UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, D.C. 20436

Before the Honorable Carl C. Charneski
Administrative Law Judge

In the Matter of	)	
	)	
CERTAIN SYSTEMS FOR DETECTING AND REMOVING VIRUSES OR WORMS, COMPONENTS THEREOF, AND PRODUCTS CONTAINING SAME	)	Investigation No. 337-TA-624

BARRACUDA NETWORK'S RESPONSE TO TREND MICRO INCORPORATED'S COMPLAINT AND NOTICE OF INVESTIGATION UNDER SECTION 337 OF THE TARIFF ACT OF 1930, AS AMENDED

Filed on Behalf of Respondent:

Barracuda Networks, Inc.
3175 S. Winchester Blvd.
Campbell, CA 95008
Telephone: (408) 342-5400
Facsimile: (408) 342-5402

Attorneys for Respondent Barracuda Networks, Inc.

James C. Otteson
Stefani Shanberg
T.O. Kong
Chris Parry
Matt Argenti
WILSON SONSINI GOODRICH & ROSATI
650 Page Mill Road
Palo Alto, CA 94304-1050
Telephone: (650) 493-9300
Facsimile: (650) 565-5100

Respondent Barracuda Networks, Inc. (3175 S. Winchester Boulevard, Campbell, California 95008, (408) 342-5400; hereinafter "Barracuda"), through its attorneys, hereby responds to the Complaint brought by Complainant Trend Micro Incorporated (hereinafter "Trend Micro") and the Notice of Investigation issued by the United States International Trade Commission on December 21, 2007, and published in the Federal Register on December 31, 2007.

I. INTRODUCTION

1. Responding to the allegations of paragraph 1, Barracuda admits that Trend Micro has filed a complaint alleging violations of Section 337 of the Tariff Act of 1930, as amended, 19 U.S.C. § 1337. Barracuda also admits that Trend Micro has requested relief. Barracuda denies that it has violated Section 337 of the Tariff Act of 1930, as amended, 19 U.S.C. § 1337 by the importation into the United States, and sale within the United States after importation by the owner, importer or consignee of articles that infringe U.S. Patent No. 5,623,600 ("the '600 patent"), entitled "Virus Detection and Removal Apparatus For Computer Networks" and naming Trend Micro as the assignee. Barracuda denies that the '600 patent is a valid and enforceable patent. Barracuda denies that Trend Micro is entitled to the relief that it has requested. Except as thus expressly admitted, Barracuda denies the allegations of paragraph 1.

2. Barracuda denies the allegations of paragraph 2 as they relate to Barracuda. Barracuda lacks knowledge or information sufficient to admit or deny the remaining allegations of paragraph 2, and, on that basis, denies those allegations.

3. Responding to the allegations of paragraph 3, Barracuda denies that it infringes any claim of the '600 patent. Barracuda admits that Claims 1, 4, 11, 13, and 18 are independent claims of the '600 patent. Barracuda lacks knowledge or information sufficient to admit or deny the remaining allegations of paragraph 3, and, on that basis, denies those allegations.

4. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 4, and, on that basis, denies those allegations.

5. Responding to the allegations of paragraph 5, Barracuda admits that what appears to be a copy of Trend Micro's '600 patent was submitted with Trend Micro's complaint as Exhibit 1. Barracuda also admits that what appears to be a copy of an assignment document was submitted with Trend Micro's complaint as Exhibit 2. Barracuda lacks knowledge or information sufficient to admit or deny the remaining allegations of paragraph 5, and, on that basis, denies those allegations.

6. Barracuda lacks knowledge or information sufficient to admit or deny the remaining allegations of paragraph 6, and, on that basis, denies those allegations.

7. Responding to the allegations of paragraph 7, Barracuda admits that Trend Micro seeks several forms of relief. Barracuda denies that Trend Micro is entitled to the relief requested against Barracuda by Trend Micro. Barracuda lacks knowledge or information sufficient to admit or deny the remaining allegations of paragraph 8, and, on that basis, denies those allegations.

II. BACKGROUND

8. Responding to the allegations of paragraph 8, Barracuda admits that the antivirus portion of its products competes with Trend Micro's products. Barracuda also admits that it designs, develops, manufactures, sells, markets, and provides support for products which include antivirus functionality. Barracuda lacks knowledge or information sufficient to admit or deny the remaining allegations of paragraph 8, and, on that basis, denies those allegations.

9. Responding to the allegations of paragraph 9, Barracuda admits that one problem that has plagued microcomputers and computer networks is the spread of computer viruses and worms. Barracuda admits that a computer virus is a section of code that is buried or hidden in another program and that once the program is executed, the code is activated and attaches itself to other programs in the system which then copy the code to other programs. Barracuda also admits that a computer worm is a program that replicates itself throughout disk and memory using up all available computer resources eventually causing the computer system to crash. Barracuda admits that computer viruses and worms are destructive, and therefore need to be detected and eliminated from computers and/or prevented from entering computers

and/or computer networks. Except as thus expressly admitted, Barracuda denies the allegations of paragraph 9.

10. Barracuda lacks knowledge or information sufficient to admit or deny the remaining allegations of paragraph 10, and, on that basis, denies those allegations.

11. Responding to the allegations of paragraph 11, Barracuda denies that the '600 patent solves the problem of preventing the entry of viruses and worms at the computer network level. Barracuda lacks knowledge or information sufficient to admit or deny the remaining allegations of paragraph 11, and, on that basis, denies those allegations.

12. Responding to the allegations of paragraph 12, Barracuda denies that the '600 patent scans for viruses and other undesired software at the gateway of a network. Barracuda lacks knowledge or information sufficient to admit or deny the remaining allegations of paragraph 12, and, on that basis, denies those allegations.

13. Responding to the allegations of paragraph 13, Barracuda admits that Trend Micro sells a product entitled InterScan Web Security Appliance and InterScan Web Security Suite. Barracuda lacks knowledge or information sufficient to admit or deny the remaining allegations of paragraph 13, and, on that basis, denies those allegations.

14. Responding to the allegations of paragraph 14, Barracuda admits that it sells products with antivirus functionality, but denies that "AV Systems" define the relevant market for Barracuda products. Barracuda denies that it has committed any unfair acts, directly or indirectly, including without limitation, the unlicensed importation into the United States, sale for importation into the United States, and/or sale within the United States after importation of products which include antivirus functionality that infringe one or more claims of the '600 patent. Barracuda denies all remaining allegations relating to Barracuda and its products. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 14 relating to other Respondents, and, on that basis, denies those allegations.

III. COMPLAINANT

15. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 15, and, on that basis, denies those allegations.

16. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 16, and, on that basis, denies those allegations.

17. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 17, and, on that basis, denies those allegations.

18. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 18, and, on that basis, denies those allegations.

19. Responding to the allegations of paragraph 19, Barracuda admits that submitted with Trend Micro's complaint as Exhibit 3 is a document that appears to be a copy of Trend Micro's domestic corporation certificate of status from the California Secretary of State. Except as thus expressly admitted, Barracuda denies the allegations of Paragraph 19.

IV. PROPOSED RESPONDENTS

A. Barracuda Networks, Inc.

20. Barracuda admits the allegations of Paragraph 20.

21. Responding to the allegations of Paragraph 21, Barracuda admits that one aspect of its business is virus protection. Barracuda also admits that it designs, develops, manufactures, and/or sells, among other things, products which include antivirus functionality in the United States. Except as thus expressly admitted, Barracuda denies the remaining allegations of Paragraph 21.

22. Responding to the allegations of Paragraph 22, Barracuda admits that the Barracuda Spam Firewall, the Barracuda IM Firewall, and the Barracuda Web Filter (collectively, the "Accused Barracuda Products") include both software and hardware for use with Barracuda's customers' networks. Except as thus expressly admitted, Barracuda denies the remaining allegations of Paragraph 22.

23. Responding to the allegations of Paragraph 23, Barracuda admits that Trend Micro has submitted as Exhibit 4 to its complaint a document entitled "Barracuda Networks Email Security Technology." Barracuda also admits that Trend Micro has attached as Exhibit 5 to its complaint print-outs from Barracuda's website. The content of Exhibits 4 and 5 speaks for itself. Except as thus expressly admitted, Barracuda denies the allegations of paragraph 23.

B. Panda Software International, S.L. and Panda Distribution, Inc.

24. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 24, and, on that basis, denies those allegations.

25. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 25, and, on that basis, denies those allegations.

26. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 26, and, on that basis, denies those allegations.

27. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 27, and, on that basis, denies those allegations.

V. PRODUCTS AT ISSUE

A. Barracuda's AV Systems

28. Responding to the allegations of paragraph 28, Barracuda admits that it designs, develops, manufactures, and/or sells products which include antivirus functionality. Barracuda denies that any of its products infringe the claims of the '600 patent. Barracuda has insufficient knowledge or information to admit or deny the allegations regarding the identity of the products at issue in this case, and therefore denies the remaining allegations of paragraph 28.

29. Responding to the allegations of paragraph 29, Barracuda admits that Trend Micro has submitted with its complaint Exhibits 4, 9, 10, and 27 which appear to be a document entitled Barracuda Networks Email Security Technology, a document entitled Barracuda Web Filter Administrator's Guide, a document entitled Barracuda Networks IM Firewall Administrator's Guide, and a print-out from the Barracuda website, respectively. The content of such documents and print-outs speaks for itself. Except as thus expressly admitted, Barracuda denies the allegations of paragraph 29.

30. Barracuda admits that Trend Micro has attached to its complaint what appear to be print-outs from the Barracuda, ClamAV, and SourceFire websites as Exhibits 4, 5, 11, and 12. The content of the print-outs speaks for itself. Except as thus expressly admitted, Barracuda denies the allegations of paragraph 30.

B. Panda's AV Systems

31. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 31, and, on that basis, denies those allegations.

32. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 32, and, on that basis, denies those allegations.

VI. CLASSIFICATION OF THE INFRINGING ARTICLE UNDER THE HARMONIZED TARIFF SCHEDULE OF THE UNITED STATES

33. Answering the allegations of paragraph 33, Barracuda admits that Trend Micro claims that the listed Harmonized Tariff Schedule ("HTS") number is intended for illustration only and not intended to be restrictive of the devices and products accused. Except as thus expressly admitted, Barracuda denies the allegations of paragraph 33.

VII. THE '600 PATENT

34. Responding to the allegations of paragraph 34, Barracuda admits that U.S. Patent No. 5,623,600 is entitled "Virus Detection and Removal Apparatus for Computer Networks." Barracuda also admits that the '600 patent names Trend Micro as assignee of Shuang Ji, et. Al. Barracuda further admits that the '600 patent issued on April 22, 1997. Except as thus expressly admitted, Barracuda denies the allegations of paragraph 34.

