IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

PACKET INTELLIGENCE LLC, **Plaintiff,** **v.** **NETSCOUT SYSTEMS, INC., TEKTRONIX COMMUNICATIONS, and TEKTRONIX TEXAS, LLC,** **Defendants.**	**Civil Action No. 2:16-cv-230** **JURY TRIAL DEMANDED**

PACKET INTELLIGENCE LLC'S COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Packet Intelligence LLC ("Packet Intelligence" or "Plaintiff"), by and through its undersigned attorneys hereby demands a jury trial and alleges the following in support of its Complaint for patent infringement against Defendants NetScout Systems, Inc., Tektronix Communications, and Tektronix Texas, LLC (collectively, "NetScout Defendants," or "Defendants"):

THE PARTIES

1. Plaintiff Packet Intelligence is a limited liability company existing under the laws of Texas with its principal place of business at 505 East Travis Street Suite 209, Marshall, TX 75670.

2. Defendant NetScout Systems, Inc. ("NetScout") is a corporation existing under the laws of Delaware, with its principal place of business at 310 Littleton Road, Westford, MA 01886-4105. The shares of NetScout Systems, Inc. are publicly traded on the NASDAQ GS Exchange under ticker symbol: NTCT. Upon information and belief, CT Corporation System, at

1999 Bryan St, Suite 900, Dallas, Texas 75201 is a registered agent of and/or is authorized to accept service of process for NetScout Systems, Inc.

3. Defendant Tektronix Communications describes itself as "a wholly owned subsidiary of NetScout Systems, Inc.," and "a NetScout Company," with its principal place of business at 3033 W. President George Bush Highway, Plano Texas 75075. Upon information and belief, Tektronix Communications can accept service of process at 3033 W. President George Bush Highway, Plano Texas 75075.

4. Defendant Tektronix Texas, LLC is a limited liability company existing under the laws of Delaware, with a principal place of business at 3033 W. President George Bush Highway, Plano Texas 75075. Upon information and belief, CT Corporation System, at 1999 Bryan St, Suite 900, Dallas, Texas 75201 is a registered agent of and/or is authorized to accept service of process for Tektronix Texas, LLC.

JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a) because this action arises under the Patent Laws of the United States, 35 U.S.C. § 1 et seq.

6. This Court has personal jurisdiction over the NetScout Defendants, who have conducted and continue to regularly conduct business within the State of Texas and within the Eastern District of Texas. The NetScout Defendants directly and/or through intermediaries (including distributors, sales agents, and others), ship, distribute, offer for sale, sell, advertise, and/or use their products (including, but not limited to, the products that are accused of patent infringement in this lawsuit) in the United States, the State of Texas, and the Eastern District of

Texas. The NetScout Defendants have committed patent infringement within the State of Texas, and, more particularly, within the Eastern District of Texas as alleged in more detail below.

7. Venue is proper in this federal district under 28 U.S.C. §§ 1391(b) and (c). On information and belief, Defendants have transacted business in this district and have committed acts of patent infringement in this district.

8. On information and belief, the NetScout Defendants have in the past, and presently continue to regularly promote, offer to sell, sell, and use infringing products and technology throughout Texas, including in and near this district. The NetScout Defendants have also sold infringing products and technology to customers for use within Texas, and within this district.

9. Defendant Tektronix Communications operates an interactive website at www.tekcomms.com that is accessible in Texas and this district. This website advertises and promotes the GeoProbe family of products and related products accused of infringement in this case. The webpages describing the GeoProbe family and related products contain hyperlinks that permit customers and/or potential customers to connect via email or request a callback with sales staff to discuss its accused products.

10. The webpages within www.tekcomms.com contain footers that include the copyright notice: "© 2016, Tektronix Communications, 3033 W President George Bush Highway, Plano, TX 75075."

11. The "Contact Us" page from the Tektronix Communications website at http://www.tekcomms.com/about-us/contact-us recites, "Tektronix Communications, 3033 President George Bush Highway Plano TX 75075" under "Head Office" and reflects this as the sole contact point for Tektronix Communications within the Americas. (*See* Exhibit 1).

12. The Tektronix Communications website includes a page identifying its Management Team, including Richard Kenedi as President of Tektronix Communications, at http://www.tekcomms.com/about-us/staff#1. (*See* Exhibit 2). Each of the five Tektronix Communications officers on the Management Team webpage has an associated "LinkedIn" webpage advertisement showing each officer presently residing in or near this judicial district.

13. Defendant NetScout operates a website at www.NetScout.com that is accessible in Texas and this district. The "Contact Us" page from this website indicates that one of NetScout's five offices in the United States is located within this district, at 6500 International Parkway, Suite 1800 Plano, TX 75093. (*See* Exhibit 3).

14. Upon information and belief, NetScout currently owns property within this district, including corporate office property located at 6504 International Parkway, #2000, Plano, Texas 75093. (*See* Exhibit 4).

15. Product literature and datasheets for the accused GeoProbe family of products are available for review and download from the Tektronix Communication website at: http://www.tekcomms.com/products/geoprobe-platform. The footers to this product literature identify the 3033 W. President George Bush Hwy address in Plano as a "NetScout" office, and state: "For more information, please visit www.netscout.com." These footers on the accused product literature state:

> Use of this product is subject to the NETSCOUT SYSTEMS, INC. ("NETSCOUT") End User License Agreement that accompanies the product at the time of shipment or, if applicable, the legal agreement executed by and between NETSCOUT and the authorized end user of this product ("Agreement"). NETSCOUT reserves the right, at its sole discretion, to make changes at any time in its technical information, specifications, service, and support programs.

(*See, e.g.,* Exhibit 5).

16. In a February 2016 Secretary of State corporate filing, Defendant Tektronix Texas, LLC lists its business address as 3033 W President George Bush HWY Plano, TX 75075, which is identical to the principal place of business for Defendant Tektronix Communications.

17. The website of Tektronix, Inc., the former parent corporation of Defendant Tektronix Texas, LLC, indicated on its website that for legal notices, the postal address of Defendant Tektronix Texas, LLC is: 3033 W. President George Bush Highway, Plano, Texas 75075. (*See* Exhibit 6).

18. Bloomberg Business prepared a "Company Overview of Tektronix Texas, LLC" that indicated Defendants Tektronix Texas, LLC and Tektronix Communications share the same President, Chief Financial Officer, and Chief Technology Officer, website, telephone number, and address at 3033 W. President George Bush Highway, Plano, Texas 75075. (*Compare* Exhibits 1, 2 and 7).

19. All of the patents asserted in this Complaint were previously asserted in a lawsuit filed in this district on March 12, 2013, in *Packet Intelligence, LLC v. Huawei Device USA Inc., et al*, Case No. 2:13-cv-00206-JRG-RSP (E.D. Tex.). The case was dismissed by agreement of the parties on March 4, 2014 (Dkts. 53 and 54).

20. All of the patents asserted in this Complaint were previously asserted in a lawsuit filed in this district on March 24, 2014, in *Packet Intelligence LLC v. Cisco Systems Inc.*, Case No. 2:14-cv-00252-JRG (E.D. Tex.). The case was dismissed by agreement of the parties on March 2, 2015 (Dkt. 106).

