly account statements on all parties.

18 H. Maintain accurate records of all receipts and expenditures that he makes as
19 Receiver.

20 I. Cooperate with reasonable requests for information or assistance from any state or
21 federal law enforcement agency.

22 J. Preserve and prohibit others from accessing Defendant Data Servers.
23

24 **RECORD KEEPING**

25 **VI.**

26 **IT IS FURTHER ORDERED** that, during the pendency of his Receivership, the
27 Receiver shall maintain records of all third party requests for data pursuant to this Order, and all
28

1 documents and other evidence supporting his determinations and actions required pursuant to
2 Paragraph V of this Order.

3
4 **PROVISION OF INFORMATION TO RECEIVER**

5 **VII.**

6 **IT IS FURTHER ORDERED** that the Defendant shall provide to the Receiver, within 24
7 hours of a request delivered by the Receiver to the Defendant via telephone, facsimile, or email,
8 any information deemed necessary by the Receiver to extract the data of a third party in
9 accordance with this Order. This information shall include, but not be limited to, passwords, IP
10 addresses, server location and identity data, and file name and location data.

11
12 **COOPERATION WITH THE RECEIVER**

13 **VIII.**

14 **IT IS FURTHER ORDERED** that Defendant, Data Centers, Upstream Service
15 Providers, and all other persons or entities served with a copy of this Order shall fully cooperate
16 with and assist the Receiver in executing his duties pursuant to this Order. Provided further, that
17 any Data Center or Upstream Service Provider that incurs costs associated with locating, copying,
18 or delivering data to third parties pursuant to this Order, may petition the Court for an order
19 directing Defendant to pay such reasonable and necessary costs.

20
21 **INTERFERENCE WITH THE RECEIVER**

22 **IX.**

23 **IT IS FURTHER ORDERED** that the Defendant and its Representatives are hereby
24 restrained and enjoined from directly or indirectly interfering with the Receiver. Such
25 interference includes, but is not limited to, failing to expeditiously provide information or similar
26 requested cooperation to the Receiver or the Receiver's duly authorized agents in the exercise of
27 their duties or authority under any order of this Court.

1 **CONSTRUCTION OF ORDER**

2 **XIII.**

3 **IT IS FURTHER ORDERED** that this Order shall not be construed to allow the release
4 of Harmful Data, other than to appropriate law enforcement authorities, to any person, including
5 any third party who requests a copy of data on Defendant Data Servers, or to the Defendant and
6 its Representatives, to provide any person with remote access to Defendant Data Servers, or to
7 provide copies of any data on Defendant Data Servers to the Defendant and its Representatives.
8 To facilitate the provision of copies of data to third parties consistent with this Order and to
9 facilitate the Defendant's cooperation as required by this Order, the Receiver may provide
10 Defendant and its Representatives, to the extent minimally necessary, the ability to view locally
11 and under the Receiver's supervision information about the organization of Defendant Data
12 Servers and the organization of the data stored thereon.

13
14 **SO ORDERED**, this _____ day of _____, 2009, at _____ m.

15
16 _____
17 RONALD M. WHYTE
18 United States District Judge
19
20
21
22
23
24
25
26
27
28