35. Responding to the allegations of paragraph 35, Barracuda denies that it infringes any claim of the '600 patent. Barracuda admits that claims 1, 4, 11, 13, and 18 are independent claims. Barracuda also admits that Trend Micro's '600 patent was at issue in In the Matter of Certain Systems for Detecting and Removing Viruses or Worms, Components Thereof and Products Containing Same, ITC INV. NO. 337-TA-510 (Luckern, J.) ("the '510 Investigation"). Barracuda further admits that the Commission found that claims 4, 7, 8, and 11-15 were not invalid or unenforceable and that such claims were infringed by Fortinet's products. Barracuda also admits that the Commission also found claims 1 and 3 to be invalid. Except as thus expressly admitted, Barracuda denies the remaining allegations of paragraph 35.

A. Non-technical Description of the '600 Patented Invention

36. Barracuda denies the allegations of paragraph 36.

37. Barracuda denies the allegations of paragraph 37.

38. Responding to the allegations of paragraph 38, Barracuda admits that the asserted claims of the '600 patent are directed to various aspects of a system and method of detecting and removing viruses and worms from a computer network. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 38, and, on that basis, denies those allegations.

B. Foreign Counterparts

39. Responding to the allegations of paragraph 39, Barracuda admits that Trend Micro has attached to its complaint as Exhibit 14 what appears to be a chart listing foreign patent applications corresponding to the '600 patent. Barracuda lacks knowledge or information sufficient to assess the accuracy of Exhibit 14, and, on that basis, denies the remaining allegations of paragraph 39.

40. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 40, and, on that basis, denies those allegations.

C. Materials Accompanying the Complaint

41. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 41, and, on that basis, denies those allegations.

42. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 42, and, on that basis, denies those allegations.

VIII. BARRACUDA'S ALLEGED UNLAWFUL ACTIVITIES

A. Alleged Specific Instances of Importation of Barracuda's Allegedly Infringing AV Systems

43. Barracuda denies the allegations of paragraph 43.

44. Responding to the allegations of paragraph 44, Barracuda admits that certain of its products contain open source antivirus software known as ClamAV. Barracuda also admits that portions of the ClamAV software code are written in part by developer team members located in Europe and Australia. Barracuda denies that it imports software specifically designed to protect against viruses at the network gateway, as Barracuda downloads ClamAV

from a server located in the United States, compiles the source code into executable code at its facilities in Campbell, California, USA, and loads ClamAV onto its hardware solutions at its facilities in Campbell, California, USA. Except as thus expressly admitted, Barracuda denies the allegations of paragraph 44.

45. Responding to the allegations of paragraph 45, Barracuda admits that the motherboard pictured in Exhibit 16 says "made in China." Barracuda also admits that the power supply pictured in Exhibit 16 says "made in China." Barracuda denies that the motherboard or power supply pictured in Exhibit 16 are non-staple articles of commerce. Barracuda also denies the Accused Barracuda Products are sold in the United States after importation, or after importation of non-staple components of such products. Except as thus expressly admitted, Barracuda denies the allegations of paragraph 45.

46. Responding to the allegations of paragraph 46, Barracuda admits that its Web Filter, Span Firewall, and IM Firewall are available for sale and sold in the United States. Barracuda also admits that its products are available for purchase through its website, its sales personnel, and/or its distributors. Barracuda further admits that its products are used by its customers in the United States. Except as thus expressly admitted, Barracuda denies the allegations of paragraph 46.

47. Responding to the allegations of paragraph 47, Barracuda admits that the Accused Barracuda Products are a subset of Barracuda's products. Barracuda also admits that Trend Micro claims that the products are enumerated only for exemplary purposes; however, Trend Micro has taken discovery on Barracuda's products and has only accused the Barracuda Spam Firewall, the Barracuda Web Filter, and the Barracuda IM Firewall of infringement. Except as thus expressly admitted, Barracuda denies the allegations of paragraph 47.

B. Alleged Direct Infringement by Barracuda

48. Barracuda denies the allegations of paragraph 48.

49. Barracuda denies the allegations of paragraph 49.

C. Alleged Contributory Infringement by Barracuda

50. Responding to the allegations of paragraph 50, Barracuda admits that it has knowledge of the '600 patent. Barracuda also admits that on March 29, 2007, it filed a lawsuit against Trend Micro in the Northern District of California seeking declaration of patent invalidity and noninfringement of the '600 patent. Except as thus expressly admitted, Barracuda denies the allegations of paragraph 50.

51. Barracuda denies the allegations of paragraph 51.

52. Barracuda denies the allegations of paragraph 53.

D. Alleged Inducement of Infringement by Barracuda

53. Responding to the allegations of paragraph 53, Barracuda admits that it has knowledge of the '600 patent as of the date of Trend Micro's notice letter written in September 2006. Barracuda also admits that on March 29, 2007, it filed a lawsuit against Trend Micro in the Northern District of California seeking declaration of patent invalidity and noninfringement of the '600 patent. Except as thus expressly admitted, Barracuda denies the allegations of paragraph 53.

54. Barracuda denies the allegations of paragraph 54.

IX. PANDA'S ALLEGED UNLAWFUL ACTIVITIES

55. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 55, and, on that basis, denies those allegations.

56. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 56, and, on that basis, denies those allegations.

57. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 57, and, on that basis, denies those allegations.

58. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 58, and, on that basis, denies those allegations.

59. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 59, and, on that basis, denies those allegations.

60. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 60, and, on that basis, denies those allegations.

61. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 61, and, on that basis, denies those allegations.

62. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 62, and, on that basis, denies those allegations.

63. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 63, and, on that basis, denies those allegations.

64. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 64, and, on that basis, denies those allegations.

65. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 65, and, on that basis, denies those allegations.

66. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 66, and, on that basis, denies those allegations.

X. THE ALLEGED DOMESTIC INDUSTRY

Barracuda denies the allegations made by Trend Micro in the introductory section of Section X. of its complaint

A. Trend Micro's Allegation that it Meets the Technical Prong of the Domestic Industry Requirement

67. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 66, and, on that basis, denies those allegations.

68. Responding to the allegations of paragraph 68, Barracuda admits that Exhibit 25 purports to be a claim chart demonstrating that Trend Micro's InterScan Web Security Suite practices an exemplary claim of the '600 patent. Barracuda denies that the chart demonstrates that Trend Micro's AV systems practice the invention claimed in the '600 patent. Except as thus expressly admitted, Barracuda denies the remaining allegations of paragraph 68.

B. Trend Micro's Allegation that it Meets the Economic Prong of the Domestic Industry Requirement

69. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 69, and, on that basis, denies those allegations.

70. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 70, and, on that basis, denies those allegations.

XI. RELATED LITIGATION

A. Pending Litigation

71. Barracuda admits that there is litigation pending relating to the '600 patent. Barracuda also admits that it filed a lawsuit against Trend Micro in the Northern District of California, Civil Action No. C07-01806-MHP, seeking declaration of patent invalidity and noninfringement of the '600 patent. Barracuda further admits that the parties were previously engaged in fact and claim construction discovery, but the case has now been stayed pursuant to 28 U.S.C. §1659 pending the resolution of this Investigation.

72. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 72, and, on that basis, denies those allegations.

B. Prior Litigation

73. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 73, and, on that basis, denies those allegations.

74. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 74, and, on that basis, denies those allegations.

75. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 75, and, on that basis, denies those allegations.

76. Barracuda lacks knowledge or information sufficient to admit or deny the allegations of paragraph 76, and, on that basis, denies those allegations.

77. Barracuda admits that the '600 patent was also at issue in In the Matter of Certain Systems for Detecting and Removing Viruses and Worms, Components Thereof and Products Containing Same, ITC Inv. No. 337-TA-510 ("the '510 Investigation"). Barracuda denies Trend Micro's characterization of the '600 patent as "the valid and enforceable '600 Patent," as claims 1 and 3 of the '600 patent were found invalid in the '510 Investigation. Barracuda lacks knowledge or information sufficient to admit or deny the remaining allegations of paragraph 77, and, on that basis, denies those allegations.

XII. RELIEF REQUESTED BY TREND MICRO

The remaining paragraphs of Trend Micro's complaint constitute prayers for relief that do not require a response. To the extent these paragraphs may be deemed to allege any facts or any factual or legal entitlement to the relief requested, Barracuda denies each and every such allegation.

RESPONSE TO NOTICE OF INVESTIGATION

Barracuda denies that it is in violation of 19 U.S.C. § 1337 and further denies that it has engaged or currently engages in the unlawful and/or unauthorized importation into the United State, the sale for importation, and/or the sale within the United States after importation of certain systems for detecting and removing viruses or worms, components thereof, and products containing same alleged to infringe any claim of the '600 patent. Barracuda admits that the Complaint alleges the existence of a domestic industry, but Barracuda lacks sufficient knowledge and information regarding Trend Micro's allegation that it meets the domestic industry requirement and denies the allegation on that basis. Barracuda denies that the Commission should issue any kind of exclusion order, cease and desist order, or any other form of relief.

STATEMENT PURSUANT TO RULE 210.13(b)

Pursuant to Rule 210.13(b), Barracuda provides the following information. Barracuda specifically denies that any of the supplied data refers or relates to any unlawful act under 19 U.S.C. § 1337 or otherwise.

78. Statistical Data on the Quantity and Value of Imports – Barracuda does not import, sell for importation, or sell after importation the Accused Barracuda Products or any non-staple component thereof, and therefore does not have statistical data on the quantity and value of any imports of the accused articles.

79. Harmonized Tariff Schedule Item Numbers – Barracuda does not import, sell for importation, or sell after importation the Accused Barracuda Products or any non-staple component thereof, and therefore does not have Harmonized Tariff Schedule item numbers to provide. Further, Barracuda did not import, sell for importation, or sell after importation the

Accused Barracuda Products or any non-staple component thereof prior to January 1, 1989, and therefore does not have Tariff Schedules item numbers to provide.

80. Barracuda's Capacity to Produce the Accused Articles – Barracuda has the capacity to produce the Accused Barracuda Products in the United States. Indeed, Barracuda currently produces, and has always previously produced, in the United States all of the Accused Barracuda Products sold in the United States.

81. Relative Significance of the United States Market to Barracuda's Operations – The United States market comprises approximately 75% of Barracuda's business.

AFFIRMATIVE DEFENSES

First Affirmative Defense

(*Failure to State a Claim*)

82. Trend Micro's claims of violations of Section 337 of the Tariff Act of 1930, as amended, by the importation into the United States, the sale for importation, and the sale within the United States after importation of certain systems for detecting and removing viruses and worms, components thereof, and products containing same by reason of infringement of claims 2 and/or 4-22 of the '600 patent against Barracuda fail to state a claim upon which relief can be granted.