21. All of the patents asserted in this Complaint have also been asserted in a lawsuit filed in this district on February 17, 2016, in *Packet Intelligence LLC v. Sandvine Corporation, et al.*, Case No. 2:16-cv-00147-JRG (E.D. Tex.). The *Sandvine* case is pending.

BACKGROUND OF DEFENDANTS

22. According to industry reports, Defendant Tektronix Communications originated from Oregon-based Tektronix, Inc.'s purchase in 2004 of a Texas company called Inet Technologies. (*See* Exhibit 8). Attempts to enter Inet Technology's website (www.inet.com) are redirected to Tektronix Communications' website (www.tekcomms.com).

23. SEC filings by Inet Technologies in 2004 state that it merged with a Tektronix, Inc. subsidiary, and the newly merged subsidiary was renamed Tektronix Texas, LLC. (*See* Exhibit 9).

24. In 2007, Danaher Corporation purchased Tektronix, Inc., and with it, Tektronix Communications and Tektronix Texas, LLC.

25. On July 14, 2015, NetScout announced it completed acquisition of Danaher Corporation's communication business via a transaction valued at $2.3 billion, whereby NetScout acquired Tektronix Communications, Arbor Networks and parts of the Fluke Networks businesses, as well as VSS Monitoring. (*See* Exhibit 10). NetScout also announced: "To ensure continuity in all of our businesses, we will preserve the organization and leadership of the acquired companies as separate business units except for sales and corporate functions, which will be immediately integrated for consistency and control." (*See* Exhibit 11).

26. In NetScout's July 14, 2015 SEC filing on the acquisition closing, Tektronix Texas LLC was specifically defined as part of the "TekComms Business" that included entities recently acquired by and associated with Tektronix Communications, such as VSS Monitoring, Inc. and Newfield Wireless.

27. In connection with an $800 million credit facility through JP Morgan to help finance the 2015 acquisition of Tektronix Communications and related Danaher communication

companies (*see* Exhibit 10), NetScout on July 14, 2015, assigned security interests to JP Morgan in patents associated with its newly acquired entities. Approximately thirty days later, Tektronix Texas, LLC recorded assignments to it from Tektronix, Inc. of several patents, including patents subject to JP Morgan's security interest.

28. According to U.S. Patent and Trademark records, Tektronix Texas, LLC is the owner of the trademarked name GEOPROBE, and the owner of trademark applications filed December 16, 2015 for GEOSOFT and GEOBLADE, all three of which name Tektronix Communications products accused of infringement in this case.

29. According to its website, Tektronix Communications calls itself, "a NetScout company," and a "wholly owned subsidiary of NetScout Systems, Inc." (*See* Exhibits 2 and 12).

30. A "LinkedIn" webpage advertisement of Roger Maddox indicates he simultaneously serves as Director of Contracts at Tektronix Texas, LLC and Tektronix Communications in Plano managing the Tektronix worldwide contracts group. He further describes Tektronix Texas, LLC as "a wholly-owned subsidiary of NetScout Systems, Inc."

31. Upon information and belief, as of the filing of this complaint, no company has submitted with a Texas Secretary of State or equivalent state corporation office in Texas, a filing wherein the "registered" name of the company submitting the filing is: "Tektronix Communications."

32. Upon information and belief, Defendant Tektronix Texas, LLC has been doing business as Tektronix Communications, and/or has been and continues to be substantially involved in the operation of Tektronix Communications, including its promotion, offer to sell, sale, and use of infringing products and technology throughout Texas, including in and near this district.

THE ASSERTED PATENTS-IN-SUIT

33. On November 18, 2003, the United States Patent and Trademark Office (USPTO) duly and legally issued U.S. Patent No. 6,651,099 ("the '099 Patent") entitled "Method and Apparatus for Monitoring Traffic in a Network." Packet Intelligence owns all substantial rights to the '099 Patent, including the right to sue and recover damages for all infringement thereof. Documents assigning the '099 Patent to Packet Intelligence were recorded at the USPTO on February 1, 2013 at Reel/Frame 29737-613. Attached hereto as Exhibit 13 is a true and correct copy of the '099 Patent.

34. The '099 patent has been cited as pertinent prior art by either an applicant, or a USPTO examiner, during the prosecution of more than 275 issued patents and published patent applications, including during the prosecution of patent applications filed by Alcatel Lucent, Arbor Networks (now part of NetScout), AT&T, Broadcom, Cisco, Ericsson, F5 Networks, Fortinet, Hewlett-Packard, IBM, Intel, Juniper Networks, McAfee, Microsoft, Nokia, Samsung, Sonus Networks, Symantec, Tektronix, Verizon, VMware, and the United States of America as represented by the National Security Agency.

35. On December 16, 2003, the USPTO duly and legally issued U.S. Patent No. 6,665,725 ("the '725 Patent") entitled "Processing Protocol Specific Information in Packets Specified by a Protocol Description Language." Packet Intelligence owns all substantial rights to the '725 Patent, including the right to sue and recover damages for all infringement thereof. Documents assigning the '725 Patent to Packet Intelligence were recorded at the USPTO on February 1, 2013 at Reel/Frame 29737-613. A true and correct copy of the '725 Patent is attached hereto as Exhibit 14.

36. The ’725 patent has been cited as pertinent prior art by either an applicant, or a USPTO examiner, during the prosecution of more than 260 issued patents and published patent applications, including during the prosecution of patent applications filed by Alcatel Lucent, Amazon, AT&T, Avaya, Broadcom, Cisco, F5 Networks, Finisar, Fortinet, Fujitsu, Huawei, Hewlett-Packard, IBM, Intel, Juniper Networks, McAfee, Microsoft, Nokia, Tektronix, Sandvine, Sun Microsystems, and Symantec.

37. On August 3, 2004, the USPTO duly and legally issued U.S. Patent No. 6,771,646 (“the ’646 Patent”) entitled “Associative Cache Structure for Lookups and Updates of Flow Records in a Network Monitor.” Packet Intelligence owns all substantial rights to the ’646 Patent, including the right to sue and recover damages for all infringement thereof. Documents assigning the ’646 Patent to Packet Intelligence were recorded at the USPTO on February 1, 2013 at Reel/Frame 29737-613. A true and correct copy of the ’646 Patent is attached hereto as Exhibit 15.

38. The ’646 patent has been cited as pertinent prior art by either an applicant, or a USPTO examiner, during the prosecution of more than 170 issued patents and published patent applications, including during the prosecution of patent applications filed by AT&T, Avaya, Broadcom, Cisco, Dell, Hewlett-Packard, IBM, Intel, Juniper Networks, Lucent, McAfee, Oracle, Nokia, Nortel Networks, Sun Microsystems, Symantec, and Tektronix.

39. On January 4, 2005, the USPTO duly and legally issued U.S. Patent No. 6,839,751 (“the ’751 Patent”) entitled “Re-Using Information from Data Transactions for Maintaining Statistics in Network Monitoring.” Packet Intelligence owns all substantial rights to the ’751 Patent, including the right to sue and recover damages for all infringement thereof. Documents assigning the ’751 Patent to Packet Intelligence were recorded at the USPTO on

February 1, 2013 at Reel/Frame 29737-613. A true and correct copy of the ’751 Patent is attached hereto as Exhibit 16.

40. The ’751 patent has been cited as pertinent prior art by either an applicant, or a USPTO examiner, during the prosecution of more than 100 issued patents and published patent applications, including during the prosecution of patent applications filed by AT&T, Avaya, Ciena, Cisco, Hewlett-Packard, IBM, Intel, McAfee, Microsoft, NEC, Oracle, Nortel Networks, Sun Microsystems, and VMware.

41. On October 11, 2005, the USPTO duly and legally issued U.S. Patent No. 6,954,789 (“the ’789 Patent”) entitled “Method and Apparatus for Monitoring Traffic in a Network.” Packet Intelligence owns all substantial rights to the ’789 Patent, including the right to sue and recover damages for all infringement thereof. Documents assigning the ’789 Patent to Packet Intelligence were recorded at the USPTO on February 1, 2013 at Reel/Frame 29737-613. A true and correct copy of the ’789 Patent is attached hereto as Exhibit 17.

42. The ’789 patent has been cited as pertinent prior art by either an applicant, or a USPTO examiner, during the prosecution of more than 90 issued patents and published patent applications, including during the prosecution of patent applications filed by Alcatel Lucent, AT&T, Finisar, Fluke (now part of NetScout), Fujitsu, Georgia Tech Research Institute, Google, Hewlett-Packard, IBM, Intel, McAfee, Microsoft, and Motorola.

43. The patents-in-suit are early pioneer patents in the field of network traffic processing and monitoring. Each of the asserted patents claim priority to provisional U.S. Patent Application No. 60/141,903 entitled “Method and Apparatus for Monitoring Traffic in a Network,” filed in the United States Patent and Trademark Office on June 30, 1999.

44. As just one measure of the pioneering status of the asserted patents, collectively they have been cited as pertinent prior art by USPTO examiners and industry leading patent applicants during the prosecution of more than 900 issued patents and published patent applications filed with the USPTO. As discussed in greater detail below, all but one of the asserted patents-in-suit have been cited in Defendants' own issued patents.

45. Mr. Russell S. Dietz, the first listed inventor on four of the five patents-in-suit is a recognized thought leader who publishes and lectures regularly on network data management, cloud computing and virtualization security solutions. Bloomberg's Executive Profile for Mr. Dietz notes that he "has more than 30 years of experience in the technology and security space. He has a proven record of success as Chief Technology Officer of multiple hardware, software and systems security companies, and is a recognized pioneer and innovator in cloud computing and virtualization security solutions. . . He has more than 20 years of leadership and expertise anticipating trends, and evaluating new technologies in data communications, data management and Enterprise security. . . He is an active member of the Internet and Engineering Task Force (IETF), Optical Internetworking Forum (OIF) and the Cloud Computing Interoperability Forum (CCIF)."

46. While the applications that matured into the patents-in-suit were pending, Mr. Dietz served as the Vice President and Chief Technology Officer at Appitude, Inc. (the original assignee of the patents-in-suit), and he continued as VP and CTO at Hifn, Inc. after Hifn acquired Appitude, Inc. and the patents-in-suit. Among his other positions, Mr. Dietz currently serves as a technology consultant to Packet Intelligence.

NETSCOUT'S TECHNOLOGY AND THE MARKET FOR ITS TECHNOLOGY

47. NetScout develops, markets, and provides systems that monitor and report on the performance of software applications and the networks on which they run. Its probes – monitoring appliances that can be placed throughout a network – allow administrators to collect information about traffic flow and to optimize application and network performance. NetScout sells directly and through resellers and distributors to corporate and government customers. NetScout's technology is used by more than 90% of FORTUNE 100 companies. NetScout's U.S. sales account for about three-quarters of its total sales. Europe accounts for more than 10% of sales, while countries in Asia represent most of the rest. Generating about 50% of its revenue through indirect sales channels, NetScout primarily markets to midsized and large corporate customers, including more than 90 FORTUNE 100 companies and about 40 from the FORTUNE Global 200 list. Target industries include financial services, health care, Internet, manufacturing, retail, technology, telecommunications, and utilities.

48. Leading up to the acquisition, analysts and trade press stated that the various communication business units NetScout was acquiring from Danaher Corp. together generated revenues of around $1.2 billion, while NetScout generated $453.7 million in its financial year to March 31, 2015. These same analysts stated that NetScout had about 160 communications service provider (CSP) customers while the acquired group from Danaher had about 200 CSP customers, with very little overlap.

49. In its most recent 10Q, NetScout reported revenue for the quarter ending December 31, 2015 in excess of $307 million compared to $122 million in the quarter ending December 31, 2014. NetScout reported gross profit at $106 million for the quarter ending December 31, 2015 compared to $95 million in the quarter ending December 31, 2014.

50. Defendants' accused network control solutions typically comprise a hardware platform and proprietary software modules that are typically bundled together to provide a system for computer network operators to monitor and collect information on the data traversing their networks.

DEFENDANTS' INFRINGING PRODUCTS[1]

51. Upon information and belief, Defendants make, use, sell, offer to sell, and/or import a family of computer network platforms under the name: "GeoProbe," (i.e., GeoProbe G10, GeoBlade, and GeoSoft RAN) that are promoted and sold to operators of fixed, mobile, and Next-Gen computer networks to provide comprehensive network monitoring and data collection across legacy and next-generation technologies. More specifically, Defendants state:

> The GeoProbe family offers the best value per square inch for instrumentation technologies on the market. This enables you with reliable data collection so that you can make informed decisions on your future.
>
> **Scalable, flexible architecture**
> GeoProbe can scale with lower footprint requirements. Operators can add more processing as their needs grow. Its carriergrade, architecture allows for efficient operations and maintenance.
>
> **Vendor independence**
> Carriers can use the GeoProbe system to gain an independent view regardless of which vendor's equipment is deployed in their network. All applications are based on data captured directly from the network, as opposed to information provided in vendor specific formats.
>
> **Multitechnology and Multiservice**
> NETSCOUT is the market leader in instrumentation technology for fixed and mobile carriers. The GeoProbe platform spans technologies and services to give you the end to end view of your network that you need. The data collected by our architecture will allow

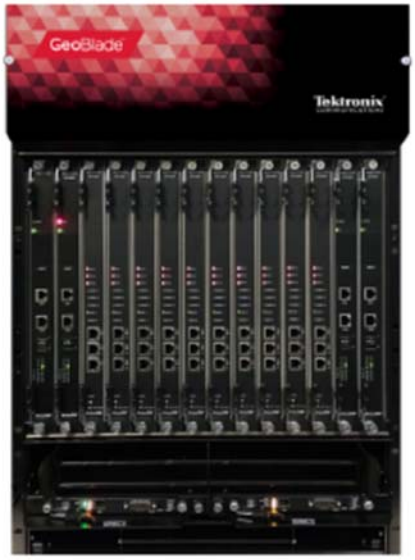
[1] Given NetScout's acquisition of Tektronix Communications and Tektronix Texas, LLC, the discussion of infringing products is intended to generally refer to the described products sold, used, offered for sale, and imported by or under the direction of all or any of the defendants in this case, even if the materials in support of this discussion originate from or refer to the name of only one of the defendants.