83. Trend Micro cannot show that the Accused Barracuda Products are imported into the United States, sold for importation, or sold within the United States after importation as required 19 U.S.C. § 337 (a)(1)(B). Trend Micro has alleged that Barracuda imports motherboards, power supplies, and software entitled ClamAV. First, the motherboards used by Barracuda in the Accused Barracuda Products are staple articles of commerce and are in no way tied to the alleged invention of the '600 patent. The photograph of the motherboard attached to Trend Micro's Complaint as Exhibit 16 prominently shows a sticker with the part number V2DP. A simple Internet search reveals that this motherboard is simply a Socket A Athlon motherboard made by Jetway Computer and designed to work in a generic computer. See Exhibit 12 submitted herewith and compare to Exhibit 16 to Trend Micro's Complaint. Second, the power supplies used by Barracuda in the Accused Barracuda Products are staple

articles of commerce and are in no way tied to the alleged invention of the ‘600 patent. See Exhibit 13 submitted herewith showing Supermicro power supply with part number PWS-0043 and compare to Exhibit 16 showing power supply with same part number. Finally, Barracuda does not import ClamAV. The ClamAV source code is publicly available for free download on the www.sourceforge.net website. The Sourceforge website provides links to a worldwide network of mirror servers for downloading the open source software, and the Sourceforge website uses technology that matches requesters with a mirror server near the requester’s geographic location. See Exhibit 14 showing that the Sourceforge website uses IP Geolocation to match a requestor with a nearby mirror server. Contrary to Trend Micro’s assertions, Barracuda downloads the ClamAV source code from a server in the United States, installs it on the Accused Barracuda Products in the United States, and manufactures and assembles the Accused Barracuda Products in the United States. See Exhibit 15 showing manufacture of the Accused Barracuda Products at Barracuda’s facility in Campbell, California.

84. In addition, Trend Micro cannot show that a domestic industry exists as defined in Section 337(a)(3). For example, Trend Micro has merely taken a cursory approach to establishing the technical prong of domestic industry. Such an approach fails to meet the Commission’s test for establishing whether a patent is being exploited. In particular, Trend Micro does not define the domestic industry anywhere in its Complaint. Further, Trend Micro has not provided claim interpretation, and thus has not provided the required analysis to show that any of the asserted claims are being exploited. In addition, Trend Micro’s general identification of unspecified investments in the exploitation of the ‘600 Patent is misleading. In making its assertions, Trend Micro overreaches by including articles and activities that are not covered by the ‘600 Patent and, thus, do not contribute to a domestic industry exploiting the ‘600 Patent. Trend Micro also overreaches by including activities not of the type to support a finding of domestic industry.

Second Affirmative Defense

(*Noninfringement*)

85. Barracuda is not infringing, nor has it ever infringed, any claim of the '600 Patent. To the extent that Trend Micro attempts to construe the scope of the claims of the '600 Patent to cover any product offered for sale, used or sold by Barracuda, such claims are invalid as failing to meet the requirements of Title 35 of the United States Code, and therefore, cannot be infringed.

86. The Accused Barracuda Products do not infringe any claim of the '600 Patent for at least the following reasons. By way of illustration using representative claim 4 of the '600 Patent, and without limitation, in Barracuda's products all files are scanned by Barracuda's virus-scanning engine to determine whether the file contains a virus. Specifically, Barracuda's products do not determine whether data is of a type that is likely to contain a virus, and Barracuda's Products check the data for a virus regardless of whether "the data is likely to contain a virus." By way of further example, the Accused Barracuda Products are missing at least the following elements of dependent claim 2 and independent claims 11, 13 and 18, and the related dependent claims, of the '600 Patent: Barracuda's products do not contain the claimed FTP proxy server or FTP daemon. Specifically, the Barracuda Spam Firewall and the Barracuda IM Firewall do not support FTP traffic. The Barracuda Web Filter does not detect viruses in FTP uploads. The Accused Barracuda Products also do not store each encoded portion of a mail message in a separate temporary file and then decode the encoded portions of the mail message. Specifically, the Barracuda Web Filter and the Barracuda IM Firewall do not handle mail messages; the Barracuda Spam Firewall does not selectively check mail messages for viruses based on whether the mail messages have encoded portions. Nor do the Accused Barracuda Products infringe the means-plus-function claim set forth in claim 18, as the implementation of the Accused Barracuda Products differs substantially from that set forth

by the specification of the '600 Patent. A chart illustrating Barracuda's noninfringement of all asserted claims is attached hereto as Exhibit 1.[1]

Third Affirmative Defense

(*Invalidity*)

87. The '600 Patent is invalid for failure to meet the statutory requirements of Title 35 of the United States Code, including, but not limited to, failure to comply with the requirements of 35 U.S.C. § 101, 102, 103 and 112.

88. The items of prior art that anticipate and/or render obvious the asserted claims of the '600 patent are cited and described in the attached Exhibits 2-11 and are produced herewith. These claim charts show how certain prior art references expressly or inherently discloses all elements of the asserted claims of the '600 patent. To the extent that a particular prior art reference does not expressly or inherently disclose all elements of an asserted claim, combining these references with other of the prior art references would have been obvious in light of the reasons and/or motivations to do so discussed below, including, among other things, market forces at the time of the '600 patent. Examples of such combinations are identified below, described below in connection with the motivation to combine and described in the attached claim charts, although numerous other combinations would also have been obvious to try both with the references disclosed in Exhibits 2-11 and those listed below as "Background References."

89. In addition to the references detailed in Exhibits 2-11 hereto, Barracuda discloses the following "Background References," all of which provide context demonstrating the invalidity of the '600 patent. Each reference listed below is submitted herewith unless notated with an * indicating that Barracuda has thus far been unable to locate and/or obtain

[1] Barracuda has produced its source code (BAR-TM 006517) to Trend Micro and will produce its source code to the Office of Unfair Import Investigations, but has not submitted its source code herewith. Barracuda's source code and/or references from source code will be provided to the ALJ at the appropriate time and subject to the appropriate precautions, or upon request for earlier provision.

third party permission to use (and therefore is unable to produce) such reference at this time, but, which, on information and belief, anticipate and/or render obvious the claims of the '600 patent.

(1) Hamner et al., E-Mail as a Tool for Sharing Binary Files among Scientists, J. Chem. Inf. Comput. Sci. (May/June 1994) (BAR-TM 002794-002800).

(2) Arnold et al., Employment of Virus Detection Procedures at Domain Boundaries, IBM Technical Disclosure Bulletin (December 1991) ("IBM Article") (BAR-TM 002341-002342).

(3) Dalva, D., Security and the World Wide Web, Trusted Information Systems (June 1994) ("Dalva Article") (BAR-TM 006124-006126).

(4) Rigney, S., "Inoculating your LAN; Software Review; Central Point Software Inc.'s Central Point Anti-Virus, Intel Corp Personal Computer Enhancement Operation's LANProtect 1.5; Evaluation," Computer Shopper (June 1993) ("Rigney Article") (BAR-TM 006611-006616).

(5) C2C Systems, "Internet From C2C Systems" (February 8, 1995) ("C2C Press Release") (BAR-TM 002986-002987).

(6) U.S. Patent No. 5,319,776, issued to Hile et al., June 7, 1994 ("Hile") (BAR-TM 003281-003291).

(7) U.S. Patent No. 5,511,163, issued to Lerche et al., April 23, 1996 ("Lerche") (BAR-TM 003446-003454).

(8) Japanese Published Patent Application No. H06-350784, published to Ooseto, December 22, 1994 ("Cited Japanese Application") (BAR-TM 003266-003275); English translation (BAR-TM 006801-006816).

(9) European Patent Application No. 0 666 671 A1, published to Dassault, August 9, 1995 ("Cited European Application") (BAR-TM 003258-003265); English translation (BAR-TM 006600-006610).

(10) U.S. Patent No. 5,649,095, issued to Cozza, July 15, 1997 ("Cozza") (BAR-TM 006542-006556).

(11) NETSYS.COM, Online discussion thread (May 27, 1994) (BAR-TM 003151-003152).

(12) UUencode web page printed from http://www.mcsr.olemiss.edu/cgi-bin/man-cgi?uuencode+1 (BAR-TM 002352-002353).

(13) Freed, N. and Borenstein, N., "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies," Network Working Group, Request for Comments: 2045 (November 1996) (BAR-TM 006572-006599).

(14) Shelldorado, "Sending Files as Mail Attachments" (BAR-TM 006567-006571).

(15) Byte Magazine, Steven Cobb, McGraw-Hill, copyright 1995 (BAR-TM 006817-006820).

(16) A Magic Bullet for Network Viruses (BAR-TM 002491-002492).

(17) Advanced Programming in the UNIX Environment (BAR-TM 002493-002530).

(18) An EMACS Based Downgrader for SAT (BAR-TM 002531-002540).

(19) Answers to Frequently Asked Questions About Network Security (BAR-TM 002541-002579).

(20) Architecture Tech. Corp., The LOCALNetter Newsletter (BAR-TM 002580-002591).

(21) Computer Security: Art and Science (BAR-TM 002592-002625).

(22) Constructing a High Assurance Mail Guard, Secure Computing Corporation (BAR-TM 002626-002635).

(23) Data and Computer Communication (BAR-TM 002636-002793).

(24) Functional Requirements for: A Trusted Mail Gateway (BAR-TM 002806-002967).

(25) Internet Firewall and Network Security (BAR-TM 002968-002985).

(26) Internet Suffers Growing Pains (BAR-TM 002988-002989).

(27) Mier, Another Brick in the Firewall - The Internet offers great possibilities; it also offers unwanted network intrusions, CommunicationsWeek, dated September 18, 1995 (TMI_BN0013872-0013874).

(28) D-Link Layer 3 Modular Chassis-based 10/100 Mbps (BAR-TM 006831-006834).

(29) Checkpoint Software Technologies, Inc., An Integrated, Secure, and Manageable Security Infrastructure (BAR-TM 006835-006858).

(30) ServGate, Gigabit Security with the ServGate SG2000 White Paper (BAR-TM 006859-006870).

(31) ServGate, Securing the Enterprise Network Application Note (BAR-TM 006871-006886).

(32) Boyle, Buyer's Guide: Virus Scanning Tools, PC Magazine, dated November 21, 1995 (BAR-TM 006887-006889).

(33) Bender, Entry-level Network Management, STACKS, dated November 1, 1994 (BAR-TM 006890-006900).

(34) Carr, The World Wide Web and Private Intranets are Inviting for VARs speaking TCP/IP, VARBUSINESS, dated December 15, 1995 (BAR-TM 006901-006905).

(35) LOCK Treck: Navigating Uncharted Space (BAR-TM 002990-002998).

(36) MAILbus Postmaster for LANs/WANs v2.0 (BAR-TM 002999-003000).

(37) NetShield 1.03 Manual (BAR-TM 003001-003012).

(38) NetShield 1.60 Manual (BAR-TM 003013-003039).

(39) Network Firewalls (BAR-TM 003040-003047).

(40) Network Security Secrets (BAR-TM 003048-003093).

(41) Product Review 1-D-FENCE, Virus Bulletin (BAR-TM 003094-003141).

(42) Proxy-Based Authorization and Accounting for Distributed Systems, Distributed Computing Systems, IEE Conf. (BAR-TM 003142-003150).