> you to see your customers like you have never seen them before, shedding great insight on their behavior and the quality of their interaction with your network.

(*See* Exhibit 18).

52. The GeoProbe G10 is a hardware device serving as a primary collection and correlation agent for Tektronix Communications' Network Intelligence solution. It is used to feed Iris applications (analysis and user interface software), and the G10 may be deployed in combination with existing collection and correlation agents to provide a comprehensive view of the network. (*See* Exhibit 19). Below is an image of a GeoProbe G10 hardware device.

53. Defendants characterize the GeoBlade platform as the newest member of the GeoProbe family, with new architecture spanning IP-based technologies and services with elastic software and innovative modular hardware. It leverages highly customizable configurations for the tightest control over how network data is processed by protocol and the desired granularity, and furthermore protects mission critical data with automatic load balancing. (*See* Exhibit 20). Below is an image of GeoBlades installed in a 16U (16 rack unit) chassis (called SplProbe).



54. Unlike the GeoProbe and GeoBlade hardware platforms described above, the GeoSoft RAN product is software for a virtual network monitor that extends 24x7 monitoring to the Radio Access Network ("RAN"), provides cost-effective comprehensive troubleshooting from core to RAN, regardless of equipment manufacturer, and has integrated geographical map capabilities visible through the Iris Session Analyzer and TrendNavigate applications. "From one single GUI, tools can be launched that enable you to see end to end signaling and media flows, analyze network performance, and optimize the RAN [Radio Access Network]." (*See* Exhibits 21 and 22).

55. The three GeoProbe platforms described above utilize Deep Packet Classification ("DPC") as an integral part of their core network monitoring functionality. Defendants state:

> With DPC, Tektronix Communications maximizes processing efficiency delving only as far into the packet as is needed to conclusively classify the application or protocol contained.
>
> - Supports line-rate, real-time packet classification
>
> DPC support at the monitoring point gives Iris applications immediate access to enriched classification data and enhanced data record feeds for third-party applications.

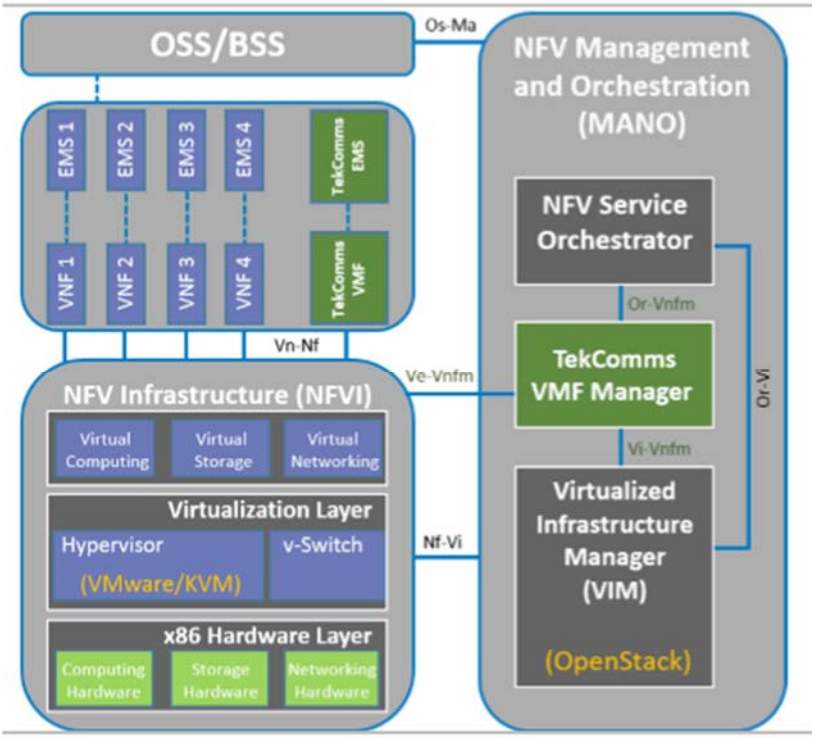
(*See* Exhibit 23).

56. The above-identified GeoProbe and GeoBlade hardware products and their associated software, including DPC, the IRIS Suite of applications, and other software associated with the GeoProbe family in the attached exhibits, as well as the GeoSoft virtual network monitor software products and its similarly associated software (again, including the IRIS applications and DPC), comprise Defendants' "**Infringing Products**."

OPERATION OF DEFENDANTS' INFRINGING PRODUCTS

57. The above section already established that the accused Geo platforms share network monitoring information with IRIS applications, such as the Iris Session Analyzer ("ISA"). (*See* Exhibit 23). Sharing Deep Packet Classification information derived from real-time packet monitoring and correlating multiple individual network sessions with each other to create complete and comprehensive conversational flows allows the ISA, among other things, to trace calls.

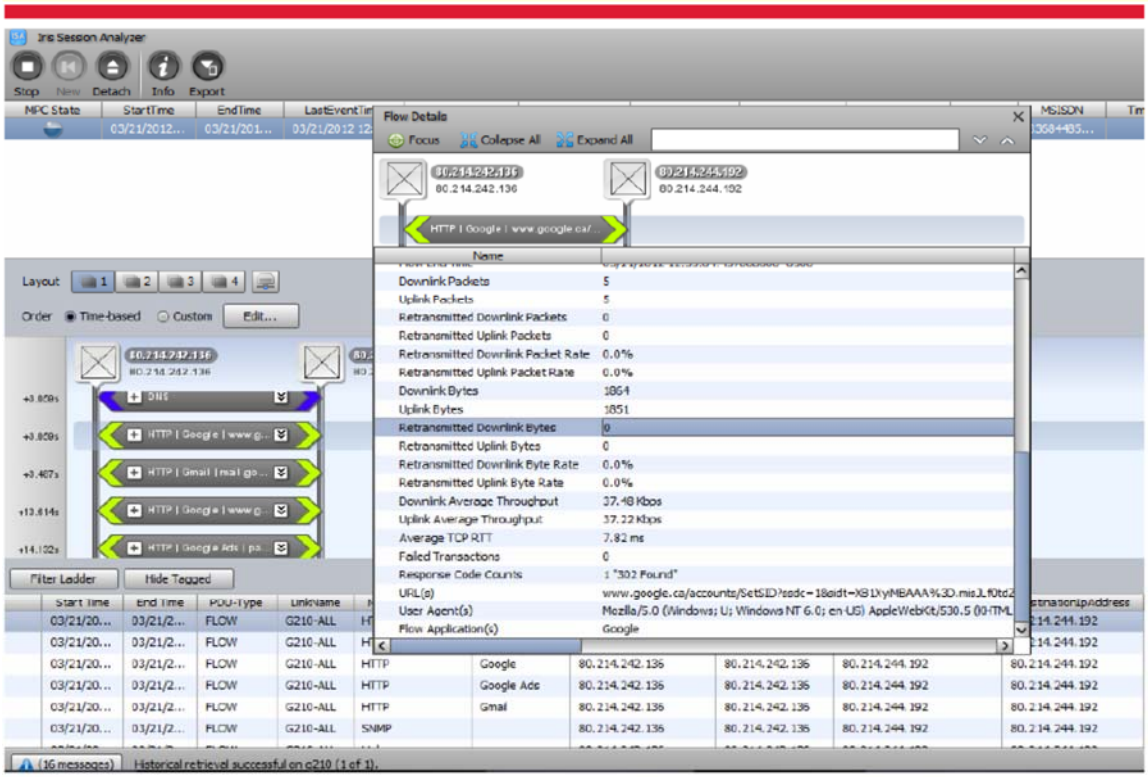
58. As shown by the two GeoProbe and GeoBlade photos above, these hardware-based devices have physical network ports that connect to a network and can act as packet acquisition devices. The GeoSoft virtual network monitor is software, and it therefore requires a host hardware device to provide similar network access through data ports or other network interface device. (*See* Exhibit 22). GeoSoft virtual devices have network interfaces provided by their host hardware servers. The graphic below shows the components of the required operating environment including "Networking Hardware" at the hardware level:



(*See* Exhibit 24).

59. The GeoBlade and GeoProbe devices are available in multiple configurations that offer 1 and 10 Gigabit GeoBlade network interface cards, or 1 and 10 Gigabit Ethernet network interface cards, respectively. (*See* "Interface Support" on page two of Exhibits 19 and 20). These network interface cards have buffer memories connected to their physical network connection ports to facilitate reception and transmission of data to and from the physical network connection point, without which the cards could not transform single bit-wide data streams used by the network into a multiple-bit wide (typically 64 bits) format used internally in computing devices.

60. Defendants' product literature on their Deep Packet Classification ("DPC") technology contains the figure below, which is a flow table entry from an Iris Session Analyzer using DPC data. (*See* Exhibit 23).



When enriched with DPC results, Iris Session Analyzer can provide powerful insights into session level behaviour and performance. Each flow presented by Iris Session Analyzer can be examined and the DPC tagging directly viewed.

61. The central rectangle named “Flow Details” in the above figure shows partial data stored in a flow-entry record, most likely from the record corresponding to the bolded line in the table with columns named “Start Time” and “End Time,” behind and partially below the “Flow Details.” The collection of flow records within the table with “Start Time” and “End Time” columns constitutes a partial list of other flows stored in a flow-entry database and which encountered the accused network monitor. (See Exhibit 23). The partial data disclosed in the “Flow Details” in the above figure, together with other product literature by defendants, indicate that the accused network monitors utilize a combination of IP addresses of the devices that are communicating, their port numbers, and the network layer protocol, to create so-called “5-Tuple” information to identify flows and parse/extract from a packet to identify whether a packet is part

of a conversational-flow sequence. (See Exhibits 23 and 25). It is regular industry practice to form a function of this 5-Tuple information (a hash), because the packets are examined in real time and hash functions greatly reduce look-up times, and the hash functions suffice to identify whether a packet is part of a conversational-flow sequence.

62. The Infringing Products use a lookup engine to compare the 5-Tuple information (in its hashed key format) of a newly arriving packet with the flow-entry key (5-Tuple information) associated with the flow-entry in the flow-entry database memory. If the identifying flow-entry key of the packet matches an entry in the flow-entry database, the lookup engine returns a match and identifies the packet as belonging to the conversational flow-entry. In the image in paragraph 60 above, the centrally positioned “Flow Details" show that 5 packets in each direction were matched with this particular flow-entry using the above-described lookup engine functionality.

63. Defendants’ product literature on Deep Packet Classification (“DPC”) further states:

> Through an innovative partnership with a leading DPI provider, Tektronix Communications' DPC capabilities offer support for over 2000 applications and protocols.
>
> - Ongoing discovery and classification of new applications is easily incorporated with the routine availability of signature “plug-ins”.
> - For out of process classification needs, Tektronix Communications offers manual GUI signature entry for rapid, customized classification response.
>
> Aggressive coverage (volume of traffic) and accuracy (correct classification) targets keep data integrity at the forefront to maximize the value of supported use cases and implementations.

(*See* Exhibit 23).

64. Defendants’ Deep Packet Classification uses the above-identified “signature plug-ins,” which are a set of predefined state patterns and state operations. The Infringing Products

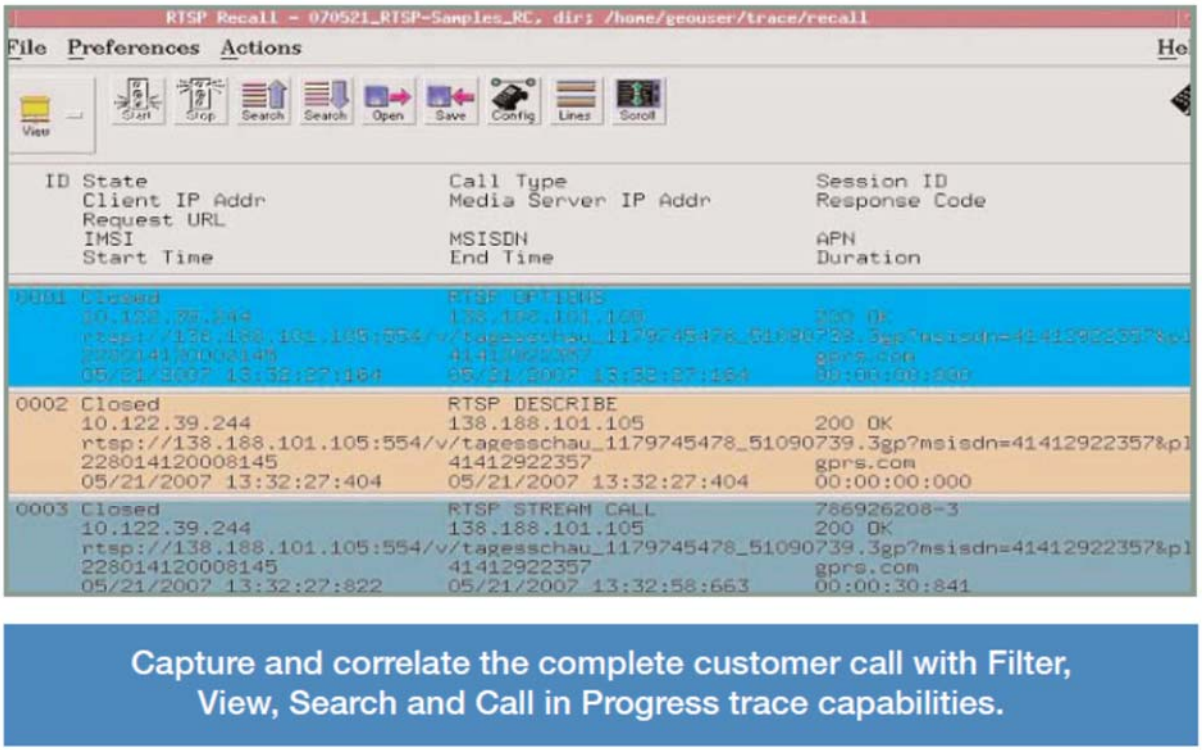
apply these state pattern operations based on the last known state of the flow. As a result, traversing a particular transition pattern as part of a particular flow-sequence of packets will ultimately indicate that the flow-sequence is associated with a particular application program.