(43) Re: virus checking utilities (BAR-TM 003151-003152).

(44) Re: virus checking utilities – 5/27/94 Email from P. Danielson (BAR-TM 003153-003154).

(45) Re: virus checking utilities – 5/28/94 Email from C. Rosenthal (BAR-TM 003155-003156).

(46) Security Pipeline Interface (SPI) (BAR-TM 003157-003165).

(47) The Design of a Secure Internet Gateway (BAR-TM 003166-003170).

(48) There Be Dragons (BAR-TM 003171-003186).

(49) Thus Far and No Further (BAR-TM 003187-003189).

(50) Virus Prevention NLMs (BAR-TM 003190-003198).

(51) United States Patent No. 5,864,683 (BAR-TM 003199-003233).

(52) United States Patent No. 5,889,943 (BAR-TM 003234-003257).

(53) European Patent No. 0 666 671 A1 (BAR-TM 003258-003265).

(54) Japan Patent No. 6350784 (BAR-TM 003266-003275).

(55) United States Patent No. 4,975,950 (BAR-TM 003276-003280).

(56) United States Patent No. 5,414,833 (BAR-TM 003298-003341).

(57) United States Patent No. 5,440,723 (BAR-TM 003342-003370).

(58) United States Patent No. 5,444,850 (BAR-TM 003371-003381).

(59) United States Patent No. 5,448,668 (BAR-TM 003382-003392).

(60) United States Patent No. 5,452,442 (BAR-TM 003393-003411).

(61) United States Patent No. 5,458,575 (BAR-TM 003412-003430).

(62) United States Patent No. 5,491,791 (BAR-TM 003431-003445).

(63) United States Patent No. 5,511,163 (BAR-TM 003446-003454).

(64) WIPO Patent No. 9322723 (BAR-TM 003455-003479).

(65) Product Review Trend's PC Rx, Virus Bulletin, October 1992. (BAR-TM 006518-006541).

(66) U.S. Patent No. 5,586,260 (BAR-TM 006647-006654).

(67) U.S. Patent No. 5,623,601 (BAR-TM 006617-006635).

(68) U.S. Patent No. 5,632,011 (BAR-TM 006636-006646).

(69) Ans Co+Re Systems, Inc. White Paper-InterLock 2.1.*

(70) Central Point Software, Inc. Anti-Virus for NetWare 2.0 product.*

(71) CheckPoint Software Technologies Ltd., Checkpoint Firewall-1-Technical White Paper.*

(72) Cheyenne Software, Inc., InocuLAN 2.5d and 3.0 products.*

(73) Gargoyle Trusted Mail Gateway Source Code.*

(74) Jeffrey Mogul, "RFC 917: Internet Subnets" (Oct. 1984) (see, e.g., pages 13-14).

(75) J. Mogul & J. Postel, "RFC 950: Internet Standard Subnetting Procedure" (Aug. 1985) (see, e.g., Section 2.2).

(76) C. Hedrick, "RFC 1058: Routing Information Protocol" (June 1988) (see, e.g., page 24).

(77) E. Krol, "RFC 1118: The Hitchhikers Guide to the Internet" (Sept. 1989) (see, e.g., page 12).

(78) T. Socolofsky & C. Kale, "RFC 1180: A TCP/IP Tutorial" (Jan. 1991) (see, e.g., Sections 5.7 and 5.8).

(79) U.S. Patent No. 5,257,381 (BAR-TM 006557-006566)

(80) Socolofsky, T. et al., A TCP/IP Tutorial, Spider Systems Limited (January 1991) (BAR-TM 006655-006687)

(81) Krol, E., The Hitchhikers Guide to the Internet, University of Illinois Urbana (September 1989) (BAR-TM 006688-006715)

(82) Hedrick, C., Routing Information Protocol, Rutgers University (June 1988) (BAR-TM 006716-006753)

(83) Mogul, J., Internet Standard Subnetting Procedure (August 1985) (BAR-TM 006754-006774)

(84) Mogul, J., Internet Subnets, Stanford University (October 1984) (BAR-TM 006775-006800)

(85) Cisco Systems, Inc., Increasing Security on IP Networks, an advertising brochure.*

(86) Command Software Systems, Inc., Net-Prot 1.24 product.*

(87) Fifth Generation Systems, Inc., Untouchable Network NLM product.*

(88) GROUP GmbH Watchdog Software.*

(89) Hilgraeve Corporation, HyperACCESS product.*

(90) Integralis MIMESweeper and WebSweeper line of products.*

(91) IBM Tivoli line of products.*

(92) InterDyn Conclave line of products.*

(93) Tumbleweed (f/k/a Worldtalk) line of products.*

(94) McAfee VirusScan 2.1 product*

(95) Norton Desktop Product, v. 2.0, Virus Bulletin.*

(96) Norton AntiVirus for NetWare 1.0 product.*

(97) Ontrack Computer Systems, Inc., Dr. Solomon's Anti-Virus Toolkit for NetWare 1.03.*

(98) Request for Comment 1579, Firewall-Friendly FTP, Network Working Group, S. Bellovin.*

(99) SAM product (Symantec Antivirus for Macintosh).*

(100) Seattle Software Labs, WatchGuard Firewall product.*

(101) Stempel, Ipaccess-an Internet Service Access System for Firewall Installations, Network and Distributed System Security, IEEE, p. 31-41.*

(102) Symantec (Norton), Norton AntiVirus product, Virus Bulletin 24.*

(103) Trend Micro Devices, Inc., Interscan product.*

(104) Trend Micro Devices, Inc. PC-Cillin product.*

(105) Trend Micro Devices, Inc., StationLOCK, Virus Bulletin.*

(106) Enhanced Multinet Gateway: Survivable Multi-Level Secure Data Communications.*

(107) Documentation regarding UNIX Expo Trade Shows: Expo '93 Office Show Directory.*

(108) Gargoyle Invoice No. ARMA-951108.*

(109) 3.5" floppy with Norman Firewall manuals from CAAS.*

(110) "The Norman Firewall Version 2.0 – Administration Guide, User Guide, Maintenance Guide".*

(111) Declaration of Lee Taylor (Feb. 1998, Senior Sales Exec. for NDDS).*

(112) Norman Technical Report #6: Internet Security Threats and Firewalls (Jan. 1995).*

(113) Six pages of Norman sales brochures.*

(114) "Joint Development and Marketing Plan – Agreement in Principle" between NDDS and CA&S, Nov. 15, 1994.*

(115) "Communications Arts & Sciences (CA&S) Internet Firewall, October 30, 1994" marketing materials.*

(116) "Internet Risks and Countermeasures" NDD presentation.*

(117) "Marketing Proposal for Norman Firewall: Automated Viral Analysis for the World" 1994.*

(118) "The Norman Firewall – User's Guide, Administration Guide, Maintenance Guide" November 1995, for Norman Firewall v. 1.3.*

(119) NDDS Firewall Source Code (F-NN 00001-134).*

(120) Intel LANDesk Virus Protect Version 3.0 product (May 9, 1995).*

(121) Intel LANProtect (v. 1.5) product (1992).*

(122) Digital Equipment Corp., Screen External Access Link (SEAL) Introductory Guide.*

(123) Neale, Secure Connections to the Internet, The Eleventh World Conference on Computer Security, Audit and Control Proceedings (Oct. 12-14, 1994) (Digital Electronic Corp.).*

(124) Amendment of Solicitation/Modification Contract between U.S. Government and TIS (July 3, 1994).*

(125) fwtk.dir source code modules v. 1.3, dated Nov. 4, 1994.*

(126) Discussions from Firewalls Mailing List, dated between Dec. 1994 and April 1995.*

(127) Article from Federal Computer Week entitled, "Vendors Offer 'Firewall' Technology for Internet Security," dated August 8, 1994.*

(128) TIS document entitled "Trusted Information Systems Internet Firewalls and Overview".*

(129) Marcus Ranum email announcing TIS fwtk 1.3, dated Nov. 4, 1994.*

(130) Business Communication Review article entitled, "Building Internetwork Firewalls" by Avolio, dated Jan. 1994.*

(131) TIS presentation slides entitled, "The Internet Firewall Toolkit Experiences and Lessons Learned," by Avolio and Ranum, dated June 3, 1994.*

(132) Gauntlet Internet Firewall Administrator's Guide for Windows NT, Ver. 1.0, copyrighted 1991, 1993, 1996-97.*

(133) Gauntlet Internet Firewall Administrator's Guide for Ver. 3.2 copyrighted 1995-96.*

(134) Gauntlet Internet Firewall Administrator's Guide for Ver. 3.1, copyrighted 1995-96.*

(135) TIS Network Security Products Presentation Material, dated Jan. 28, 1996.*

(136) Memorandum from Lipner to Avolio regarding the TIS Firewall Information and Financial Data, dated Aug. 6, 1999.*

(137) Ranum, Internet Firewalls – An Overview, a slide presentation, TIS (1993 and/or 1994).*

(138) TIS document entitled "TIS, Secure External Access and Service-Providing Protection for the Network," dated September 17, 1993.*

(139) TIS, "Secure Access and Service Prototype," April 9, 1993.*

(140) Jarpenpaa and Ives, Digital Equipment Corporation: The Internet Company (A) (Oct. 1994).*

(141) Stevens, Advanced Programming in the UNIX Environment (1993).*

(142) Tirenin et al., Enhanced Multinet Gateway: Survivable Multi-Level Secure Data Communications, Milcom IEEE, pp. 740-744 (1991).*

90. Exhibit 2 demonstrates how the claims of the '600 patent are anticipated and/or rendered obvious by the Norman Firewall product which was publicly demonstrated at the Federal Office Systems Expo (FOSE) trade show in March 1995, and therefore qualifies as prior under at least 35 U.S.C. § 102(a) and (g). At least David Stang, Michael Crider, Jay Nispel, Kristian Bognaes, Kurt Natvig, Gunnel Wullstein, Lee Taylor, John Morris, Gina Dolan, Alan Walden, John Bradshaw and Tim McGee may have been involved in the creation of Norman Firewall. It is described in the following documents submitted herewith:

(1) Norman Data Defense, Inc., The Norman Firewall User and Administration/Maintenance Guides (April 1995) (BAR-TM 005074-005100).

(2) Kothari, et al., The Norman Firewall White Paper, Norman Development US (1995) (BAR-TM 005101-005110).

(3) Press Release "Norman Data Defense Systems Unveils The Norman Firewall", PR Newswire, March 21, 1995 (BAR-TM 005071-005073).

(4) Norman Data Defense, Inc., An Introduction to the Norman Firewall, (June 1995) (BAR-TM 005057-005070).

(5) Norman Data Defense, Inc., Marketing Proposal for Norman Firewall: Automated Virus Analysis for the World (1994) (TMI_BN00057834-00057836).

(6) Norman Data Defense Systems, Inc. Product Service Profile and News Release re FOSE '95, March 6, 1995 (BAR-TM 002299).