65. The infringing products have a protocol/state identification mechanism that is coupled to the state patterns/operations memory (where the "signature plug-ins" are stored) and to the lookup engine. The protocol/state identification mechanism "delves into the packet only as far as is needed" to perform the operations provided by the "signature plug-ins" to "conclusively classify the application or protocol contained." (*See* Exhibit 23). In the instance of the Figure in paragraph 60 with the "Flow Details," the protocol/state identification mechanism had determined, using the signature plug-ins (state machine patterns) that Google is the "Flow Application."

66. If the current state of the flow as recorded in the flow-entry database indicates that state transition patterns need to be applied to identify the application (protocol), then the packet will be processed by the DPC (Deep Packet Classification) engine which is coupled to the signature-plugins database that contains one or more predefined state operations to be performed on the current packet of the flow. Because it is possible for applications to require more than a single packet to be completely identified such that it will have no further state transitions, the DPC engine applies the next state machine transition (signature-plugin) that follows from the last state recorded for the conversational flow. (*See* Exhibit 23).

67. The Infringing Products have a parsing/extractions memory that contains information describing how to determine at least one of the protocols used in a packet from data in the packet. For instance, the products are configured to analyze RTSP (Real Time Streaming Protocol) sessions. RTSP is an application layer protocol that is used for delivery of multimedia

content (audio-video for instance) across IP networks (like the networks of mobile network operators). RTSP is a child protocol of TCP (meaning that the Layer 4 transport protocol TCP can include in its data portion the RTSP protocol and its data unit). Therefore, RTSP control sessions are encapsulated within TCP sessions. For actual content streaming, the RTP protocol uses UDP instead of TCP as the transport layer protocol. RTCP, which is used to communicate quality and other information bi-directionally is also a UDP, not a TCP-based protocol. For a multi-media stream (containing separate streams for sound and video for instance), a plurality of connections between the server and the client are established to setup, control, and provide the data stream(s). The Infringing Products have a parsing/extraction operations memory that is configured to parse/extract at least one protocol used in a packet from data in the packet. In the example above, the TCP protocol (as well as the UDP protocol) is a transport layer protocol. Because the Infringing Products support the RTSP protocol, they also support the TCP protocol and they have a memory that contains instructions on how to determine that an IP packet contains TCP data and within the TCP portion information to determine that the RTSP protocol is contained. (See Exhibit 25 and the figure immediately below, taken therefrom.)



Capture and correlate the complete customer call with Filter, View, Search and Call in Progress trace capabilities.

INFRINGEMENT OF U.S. PATENT NO. 6,651,099

68. Packet Intelligence realleges paragraphs 1 through 67 as though fully set forth herein.

69. Each Defendant has infringed directly and continues to infringe directly at least claim 1 of the ’099 Patent by its manufacture, sale, offer for sale, and use of any one or more of the Infringing Products. Each Defendant is therefore liable for infringement of the ’099 Patent pursuant to 35 U.S.C. § 271.

70. Arbor Networks, Inc. (which is now part of NetScout), first learned of the ’099 Patent no later than on or around June 16, 2004, when the U.S. Patent & Trademark Office mailed a Patent Examiner’s citation to the ’099 Patent during prosecution of Arbor Networks, Inc.’s U.S. patent application 09/706,503 (“the ’503 application”). Packet Intelligence’s ’099 Patent is therefore listed as a prior art reference on the opening pages of Arbor Networks, Inc.’s

patent 7,790,886 that issued from the ’503 application on June 28, 2011, and in which NetScout assigned a security interest to JPMorgan on July 14, 2015.

71. As of the time each Defendant first had notice of the ’099 Patent, whether through prior notice or through this complaint, each Defendant indirectly infringed and continues to indirectly infringe at least claim 1 of the ’099 Patent by active inducement under 35 U.S.C. § 271(b). Each Defendant has induced, caused, urged, encouraged, aided and abetted its direct and indirect customers to make, use, sell, offer for sale and/or import the Infringing Products, and thus indirectly infringes at least claim 1 of the ’099 Patent. Each Defendant has done so by acts including but not limited to selling such products including features that—when used or resold—infringe the ’099 Patent; and by marketing the infringing capabilities of such products; and by providing instructions, technical support, and other support and encouragement for the use of such products. Such conduct by each Defendant was intended to and actually did result in direct infringement by Defendants’ direct and indirect customers, including the making, using, selling, offering for sale and/or importation of the Infringing Products in the United States.

72. As of the time each Defendant first had notice of the ’099 Patent, whether through prior notice or through this complaint, each Defendant is a contributory infringer of at least claim 1 of the ’099 Patent under 35 U.S.C. § 271(c). Each Defendant offers to sell and sells components, materials, or apparatuses with or as part of its Infringing Products that are specially made or adapted to examine packets passing through a connection point on a computer network in the manner claimed in at least claim 1 of the ’099 Patent. The components, materials, or apparatuses provided by each Defendant with its Infringing Products constitute a material part of the invention claimed within the ’099 Patent, are not staple articles, and have no substantial use that does not infringe the ’099 Patent.

73. Defendants' infringement of the '099 Patent has damaged Packet Intelligence, and Each Defendant is liable to Packet Intelligence in an amount to be determined at trial that compensates Packet Intelligence for the infringement, which by law can be no less than a reasonable royalty.

74. As a result of Defendants' infringement of the '099 Patent, Packet Intelligence has suffered irreparable harm and will continue to suffer loss and injury unless each Defendant is enjoined by this Court.

75. As of the time each Defendant first had notice of the '099 Patent, each Defendant has continued with its infringement despite the objectively high likelihood that its actions constitute infringement and Defendant's subjective knowledge of this obvious risk. As each Defendant has no good faith belief that it does not infringe the '099 Patent, each Defendant's infringement of the '099 Patent is willful and deliberate, entitling Packet Intelligence to increased damages under 35 U.S.C. § 284 and to attorneys' fees and costs incurred in prosecuting this action under 35 U.S.C. § 285.

INFRINGEMENT OF U.S. PATENT NO. 6,665,725

76. Packet Intelligence realleges paragraphs 1 through 67 as though fully set forth herein.

77. Each Defendant has infringed directly and continues to infringe directly at least claim 17 of the '725 Patent by its manufacture, sale, offer for sale, and use of any one or more of the Infringing Products. Each Defendant is therefore liable for infringement of the '725 Patent pursuant to 35 U.S.C. § 271.

78. Tektronix Texas, LLC (which is also now part of NetScout), first learned of the '725 Patent no later than on or around December 15, 2004, when the U.S. Patent & Trademark

Office mailed a Patent Examiner's citation to the '725 Patent during prosecution of Tektronix's U.S. patent application 09/832,416 ("the '416 application"). Packet Intelligence's '725 Patent is therefore listed as a prior art reference on the face of Tektronix Texas, LLC's patent 7,466,718 that issued from the '416 application on December 16, 2008, and in which NetScout assigned a security interest to JPMorgan on July 14, 2015.