(7) The Norman Firewall White Paper, Norman Development USA (BAR-TM 005101-005110).

(8) Diskette containing source code for the anti-virus platform of Norman Firewall product (BAR-TM 005111). [2]

(9) Source Code for the anti-virus platform of Norman Firewall product-"index" (BAR-TM 005112).

(10) Photographs of the Norman Firewall as displayed at a demonstration booth at the CeBit trade show exhibition in March 13, 1995 (BAR-TM 005113-005123).

(11) Email Correspondence between Kristian Bognaes and counsel for Fortinet (BAR-TM 005124-005266).

(12) Source Code for the anti-virus platform of Norman Firewall product titled, "Firewall.C" (BAR-TM 005267-005326).

(13) Source Code for the anti-virus platform of the Norman Firewall product titled "AV.C." (BAR-TM 005327-005386).

(14) Source Code for the anti-virus platform of the Norman Firewall product titled "AV.TXT." (BAR-TM 005391-005398).

(15) Source Code for the anti-virus platform of the Norman Firewall product titled "FW.TXT." (BAR-TM 005391-005398).

(16) Deposition Transcript and Video of Kristian Bognaes in Certain Systems for Detecting and Removing Viruses or Worms, Components Thereof and

[2] The source code for the Norman Firewall antivirus platform (BAR-TM 005111) and for the TIS Firewall Toolkit (BAR-TM 005975) has been produced to Trend Micro and will be produced to the Office of Unfair Import Investigations, but is not submitted herewith. Source code and/or references from source code will be provided to the ALJ at the appropriate time and subject to the appropriate precautions, or upon request for earlier provision.

Products Containing Same, Investigation No. 337-TA-510 (BAR-TM 005399-005455).

(17) Declaration of Dr. David Stang in *Integralis, Inc. v. Trend Micro, Inc.* Litigation (TMI_BN0024510-0024513).

91. Exhibit 3 demonstrates how the claims of the '600 patent are anticipated and/or rendered obvious by the Intel LANProtect Version 1.5 product (1992) and Intel LANDesk Virus Protect Version 3.0 product (May 9, 1995) which were publicly offered for sale in the United States by Intel Corp ("Intel Products"), and therefore qualifies as prior under at least 35 U.S.C. § 102(a) and (g). The Intel LANDesk Virus Protect product was a later version of the Intel LANProtect product. At least Eva Chen, John Sutherland, Cliff Liang, Steve Chang, Jenny Chang, Oscar Chang, Tyrone Pike, Ed Ekstrom, Colin Cook, Cindy Snow, David Rowe and Dana Doggett may have been involved in the creation of the Intel Products. On information and belief, the inventions of the '600 patent are invalid under 35 USC § 102(f) because the patent fails to name all actual inventors and only the actual inventors. Individuals at Intel contributed to the conception of the inventions of the '600 patent. The inventions of the '600 patent are further invalid under 35 USC § 102(g) because the inventions claimed '600 patent were derived from one or more persons from Intel, the identities of whom are yet to be determined. The Intel Products are described in the following documents submitted herewith:

(1) Transcript of Deposition of Eva Chen taken June 3, 1999 in Trend Micro, Inc. v. Network Associates (TMI_BN0015211-0015249).

(2) Transcript of Deposition of Eva Chen taken July 13, 1999 in Trend Micro, Inc. v. Network Associates (TMI_BN0015715-0015768).

(3) Understanding Virus Firewall Protection: The Intel LANDesk Virus Protect Solution, Intel Corporation (July 1997) (BAR-TM 005050-005056).

(4) Intel and Novell Sign Site Licensing Agreement for Intel's LANProtect Network Virus Protection Software (BAR-TM 004492-004493).

(5) Intel Corp. LANDesk (BAR-TM 004494).

(6) Intel DX2, Microcomputer Solutions (BAR-TM 004495-004521).

(7) Intel FlashFile Memory and the Low-voltage Intel 386 SL Microprocessor, Microcomputer Solutions (BAR-TM 004522-004548).

(8) Intel LANDesk Management Suite v2.5 A Closer Look (BAR-TM 004549-004672).

(9) Intel LANDesk Management Suite v2.5 (BAR-TM 004673-004720).

(10) Intel LANDesk Server Monitor Module Installation and User's Guide (BAR-TM 004721-004918).

(11) Intel LANDesk Virus Protect User's Guide (BAR-TM 006403-006516).

(12) Intel LANProtect 30-Day Test Drive Version (BAR-TM 004919-004953).

(13) Intel LANProtect Software User's Guide (BAR-TM 004954-005042).

(14) Intel LANDesk provides solid management base (BAR-TM 005043-005044).

(15) Intel LANProtect 1.5 Software Offers Enhanced Network Virus Protection (BAR-TM 005045-005047).

(16) LANDesk 2.0 adopts DMI to control PC costs (BAR-TM 005048).

(17) SMS, LANDesk offer much-needed IT relief (BAR-TM 005049).

(18) Understanding Virus Firewall Protection: The Intel LANDesk Virus Protect Solution (BAR-TM 005050-005056).

92. Exhibit 4 demonstrates how the claims of the '600 patent are anticipated and/or rendered obvious by the Trusted Information Systems Firewall Toolkit Version 1.3, by Marcus Ranum et al. (publication release date: November 4, 1994), and therefore qualifies as prior under at least 35 U.S.C. § 102(a) and (g). The Gauntlet Firewall is an implementation of the TIS Firewall Toolkit (collectively "TIS Firewall"). At least Frederick Avolio, Marcus Ranum, Edward Walters, Steven Lipner, David Dalva, Stephen T. Walker, Gene Hodges, Sandra England, Stephen Kane, Tom Ashoff, Peter Churchyard, Jeff Graham, Vincent Hwang, Dave Mason, Steve Chew, Doug Rothnie and Tycho, Hayashibara may have been involved in the

creation of TIS Firewall. TIS Firewall is further described in the following documents submitted herewith:

(1) TIS Firewall Toolkit Overview (1994) (TMI_BN0040493-0040506).

(2) TIS Source Code (BAR-TM 006127-006195 and BAR-TM 006222-006231).

(3) Ranum, M. et al., A Toolkit and Methods for Internet Firewalls, Summer 1994 USENIX Conference (TMI_BN0013890-0013898).

(4) Gauntlet Internet Firewall FAQ (BAR-TM 005996-006004).

(5) Ranum Declaration in Integralis v. Trend Micro litigation (TMI_BN0052141-0052143).

(6) A Network Perimeter with Secure External Access (BAR-TM 005861-005870).

(7) A Network Firewall, Digital Equipment Corporation, Washington Open Systems Resource Center, Greenbelt, Maryland (BAR-TM 005871-005880).

(8) Brief History of Changes Made to the FWTK (BAR-TM 005891-005895).

(9) Brief History of Changes Made to the FWTK v.1.0 (BAR-TM 005896-005897).

(10) Brief History of Changes Made to the FWTK v.1.2 (BAR-TM 005898-005900).

(11) Brief History of Changes Made to TIS Firewall (BAR-TM 005901-005920).

(12) C Library Functions (manpages) (BAR-TM 005921-005956).

(13) Commercial Internet Security Firewall Announced by Trusted Information Systems: Computer Security Threat Monitoring and Surveillance (BAR-TM 005957-005958).

(14) Digital Equipment Corporation: The Internet Company (A) (BAR-TM 005959-005974).

(15) Firewall ToolKit Archive Information (BAR-TM 005975).

(16) Firewall User's Overview (BAR-TM 005976-005980).

(17) FWTK Downloads (BAR-TM 005981-005984).

(18) FWTK FAQ version 3.2 (BAR-TM 005985-005988).

(19) FWTK Patches (BAR-TM 005989-005990).

(20) Gauntlet Firewall Prospectus (BAR-TM 005991-005995).

(21) Gauntlet Firewall FAQ (BAR-TM 005996-006004).

(22) Gauntlet Firewall Overview (BAR-TM 006005).

(23) Gauntlet Product Overview (BAR-TM 006006-006035).

(24) History of the FWTK (BAR-TM 006036-006038).

(25) Internet Firewalls: An Overview (BAR-TM 006039-006099).

(26) Network (IN) Security Through IP Packet Filtering, Proceeding of the Third USENIX UNIX Security Symposium (BAR-TM 006100-006113).

(27) Secure Connections to the Internet, The Eleventh World Conference on Computer Security, Audit and Control Proceedings (BAR-TM 006114-006123).

(28) Security and the World Wide Web (BAR-TM 006124-006126).

(29) Source Code from Marcus J. Ranum (BAR-TM 006127-006195).

(30) Thinking About Firewalls, Trusted Information Systems, Inc. (BAR-TM 006196-006205).

(31) Three New Firewall Proxies from TIS (BAR-TM 006206-006207).

(32) TIS Firewall Toolkit Configuration and Administration (BAR-TM 006208-006221).

(33) TIS Source Code (from Marcus J. Ranum) (BAR-TM 006222-006231).

(34) Deposition of Fredrick Avolio (TMI_BN0040874-41030).

93. Exhibit 5 demonstrates how the claims of the '600 patent ware anticipated and/or rendered obvious by the Sidewinder product ("Sidewinder") which was available from Secure Computing Corporation and publicly known in the United States by 1994, and therefore qualifies as prior under at least 35 U.S.C. § 102(a) and (g). At least William Boebert, Spencer

Mineaer, Clyde Rogers, Glenn Andreas, Scott Hammond and Mark Gooderman may have been involved in the creation of Sidewinder. It is described in the following documents submitted herewith:

(1) The LOCALNetter Newsletter - Special Report: Secure Computing Corporation and Network Security, Vol. 14, No. 12, Dec. 1994 (BAR-TM 002580-2591).

(2) Secure Computing Corporation - Answers to Frequently Asked Questions About Network Security, Secure Computing Corporation (1994) (TMI 00076385-76423).

(3) Sidewinder Administration Guide v.1.0 (BAR-TM 005456-005505).

(4) Boebert, W. et al., Sidewinder and Virus Scans, on-line discussion October 16, 1999, www.netsys.com (TMI_BN0014147-0014149).

(5) Sidewinder Administration Guide v.2.0 (BAR-TM 005506-005857).

(6) Ranum Declaration in Integralis v. Trend Micro litigation (TMI_BN0052141-143).

(7) Eng, S., "Software the Reins in 'Trojan Horses,'" Business Week (October 31, 1994) (TMI_BN0065651).

(8) Rodriguez, Karen, "Sidewinder provides ironclad security; Firewall system used by military," InfoWorld (October 10, 1994) (TMI_BN0083122-0083123).

(9) Sidewinder: Application of Type Enforcement (BAR-TM 005858-005860).