79. As of the time each Defendant first had notice of the '725 Patent, whether through prior notice or through this complaint, each Defendant indirectly infringed and continues to indirectly infringe at least claim 17 of the '725 Patent by active inducement under 35 U.S.C. § 271(b). Each Defendant has induced, caused, urged, encouraged, aided and abetted its direct and indirect customers to make, use, sell, offer for sale and/or import the Infringing Products, and thus indirectly infringes at least claim 17 of the '725 Patent. Each Defendant has done so by acts including but not limited to selling such products including features that—when used—infringe the '725 Patent; marketing the infringing capabilities of such products; and providing instructions, technical support, and other support and encouragement for the use of such products. Such conduct by each Defendant was intended to and actually did result in direct infringement by NetScout's direct and indirect customers, including the making, using, selling, offering for sale and/or importation of Infringing Products in the United States.

80. As of the time each Defendant first had notice of the '725 Patent, whether through prior notice or through this complaint, each Defendant was a contributory infringer of at least claim 17 of the '725 Patent under 35 U.S.C. § 271(c). Each Defendant offers to sell and sells components, materials, or apparatuses with or as part of its Infringing Products that are specially made or adapted to perform protocol specific operations on a packet passing through a connection point on a computer network in the manner claimed in at least claim 17 of the '725

Patent. The components, materials, or apparatuses provided by each Defendant with its Infringing Products constitute a material part of the invention claimed within the ’725 Patent, are not staple articles, and have no substantial use that does not infringe the ‘725 Patent.

81. Defendants’ infringement of the ’725 Patent has damaged Packet Intelligence, and each Defendant is liable to Packet Intelligence in an amount to be determined at trial that compensates Packet Intelligence for the infringement, which by law can be no less than a reasonable royalty.

82. As a result of Defendants’ infringement of the ’725 Patent, Packet Intelligence has suffered irreparable harm and will continue to suffer loss and injury unless each Defendant is enjoined by this Court.

83. As of the time each Defendant first had notice of the ’725 Patent, each Defendant continued with its infringement despite the objectively high likelihood that its actions constitute infringement and its subjective knowledge of this obvious risk. As each Defendant had no good faith belief that it does not infringe the ’725 Patent, Defendants’ infringement of the ’725 Patent is willful and deliberate, entitling Packet Intelligence to increased damages under 35 U.S.C. § 284 and to attorneys’ fees and costs incurred in prosecuting this action under 35 U.S.C. § 285.

INFRINGEMENT OF U.S. PATENT NO. 6,771,646

84. Packet Intelligence realleges paragraphs 1 through 67 as though fully set forth herein.

85. Each Defendant has infringed directly and continues to infringe directly at least claim 7 of the ’646 Patent by its manufacture, sale, offer for sale, and use of any one or more of Defendants’ Infringing Products. Each Defendant is thus liable for infringement of the ’646 Patent pursuant to 35 U.S.C. § 271.

86. Tektronix Texas, LLC (which is also now part of NetScout), first learned of the '646 Patent no later than on or around January 12, 2011, when the U.S. Patent & Trademark Office mailed a Patent Examiner's citation to the '646 Patent during prosecution of Tektronix's U.S. patent application 12/043,105 ("the '105 application"). Packet Intelligence's '646 Patent is therefore listed as a prior art reference on the face of Tektronix Texas, LLC's patent 8,254,939 that issued from the '105 application on August 28, 2012, and in which NetScout assigned a security interest to JPMorgan on July 14, 2015.

87. As of the time each Defendant first had notice of the '646 Patent, whether through prior notice or through this complaint, each Defendant indirectly infringed and continues to indirectly infringe at least claim 7 of the '646 Patent by active inducement under 35 U.S.C. § 271(b). Each Defendant has induced, caused, urged, encouraged, aided and abetted its direct and indirect customers to make, use, sell, offer for sale and/or import the Infringing Products, and thus indirectly infringes at least claim 7 of the '646 Patent. Each Defendant has done so by acts including but not limited to selling such products including features that—when used or resold—infringe at least claim 7 of the '646 Patent; marketing the infringing capabilities of such products; and providing instructions, technical support, and other support and encouragement for the use of such products. Such conduct by each Defendant was intended to and actually did result in direct infringement by its direct and indirect customers, including the making, using, selling, offering for sale and/or importation of Infringing Products in the United States.

88. When each Defendant first had notice of the '646 Patent, whether through prior notice or through this complaint, each Defendant was a contributory infringer of at least claim 7 of the '646 Patent under 35 U.S.C. § 271(c). Each Defendant offers to sell and sells components, materials, or apparatuses with or as part of its Infringing Products that are specially made or

adapted to examine packets passing through a connection point on a computer network in the manner claimed in at least claim 7 of the ’646 Patent. The components, materials, or apparatuses provided by each Defendant with its Infringing Products constitute a material part of the invention claimed within the ’646 Patent, are not staple articles, and have no substantial use that does not infringe the ’646 Patent.

89. Defendants’ infringement of the ’646 Patent has damaged Packet Intelligence, and each Defendant is liable to Packet Intelligence in an amount to be determined at trial that compensates Packet Intelligence for the infringement, which by law can be no less than a reasonable royalty.

90. As a result of Defendants’ infringement of the ’646 Patent, Packet Intelligence has suffered irreparable harm and will continue to suffer loss and injury unless each Defendant is enjoined by this Court.

91. As of the time each Defendant first had notice of the ’646 Patent, each Defendant has continued with its infringement despite the objectively high likelihood that its actions constitute infringement and Defendant’s subjective knowledge of this obvious risk. As each Defendant has no good faith belief that it does not infringe the ’646 Patent, its infringement of the ’646 Patent is willful and deliberate, entitling Packet Intelligence to increased damages under 35 U.S.C. § 284 and to attorneys’ fees and costs incurred in prosecuting this action under 35 U.S.C. § 285.

INFRINGEMENT OF U.S. PATENT NO. 6,839,751

92. Packet Intelligence realleges paragraphs 1 through 67 as though fully set forth herein.

93. Each Defendant has infringed directly and continues to infringe directly at least claim 17 of the ’751 Patent by its manufacture, sale, offer for sale, and use of network components that include or use at least any one or more of the Infringing Products. Each Defendant is thus liable for infringement of the ’751 Patent pursuant to 35 U.S.C. § 271.

94. As of the time each Defendant first had notice of the ’751 Patent, which is no later than the filing date of this complaint, each Defendant indirectly infringed and continues to indirectly infringe at least claim 17 of the ’751 Patent by active inducement under 35 U.S.C. § 271(b). Each Defendant has induced, caused, urged, encouraged, aided and abetted its direct and indirect customers to make, use, sell, offer for sale and/or import the Infringing Products, and thus indirectly infringes at least claim 17 of the ’751 patent. Each Defendant has done so by acts including but not limited to selling such products including features that—when used or resold—infringe at least claim 17 the ’751 Patent; marketing the infringing capabilities of such products; and providing instructions, technical support, and other support and encouragement for the use of such products. Such conduct by each Defendant was intended to and actually did result in direct infringement by Defendants’ direct and indirect customers, including the making, using, selling, offering for sale and/or importation of Infringing Products in the United States.