94. Exhibit 6 describes how the claims of the '600 patent are anticipated and/or rendered obvious by Smith R., Constructing a High Assurance Mail Guard, Secure Computing Corporation (1994) (TMI_BN0083213-0083219), and therefore qualifies as prior under at least 35 U.S.C. § 102(a) and (g). The Secure Network Server Mail Guard ("SMG") was available from Secure Computing Corporation and publicly known in the United States by at least 1994.

95. Exhibit 7 describes how the claims of the ‘600 patent are rendered obvious by Cheswick, W. et al., Firewalls and Internet Security, AT&T Bell Labs, Inc. (April 30, 1994) (“Cheswick”) (BAR-TM 002806-002967). This publication qualifies as prior art under at least 35 U.S.C. §§ 102(a) and (b).

96. Exhibit 8 describes how the claims of the ‘600 patent are rendered obvious by Layland, R., A Gateway to Internet Health and Happiness, Data Communications (September 21, 1994) (“Layland”) (BAR-TM 002489-002490). This publication qualifies as prior art under at least 35 U.S.C. §§ 102(a) and (b).

97. Exhibit 9 demonstrates how claims of the ‘600 patent are anticipated and/or rendered obvious by the Gelb Firewall, created by Edward J. Gelb which was created in the United States prior to May 1995), and therefore qualifies as prior under at least 35 U.S.C. § 102(a) and (g). The Gelb Firewall is described in the following documents submitted herewith:

(1) U.S. patent No. 5,550,984 (BAR-TM 004485-004491).

(2) Virus Bulletin (October 1992) (BAR-TM 006518-006541).

(3) Chapters 1-4 and FAQs from gelb.com (BAR-TM 004430-004478, BAR-TM 004479-004484).

98. Exhibit 10 demonstrates how the claims of the ‘600 patent are anticipated and/or rendered obvious by the Gargoyle system which was created by Armadillo Systems, Inc. and offered for sale in the United States no later than May 1995 (“Gargoyle”), and therefore qualifies as prior under at least 35 U.S.C. § 102(a) and (g). At least Leroy Lacy, Randolf B. Brown and Michael Rose may have been involved in the creation of Gargoyle. It is described in the following documents submitted herewith:

(1) Costales et al., sendmail, O’Reilly and Associates, Inc., 1993 (TMI_BN0008958-0009038).

(2) Purchase Order for Trusted Mail Gateway for Her Majesty’s Treasury (BAR-TM 003964).

(3) A Standard for Secure Encapsulation and Transfer, Draft A (BAR-TM 003532-003574).

(4) CASM, Prototype CryptGuard, Test Plan, Draft A (BAR-TM 003575-003583).

(5) CASM, Securing Electronic Mail Within Government, Prototype CryptGuard: Concept of Operation, Issue 1.0 (BAR-TM 003584-003595).

(6) CASM, Securing Electronic Mail Within Government, Prototype CryptGuard: Concept of Operation, Issue 1.0 (BAR-TM 003584-003595).

(7) Enterprise Mail Version 3 for Window: installation and Configuration Guide (BAR-TM 003596-003716).

(8) Functional Requirements for: A Trusted Mail Gateway (BAR-TM 003717-003725).

(9) Gargoyle Documentation (BAR-TM 003726-003767).

(10) Gargoyle Documentation re NIO Proposal (BAR-TM 003768-003828).

(11) Gargoyle Notes and Documentation re SXG (BAR-TM 003829-003884).

(12) Gargoyle Trusted Mail Gateway Diagram (BAR-TM 003885).

(13) Gargoyle Trusted Mail Marketing Documents: Gargoyle Trusted Mail Gateway System Description (BAR-TM 003886-003897).

(14) Gargoyle Trusted Mail Marketing Documents: Gargoyle Options (BAR-TM 003898-003899).

(15) Gargoyle Trusted Mail Marketing Documents: Securing Networks in a Changing World (BAR-TM 003900-003906).

(16) Gargoyle Trusted Mail Marketing Documents: Trusted Mail Gateway System Specification (BAR-TM 003907-003908).

(17) Gargoyle Trusted Mail Marketing Documents: Armadillo Systems PowerPoint Presentation (BAR-TM 003909-003941).

(18) GuardMail Version 3.0 Configuration Guide (BAR-TM 003942-003957).

(19) Invoice Number ARMA-950601 (BAR-TM 003958).

(20) Release Notes for GuardMail 1.3 (BAR-TM 003965).

(21) SecureMail User's Guide (BAR-TM 003966-004095).

(22) SecureMail User's Guide for the Compartmented Mode Workstation (CMW) (BAR-TM 004096-004235).

(23) Securing Electronic Mail Within HMG, Part 1, Infrastructure and Protocol (BAR-TM 004236-004263).

(24) Task Requirements Specification for CASM CryptGuard, Draft B (BAR-TM 004264-004278).

(25) White Paper: Gargoyle as a CASM CryptGuard for Serco CIT (BAR-TM 004279-004349).

99. Exhibit 11 demonstrates how the claims of the '600 patent are anticipated and/or rendered obvious by the MpScan, VFind and CVDL products (collectively "MpScan") which were developed, publicly demonstrated and offered for sale in the United States by Peter Radatti and CyberSoft, Inc. by 1993), and therefore qualifies as prior under at least 35 U.S.C. § 102(a), (b), and (g). On information and belief, the MpScan products also anticipate and/or render obvious the claims of the '600 patent. The MpScan products are described in the following documents submitted herewith:

(1) Computer Viruses In Unix Networks (BAR-TM 004350-004362).

(2) Connecting to the Internet: Security Considerations (BAR-TM 004363-004369).

(3) Documentation and Advertising re: products: CyberSoft, Inc. Advertising Sheet (BAR-TM 004370).

(4) Documentation and Advertising re: products: Synopses of CyberSoft and Products (BAR-TM 004371-004372).

(5) Documentation and Advertising re: products: CyberSoft Products List (BAR-TM 004373).

(6) Documentation and Advertising re: products: Vfind (BAR-TM 004374-004385).

(7) Documentation and Advertising re: products: Why Vfind (BAR-TM 004386-004397).

(8) Documentation and Advertising re: products: K-Lock (BAR-TM 004398).

(9) Documentation and Advertising re: products: Transworld Talk (BAR-TM 004399).

(10) Documentation and Advertising re: products: MpScan (BAR-TM 004400-004401).

(11) Documentation and Advertising re: products: Federalist (BAR-TM 004402).

(12) Documentation and Advertising re: products: COPS (BAR-TM 004403).

(13) Documentation and Advertising re: products: Hot News for the Press (BAR-TM 004404).

(14) Documentation and Advertising re: products: Vfind locates viruses on Unix, Mac, DOS Systems (BAR-TM 004405).

(15) Documentation re: Unix Expo Trade Shows: Expo '94 Official Show Directory (BAR-TM 004406-004407).

(16) Documentation re: Unix Expo Trade Shows: Qualix Group Buyers' Guide (BAR-TM 004408-004409).

(17) Documentation re: Unix Expo Trade Shows: Expo '93 Nametag for P. Radatti (BAR-TM 004414-004415).

(18) Documentation re: Unix Expo Trade Shows: Expo '93 Floor Plan (BAR-TM 004416-004419).

(19) Documentation re: Unix Expo Trade Shows: Computer Virus Awareness for UNIX, from NCSA News (BAR-TM 004420).

(20) Documentation re: Unix Expo Trade Shows: MpScan Promotional Materials (BAR-TM 004421-004422).

(21) Technical White Paper: Heterogeneous Computer Viruses in a Networked Unix Environment (BAR-TM 004423-004424).

(22) Technical White Paper: The CyberSoft Virus Description Language (BAR-TM 004425-004429).

100. Antigen, created by Sybari, was publicly available in the United States before the conception of the '600 patent, and therefore qualifies as prior under at least 35 U.S.C. § 102(a) and (g). At least Gregory Tetrault, Denis Lisica and Kenneth D. Toole may have been involved in the creation of Antigen. On information and belief, Antigen also anticipates and/or renders obvious the claims of the '600 patent.

101. MIMESweeper, created by Integralis Ltd. and/or Authentium, was publicly available in the United States before the conception of the '600 patent, and therefore qualifies as prior under at least 35 U.S.C. § 102(a) and (g). On information and belief, MIMESweeper also anticipates and/or renders obvious the claims of the '600 patent.

102. Specifically, claim 2 is anticipated and/or rendered obvious by at least each of the following references: Norman Firewall, TIS Firewall, Sidewinder and Cheswick alone or in combination with one another or one or more of the Background References listed below and/or the references identified in Exhibits 2-11. Barracuda notes that claim 1, from which claim 2 depends, was found to be invalid in Investigation No. 337-TA-510 in light of the Norman Firewall reference. See Final Initial Determination and Recommendation dated May 9, 2005.

103. Claims 4 and 5 are anticipated and/or rendered obvious by at least each of the following references: Norman Firewall, Intel LANProtect, TIS Firewall, Sidewinder, SMG and Gelb alone or in combination with one another or one or more of the Background References listed below and/or the references identified in Exhibits 2-11.

104. Claim 6 is anticipated and/or rendered obvious by at least each of the following references: Norman Firewall, Intel LANProtect, TIS Firewall, Sidewinder and Gelb alone or in combination with one another or one or more of the Background References listed below and/or the references identified in Exhibits 2-11.

105. Claims 7 and 8 are anticipated and/or rendered obvious by at least each of the following references: Norman Firewall, Intel LANProtect, TIS Firewall, Sidewinder, SMG and Gelb alone or in combination with one another or one or more of the Background References listed below and/or the references identified in Exhibits 2-11.

106. Claims 9 and 10 are anticipated and/or rendered obvious by at least each of the following references: Norman Firewall, TIS Firewall, Sidewinder and Cheswick alone or in combination with one another or one or more of the Background References listed below and/or the references identified in Exhibits 2-11.

107. Claims 11, 12, 14, 15, 16, and/or 17 are anticipated and rendered obvious by at least Norman Firewall, alone or in combination with the Background References listed below and/or the references identified in Exhibits 2-11. For example, combining Norman Firewall, Sidewinder, Gelb and/or the Gargoyle Firewall renders obvious claims 11, 12, 13, 14, 15, 16, and 17.

108. Claim 13 is anticipated and/or rendered obvious by at least each of the following references: Norman Firewall, TIS Firewall, Sidewinder, SMG, Cheswick and MPScan alone or in combination with one another or one or more of the Background References listed below and/or the references identified in Exhibits 2-11.

109. Claim 18 is anticipated and/or rendered obvious by at least each of the following references: Norman Firewall, Intel LANProtect, TIS Firewall, Sidewinder, SMG, Cheswick, Layland, Gelb, Gargoyle and MpScan alone or in combination with one another or one or more of the Background References listed below and/or the references identified in Exhibits 2-11.

110. Claim 19 is anticipated and/or rendered obvious by at least each of the following references: Norman Firewall, Intel LANProtect, TIS Firewall, Sidewinder and Gelb alone or in combination with one another or one or more of the Background References listed below and/or the references identified in Exhibits 2-11.

111. Claim 20 is anticipated and/or rendered obvious by at least each of the following references: Norman Firewall, Intel LANProtect, TIS Firewall, Sidewinder, SMG and Gelb

alone or in combination with one another or one or more of the Background References listed below and/or the references identified in Exhibits 2-11.

112. Claim 21 is anticipated and/or rendered obvious by at least each of the following references: Norman Firewall, Intel LANProtect, TIS Firewall, Sidewinder, SMG and Gelb alone or in combination with one another or one or more of the Background References listed below and/or the references identified in Exhibits 2-11.

113. Claim 22 is anticipated and/or rendered obvious by at least each of the following references: Norman Firewall, TIS Firewall, Sidewinder, SMG, Cheswick, Layland, Gelb, Gargoyle and MPScan alone or in combination with one another or one or more of the Background References listed below and/or the references identified in Exhibits 2-11.

114. The inventors of the '600 patent admit on the face of the patent that they did nothing more than combine familiar elements according to known methods to yield predictable results, thus rendering the '600 patent obvious. Specifically, the '600 patent explains that "those skilled in the art will realize that the information system 20 may include any number of networks 26. This information system 20 may include any number of networks, each of the networks being its own protected domain and having any number of nodes…. Each of the networks 22, 24, 26 includes a node 32 that acts as a gateway to link the respective network 22, 24, 26 to other networks 22, 24, 26." '600 patent, 1: 22-36. Thus, gateway nodes were known by those skilled in the art prior to the '600 patent. Similarly, the patent admits that "[t]he prior art has attempted to reduce the effects of viruses and prevent their proliferation by using various virus detection programs…. [A] virus detection method known as signature scanning, scans program code that is being copied onto the system. The system searches for known patterns of program code used for viruses." '600 patent, 1:58-2:11. Moreover, the '600 patent expressly directs that "[t]his is preferably done by invoking a virus-checking program on the temporarily stored file. For example, a program that performs a version of signature scanning virus detection such as PC-Cillin manufactured and sold by Trend Micro Devices Incorporated of Cupertino, Calif. may be used." '600 patent, 7:58-63. Antivirus scanning was also known to those skilled in the art long before the '600 patent.

115. The face of the patent also confirms that market forces known to those skilled in the art led to the alleged invention. The patent explains that "[d]uring the recent past, the use of computers has become widespread. Moreover, the interconnection of computers into networks has also become prevalent." '600 patent, 1:16-18. The patent goes on to explain that "[w]ith the advent of the Internet and its increased popularity, there are no prior art methods that have been able to successfully scan connections 36 such as those utilized by a gateway node in communicating with other networks." '600 patent, 1:19-22. "Therefore, there is a need for a system and method for effectively detecting and eliminating viruses without significantly effecting the performance of the computer. Moreover, there is a need for a system and method that can detect and eliminate viruses in networks attached to other information systems by way of gateways or the Internet." '600 patent, 2:30-35. This stated need was satisfied by the prior art—indeed, scanning at the gateway and doing so efficiently, were well known.

116. The prior art references identified in Exhibits 2-11 hereto and below demonstrate that each of these concepts was well known at the time of the '600 patent, such that the solution would be apparent to one of skill in the art upon stating the problem. For example, the Cheswick book explained that "a location with many PC users might wish to scan incoming files for viruses" at the "application-level gateway." BAR-TM 002851-2852. Numerous prior art references addressed these same issues, and these concepts would have been familiar to those of ordinary skill in the art. The reason or motivation to combine these references derives from the nature of the problem to be solved by the '600 patent, the prior art references themselves, including the references cited in the '600 patent, market forces at the time of the '600 patent and/or from the knowledge of one of ordinary skill in the art at the time of the purported invention of the '600 patent.

117. Though no longer required by the United States Supreme Court, Barracuda discloses the following exemplary motivations to combine prior art references to render the claims of the '600 patent obvious, as the presence of motivation to combine remains a factor in determining the obviousness of a patent.

118. Numerous references, both cited and not cited, show that there was motivation, teaching and suggestion in the field of the '600 patent to combine prior art firewall or gateway, including proxy servers and prior art virus checking software. The existence of this motivation in the field is confirmed by numerous sources including the fact that numerous systems for conducting virus scanning on data entering or leaving a network were created prior to or simultaneously with the invention claimed in the '600 patent.

119. For instance, the Hile prior art reference discloses and describes the benefit of an invention that scans for viruses in "data transfer systems" including a "network architecture":

> The computer virus problem is particularly acute in networked systems, where the opportunity for transmitting the virus from computer to computer is greatly increased. ... One major shortcoming of [desktop] virus scanning programs is that the virus may have already corrupted the data storage medium before the scanning program is used. ... The present invention solves this problem by performing an in transit detection of computer viruses using a finite state machine technique which allows multiple virus signatures to be simultaneously tested for. Because the invention is able to test for viruses "on the fly," it is useful in data communications systems and in file copying systems to inhibit the virus from entering the computer in the first place.

Hile at 1:10-62 (BAR-TM 003281-003291).

120. The Cited Japanese Application and Cited European Application likewise describe scanning for viruses at the point of entry to a computer network. Cited Japanese Application at Abstract (BAR-TM 006801-006816); Cited European Application at BAR-TM 003258-003265 (translation at BAR-TM 006600-006610).

121. The IBM Article, published in 1991 discloses "examin[ing] executable objects for computer viruses or other malicious software when the objects cross any set of domain boundaries," including "[t]he transmission of an executable object via local- or wide-area network." IBM Article at BAR-TM 002341-002342 at 002341. It recites as an implementation "[a] 'filter' in a store-and-forward network that inspects all files that pass through a given node and holds for human inspection any file that satisfies certain criteria." Id. at BAR-TM 002342. The article further describes such boundary scanning as either an addition to or a replacement for conventional desktop virus scanning. Id. at BAR-TM 002341.

122. The Layland article, published in 1994, describes the features and desirability of a yet to be invented "Internet gateway" that would intercept and process data, including email messages, going between a corporate network and the Internet. Layland at BAR-TM 002489. With regard to the threat of virus attacks, the article explains that:

> The Internet gateway would subject all incoming files to a virus scan, with any suspect file immediately discarded. The gateway would also keep a log detailing any incidence of corrupted files and the sources of those files.

Id. at BAR-TM 002489-90. The article also recognizes that the pieces of the described "Internet gateway" already existed at the time and expresses confidence that they would be combined into a commercial product. *Id*. at BAR-TM 002490.

123. As illustrated by the above references, the combination of firewalls or gateways and antivirus scanning were well known before the conception of the alleged invention. The Cheswick reference, an authoritative book on firewalls and gateways, was published in 1994. Like Layland, it describes the barrier between a network and the Internet as a fitting place to perform virus scanning. Cheswick at BAR-TM 002851-002852. This is further evidenced by products available at the time. See e.g., Exhibits 2-6, 9-11; C2C Press Release (BAR-TM 002986-002987); Rigney Article at BAR-TM 006611-006616.

124. Online discussions from 1994 also evidence the known desirability of scanning data at a gateway node for the presence of malicious code and describe how to do so. In October of 1994, Earl Boebert, who was involved with the Sidewinder system, posted on an online discussion board how to implement virus scanning in conjunction with Sidewinder and responded to skepticism from Marcus Ranum, a competitor involved with TIS Firewall, by saying "I don't view the elementary application of statistical pattern recognition to detecting object code for specific machines, followed by the customer's virus scanner of choice, to be in the class of 'hard problems.'" Boebert, W. et al., Sidewinder and Virus Scans, on-line discussion October 16, 1999, www.netsys.com (TMI_BN0014147-0014149) at 0014147-0014148; see also Ranum Declaration in Integralis v. Trend Micro litigation (TMI_BN0052141-0000143); Eng, S., "Software the Reins in 'Trojan Horses,'" Business Week (October 31, 1994) (TMI_BN0065651); Rodriguez, Karen, "Sidewinder provides

ironclad security; Firewall system used by military," InfoWorld (October 10, 1994) (TMI_BN0083122-0083123). Furthermore, Sidewinder documentation specifically references the Cheswick book which, as explained above, suggests the combination of a firewall or gateway with prior art virus scanning software. Answers to Frequently Asked Questions About Network Security, Secure Computing Corporation (1994) (BAR-TM 002541-002579) at 002577. As with Sidewinder, it was also known in the industry to use TIS Firewall with antivirus scanning software. In May of 1994, the following question was posted on a public internet bulletin board: "Does anyone know of virus-scanning software which will play on a unix (sparc-2, sunos 4.1.3) bastion host running with TIS Firewall Toolkit?". NetSys.com posting, May 27, 1994 (BAR-TM 003151-003152). In addition, the FAQ list for Gauntlet Firewall, a commercial implementation of TIS Firewall, specifically states that "virus scanning software is supported by the Gauntlet Internet Firewall." BAR-TM 005996-006004 at 005997.

125. The Dalva Article addresses security issues arising from the interface of corporate networks with the Internet. One of the potential solutions to such security issues it describes is the use of proxy filtering. A suggested use for proxy filtering is to "filter out data and programs that are known to be dangerous" which would include scanning for viruses or "known dangerous constructs." Dalva Article at BAR-TM 006124-006126 at 006126.

126. The Norman Firewall was itself the literal combination of separate firewall and antivirus scanning software. It used proxy servers and virus scanning techniques to scan data transfers for viruses at the Firewall. See generally Exhibit A. Specifically, "the Norman Firewall combines an integrated front-end server, proxy server and virus detector to defend systems and information." "Norman Data Defense Systems Unveils the Norman Firewall," PR Newswire, March 21, 1995 (BAR-TM 005071-000073) at 005071. The Norman Firewall was publicly demonstrated at the Federal Office Systems Expo (FOSE) trade show in March 1995 and was otherwise publicly available before the conception of the alleged invention claimed in the '600 patent. See e.g., id.

127. The Norman Firewall also teaches decoding and scanning email attachments for viruses and specifically uuencoded email attachments. See Exhibit A. Furthermore, both

Sidewinder and SMG teach the construction of a filter to examine email attachments for the presence of executable binary files:

> Mail—The System Administrator is able to set-up mail filtering for both inbound and outbound messages. ...the System Administrator can prohibit the mailing of messages which are not comprised of English-language plaintext. This latter form of filtering prevents users from...sending or receiving potentially dangerous, offensive, or illegal material, such as object code containing viruses....

Architecture Tech. Corp., *The LOCALNetter Newsletter*, Secure Computing Corporation and Network Security (December 1994) (BAR-TM 002580-002591) at 002588.

> Attachment file types. The filter searches the message for attached files in a variety of application specific formats. Each attached file must be of a type that is permitted to traverse the SMG. A site can use this facility to block the accidental importation of executable binary files that may contain virus software.

Smith, R., *Constructing a High Assurance Mail Guard*, Secure Computing Corp. (1994) (TMI_BN0083213-0083228) at 0083214. In addition, the Norman Firewall, the TIS Firewall and the Cheswick book teach the use of a FTP proxy server as set forth in claim 9. *See* Exhibits 2, 4, and 7.