95. When each Defendant first had notice of the ’751 Patent, which is no later than the filing date of this complaint, each Defendant was a contributory infringer of at least claim 17 of the ’751 Patent under 35 U.S.C. § 271(c). Each Defendant offers to sell and sells components, materials, or apparatuses with or as part of its Infringing Products that are specially made or adapted to examine packets passing through a connection point on a computer network in the manner claimed in at least claim 17 of the ’751 Patent. The components, materials, or apparatuses provided by each Defendant with its Infringing Products constitute a material part of

the invention claimed within the ’751 Patent, are not staple articles, and have no substantial use that does not infringe the ’751 Patent.

96. Defendants’ infringement of the ’751 Patent has damaged Packet Intelligence, and each Defendant is liable to Packet Intelligence in an amount to be determined at trial that compensates Packet Intelligence for the infringement, which by law can be no less than a reasonable royalty.

97. As a result of Defendants’ infringement of the ’751 Patent, Packet Intelligence has suffered irreparable harm and will continue to suffer loss and injury unless each Defendant is enjoined by this Court.

98. As of the time each Defendant first had notice of the ’751 Patent, which is no later than the filing date of this complaint, each Defendant has continued with its infringement despite the objectively high likelihood that its actions constitute infringement and Defendants’ subjective knowledge of this obvious risk. As each Defendant has no good faith belief that it does not infringe the ’751 Patent, each Defendant’s infringement of the ’751 Patent is willful and deliberate, entitling Packet Intelligence to increased damages under 35 U.S.C. § 284 and to attorneys’ fees and costs incurred in prosecuting this action under 35 U.S.C. § 285.

INFRINGEMENT OF U.S. PATENT NO. 6,954,789

99. Packet Intelligence realleges paragraphs 1 through 67 as though fully set forth herein.

100. Each Defendant has infringed directly and continues to infringe directly at least claim 19 of the ’789 Patent by its manufacture, sale, offer for sale, and use of network components that include or use at least any one or more of the Infringing Products. Each Defendant is thus liable for infringement of the ’789 Patent pursuant to 35 U.S.C. § 271.

101. A unit of Fluke Corporation (that is now part of NetScout), first learned of the '789 Patent no later than on or around July 20, 2009, when the U.S. Patent & Trademark Office mailed a Patent Examiner's citation to the '789 Patent during prosecution of Fluke's U.S. patent application 11/477,868 ("the '868 application"). Packet Intelligence's '789 Patent is therefore listed as a prior art reference on the opening pages of Fluke patent 7,804,787 that issued from the '868 application on September 28, 2010, and in which NetScout assigned a security interest to JPMorgan on July 14, 2015.

102. As of the time each Defendant first had notice of the '789 Patent, whether through prior notice or through this complaint, each Defendant indirectly infringed and continues to indirectly infringe at least claim 19 of the '789 Patent by active inducement under 35 U.S.C. § 271(b). Each Defendant has induced, caused, urged, encouraged, aided and abetted its direct and indirect customers to make, use, sell, offer for sale and/or import the Infringing Products. Each Defendant has done so by acts including but not limited to selling such products including features that—when used or resold—infringe at least claim 19 of the '789 Patent; marketing the infringing capabilities of such products; and providing instructions, technical support, and other support and encouragement for the use of such products. Such conduct by each Defendant was intended to and actually did result in direct infringement by Defendants' direct and indirect customers, including the making, using, selling, offering for sale and/or importation of Infringing Products in the United States.

103. As of the time each Defendant first had notice of the '789 Patent, whether through prior notice or through this complaint, each Defendant was a contributory infringer of at least claim 19 of the '789 Patent under 35 U.S.C. § 271(c). Each Defendant offers to sell and sells components, materials, or apparatuses with or as part of its Infringing Products that are specially

made or adapted to examine packets passing through a connection point on a computer network in the manner claimed in at least claim 19 of the ’789 Patent. The components, materials, or apparatuses provided by each Defendant with its Infringing Products constitute a material part of the invention claimed within the ’789 Patent, are not staple articles, and have no substantial use that does not infringe the ’789 Patent.

104. Defendants’ infringement of the ’789 Patent has damaged Packet Intelligence, and each Defendant is liable to Packet Intelligence in an amount to be determined at trial that compensates Packet Intelligence for the infringement, which by law can be no less than a reasonable royalty.

105. As a result of Defendants’ infringement of the ’789 Patent, Packet Intelligence has suffered irreparable harm and will continue to suffer loss and injury unless each Defendant is enjoined by this Court.

106. As of the time each Defendant first had notice of the ’789 Patent, each Defendant has continued with its infringement despite the objectively high likelihood that its actions constitute infringement and its subjective knowledge of this obvious risk. As each Defendant has no good faith belief that it does not infringe the ’789 Patent, its infringement of the ’789 Patent is willful and deliberate, entitling Packet Intelligence to increased damages under 35 U.S.C. § 284 and to attorneys’ fees and costs incurred in prosecuting this action under 35 U.S.C. § 285.

DEMAND FOR JURY TRIAL

107. Plaintiff Packet Intelligence demands a trial by jury on all issues so triable, pursuant to Rule 38 of the Federal Rules of Civil Procedure.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Packet Intelligence prays for the following relief:

A. A judgment in favor of Packet Intelligence that the NetScout Defendants have infringed and are infringing the ’099, ’725, ’646, ’751, and ’789 Patents;

B. An Order permanently enjoining the NetScout Defendants, their respective officers, agents, employees, and those acting in privity with it, from further direct and/or indirect infringement of the ’099, ’725, ’646, ’751, and ’789 Patents;

C. An award of damages to Packet Intelligence arising out of the NetScout Defendants’ infringement of the ’099, ’725, ’646, ’751, and ’789 Patents, including enhanced damages pursuant to 35 U.S.C. § 284, together with prejudgment and post-judgment interest, in an amount to be determined at trial;

D. An award of an ongoing royalty for the NetScout Defendants’ post-judgment infringement in an amount to be determined at trial;

E. A judgment declaring this case exceptional under 35 U.S.C. § 285 and awarding Packet Intelligence its attorneys’ fees with prejudgment and post-judgment interest; and

F. Granting Packet Intelligence its costs and any further relief as the Court may deem just and proper.

Date: March 15, 2016

Respectfully submitted:

/s/ Paul J. Skiermont
Paul J. Skiermont
Texas SB # 24033073
Sarah E. Spires
Texas SB # 24083860
Steven W. Hartsell
Texas SB # 24040199
Steve Udick
Texas SB # 24079884
SKIERMONT DERBY LLP
2200 Ross Avenue, Suite 4800W
Dallas, Texas 75201
(214) 978-6600 (telephone)
(214) 978-6601 (facsimile)
pskiermont@skiermontderby.com
sspires@skiermontderby.com
shartsell@skiermontderby.com
sudick@skiermontderby.com

Attorneys for Packet Intelligence LLC