128. Similarly, the Gelb Firewall combined a firewall at the application gateway with a commercially available virus scanning solution—Trend Micro's PC Rx. See e.g., BAR-TM 004430-004478; BAR-TM 006518-006541).

129. It would have been obvious to one of ordinary skill in the art at the time of the '600 patent, given the nature of the problem to be solved by scanning email attachments for viruses, that each email attachment, or encoded portion, would have to be stored in a temporary file, decoded and scanned. Users of uuencoding, the system for encoding files for transmission via email in popular use at the time of the invention claimed in the '600 patent, in practice only encoded a single file per email message. Consequently, uudecoders would typically be incapable of outputting more than a single file. UUencode web page printed from http://www.mcsr.olemiss.edu/cgi-bin/man-cgi?uuencode+1 (BAR-TM 002352-002353); Shelldorado, "Sending Files as Mail Attachments" (BAR-TM 006567-006571). In contrast, MIME encoding, which began to gain acceptance around the time of the invention claimed by

the ‘600 patent, was specifically designed to handle multiple attached sections and thus its decoders had to be able to output multiple files. Because stand-alone antivirus scanners have the ability to scan individual files, a person of ordinary skill in the art would simply scan the decoded file or files that the decoding algorithm produced. See e.g., Freed, N. and Borenstein, N., “Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies,” Network Working Group, Request for Comments: 2045 (November 1996) (BAR-TM 006572-006599).

130. In addition to the previous reasons to combine, it would have been obvious to a person of ordinary skill in the art to scan only certain types of files for viruses at the firewall or gateway. This combination derives from the prior art itself, the knowledge of persons of ordinary skill in the art and the nature of the problem to be solved by selectively scanning by file type. Before the conception of the invention claimed by the ‘600 patent, it was well-known among those skilled in the art that there existed a tension between the scanning speed and the accuracy/security of virus scanning software depending on whether such software scanned all files or only certain types of files for viruses. See e.g., Product Review 2: Trend’s PC Rx, Virus Bulletin (October 1992) (BAR-TM 006518-006541) at BAR-TM 006539; Cozza at 5:58-64 at BAR-TM 006554. For example, as set forth in detail below, the Norman Firewall implemented this functionality before the time of the ‘600 patent.

131. Barracuda may also rely upon one or more of the following references to show that the references identified inherently disclose “determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network” (claims 9 and 22) or that it would have been obvious to modify such references to do so: Jeffrey Mogul, “RFC 917: Internet Subnets” (Oct. 1984) (see, e.g., pages 13-14); J. Mogul & J. Postel, “RFC 950: Internet Standard Subnetting Procedure” (Aug. 1985) (see, e.g., Section 2.2); C. Hedrick, “RFC 1058: Routing Information Protocol” (June 1988) (see, e.g., page 24); E. Krol, “RFC 1118: The Hitchhikers Guide to the Internet” (Sept. 1989) (see, e.g., page 12); and T. Socolofsky & C. Kale, “RFC 1180: A TCP/IP Tutorial” (Jan. 1991) (see, e.g., Sections 5.7 and 5.8).

132. The asserted claims are invalid due to the failure of the specification to set forth the best mode known to the inventors (35 U.S.C. § 112, ¶ 1). Specifically, the specification does not disclose a method of spawning processes such that multiple processes would be pre-spawned before making a connection.

133. Claims 4 and all claims that depend from claim 4 are invalid under 35 U.S.C. § 112, ¶ 2 because they are indefinite. Claim 4 is indefinite because it recites steps that are contradictory, reciting the steps of "determining whether the data contains a virus at the sever" and "performing a preset action" on the one hand and reciting "transmitting the data . . . without performing the steps of determining whether the data contains a virus and performing a preset action . . ." on the other hand. Likewise, claim 21 is indefinite because it contains similar contradictory steps.

134. Claim 5 and all claims that depend from claim 5 are invalid under 35 U.S.C. § 112, ¶ 2 because they are not what the inventor regarded as his or her invention and invalid under 35 U.S.C. § 112, ¶ 1 because they are not supported by the written description. The specification does not disclose "storing the data in temporary file at the server after the step of electronically transmitting."

135. Claim 13 is invalid under 35 U.S.C. § 112, ¶ 2 because it is not what the inventor regarded as his invention and invalid under 35 U.S.C. § 112, ¶ 1 because it is not supported by the written description. The specification for the '600 patent describes a system that determines whether mail messages have encoded portions and only determines whether the message has a virus if it has encoded portions. In contrast, claim 13 recites checking mail messages for encoded portions and determining whether it has virus regardless of whether it has encoded portions. In the alternative, claim 13 is indefinite because the elements are contradictory and unintelligible.

136. Claim 21 is indefinite because the phrase "the steps of scanning . . ." has no antecedent basis and because the last element of claim 21 contradicts the "means for determining . . ." element in claim 18. Alternatively, claim 21 is invalid for the reasons set forth above.

137. Claims 18, 19, 21 and 22 are invalid under 35 U.S.C. § 112, ¶ 2 and ¶ 6. These claims are invalid because they recite means-plus-function elements and the specification fails to disclose and link corresponding structures to the recited elements. Alternatively, claim 21 is invalid for the reasons set forth above.

Fourth Affirmative Defense

(*Unenforceability of the '600 Patent*)

138. The '600 Patent is unenforceable as a result of the inequitable conduct attributable to the false and/or misleading statements and/or material omissions made during the prosecution of the application which ultimately issued as the '600 Patent.

139. Upon information and belief, one of the named inventors (Ms. Chen) was aware of products and product concepts that practiced the subject matter of the claims during her work with Intel Corporation, which predated the filing of the application which resulted in the '600 Patent by more than one year. Moreover, Ms. Chen failed to disclose her work on the Intel LANDesk product to the patent examiner during the prosecution of the '600 Patent.

140. Upon information and belief, the prior art Intel LANDesk Virus Protection Version 3.0, Publication Release Date 1995, was more relevant to the patentability of the subject matter of the '600 Patent than any art before the examiner in the patent file history. Ms. Chen was clearly aware of this prior art, as upon information and belief, she was directly involved with the development of the same while working with by Intel. Yet, Ms. Chen failed to disclose such art to the patent examiner. Upon information and belief, such omission was material to the decision of the United States Patent and Trademark Office to issue the '600 Patent, and but for the intentional omission of at least this material fact, the Patent Examiner would have rejected the application which matured into the '600 Patent, and the '600 Patent would not have issued. This knowing and intentional withholding of material information from the USPTO about her own prior art devices sold under the Intel LANDesk trademark renders the '600 Patent unenforceable.

Fifth Affirmative Defense

(*License*)

141. Trend Micro has licensed the '600 patent to Barracuda. Barracuda provides license agreements for its products and services. Barracuda's products and services also include software that is governed by open source licenses, including the GNU General Public License. The license agreements are shown on Barracuda's public website (see, e.g., http://www.barracudanetworks.com/ns/support/product_warranty_us_canada.php). Paragraph 6 of Barracuda's Software License Agreement reads in part: "6. LICENSE. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT YOU WILL PROVIDE AN UNLIMITED ZERO COST LICENSE TO BARRACUDA FOR ANY PATENTS OR OTHER INTELLECTUAL PROPERTY RIGHTS UTILIZED IN THE BARRACUDA SOFTWARE WHICH YOU EITHER OWN OR CONTROL." See, e.g., Trend's Complaint, Exhibit 18 at 141-152. One or more employees and agents of Trend Micro, including but not limited to James Zubb, agreed to the terms of said license agreements. Trend Micro has granted Barracuda an unlimited, free (zero cost) license to the '600 patent.

Sixth Affirmative Defense

(*Unclean Hands*)

142. Trend Micro should not be granted relief in that has unclean hands.

143. Specifically, Trend Micro made misleading and incomplete statements regarding importation by Barracuda.

144. Further, Trend Micro has requested relief based upon the alleged infringement of the '600 Patent, a patent that it knows or reasonably should know is invalid.

PRAYER FOR RELIEF

WHEREFORE, Barracuda Networks, Inc. respectfully requests that the United States International Trade Commission determine and direct:

A. That Barracuda does not violate Section 337 of the Tariff Act of 1930, as amended, by the importation into the United States, the sale for importation, and the sale within the United States after importation of certain systems for detecting and removing

viruses or worms, and components thereof, and products containing same by reason of infringement of any claim of U.S. Patent No. 5,623,600;

B. That U.S. Patent No. 5,623,600 is not infringed, is invalid and is unenforceable;

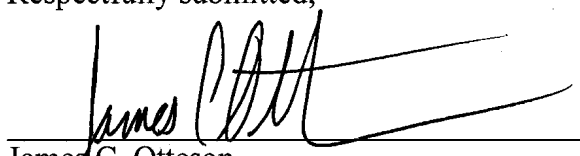
C. That it is not in the public interest to provide any relief to Complainant;

D. That the relief sought by Complainant is denied in its entirety; and

E. That Barracuda is entitled to all such other relief that the ALJ deems just and proper.

Dated: January 18, 2008

Respectfully submitted,



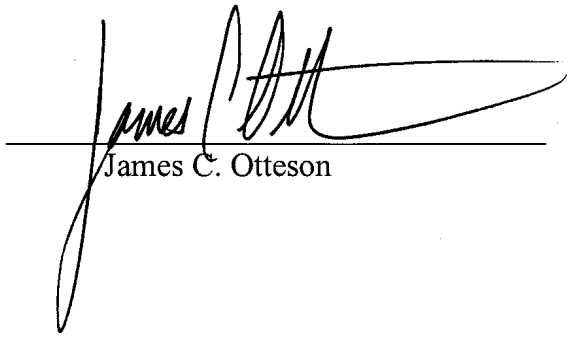
James C. Otteson
Stefani E. Shanberg
Christopher R. Parry
Matthew A. Argenti
Robin L. Brewer
WILSON SONSINI GOODRICH & ROSATI, P.C.
650 Page Mill Road
Palo Alto, CA 94304
Telephone: (650) 493-9300
Facsimile: (650) 565-5100

T.O, Kong
WILSON SONSINI GOODRICH & ROSATI
One Market, Spear Tower, Suite 3300
San Francisco, CA 94104
Telephone: (415) 947-2000
Facsimile: (415) 947-2099

Counsel for Respondents
Barracuda Networks, Inc.

VERIFICATION OF RESPONSE

Pursuant to the Rules of the United States International Trade Commission, and under penalty of perjury, I, James C. Otteson, attest that I am counsel of record for Barracuda Networks, Inc.; have read the Response submitted herewith, and verify the Response to the Complaint of Trend Micro Incorporated, *In re Certain Systems for Detecting and Removing Viruses or Worms, Components Thereof, and Products Containing Same*, in Investigation No. 337-TA-624.



James C. Otteson