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

PACKET INTELLIGENCE LLC, Plaintiff, vs. NOKIA SOLUTIONS AND NETWORKS US LLC, Defendant.	CASE NO.: 2:18-cv-382 **JURY TRIAL DEMANDED**

PACKET INTELLIGENCE LLC'S COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Packet Intelligence LLC, by and through its undersigned attorneys hereby demands a jury trial and alleges the following in support of its Complaint for patent infringement against Defendant Nokia Solutions and Networks US LLC:

I. THE PARTIES

1. Plaintiff Packet Intelligence LLC ("Packet Intelligence" or "Plaintiff") is a limited liability company existing under the laws of Texas since June 2012. Plaintiff maintains its principal place of business at 505 East Travis Street Suite 209, Marshall, TX 75670.

2. Defendant Nokia Solutions and Networks US LLC ("Nokia" or "Defendant") is a limited liability company organized and existing under the laws of Delaware, with a principal place of business at 6000 Connection Drive, Irving, Texas 75039. Nokia may be served with process by serving Corporation Service Company d/b/a CSC-Lawyers Incorporating Service Company at 211 E. 7th Street, Suite 620, Austin, TX 78701.

II. JURISDICTION AND VENUE

3. This is an action for infringement of several United States patents. Federal question jurisdiction is conferred to this Court over such action under 28 U.S.C. §§ 1331 and 1338(a).

4. Defendant maintains a regular and established place of business within the Eastern District of Texas at 601 Data Drive, Plano, Texas 75075. Defendant develops and/or sells the Accused Products, identified below, from this location.

5. Defendant has sufficient minimum contacts with the Eastern District of Texas such that this venue is fair and reasonable. Defendant has committed such purposeful acts and/or transactions in this District that it reasonably should know and expect that they could be hailed into this Court as a consequence of such activities. Defendant has transacted and, at the time of the filing of this Complaint, continues to transact business within the Eastern District of Texas.

6. Further, Defendant makes or sells products that are and have been used, offered for sale, sold, and/or purchased in the Eastern District of Texas. Defendant directly and/or through its distribution network, places infringing products or systems within the stream of commerce, which stream is directed at this district, with the knowledge and/or understanding that those products will be sold and/or used in the Eastern District of Texas.

7. For these reasons, personal jurisdiction exists and venue is proper in this Court under 28 U.S.C. §§ 1391(b) and (c) and 28 U.S.C. § 1400(b), respectively.

III. THE PATENTS-IN-SUIT

8. 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.

9. 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)." Russel S. Dietz: Executive Profile & Biography – Bloomberg, https://www.bloomberg.com/research/stocks/private/person.asp?personId=510317&privcapId=1354032 (visited July 27, 2018).

10. 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 A is a true and correct copy of the '099 Patent.

11. 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 one patent application of Nokia Corp., the parent entity of Defendant.

12. 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 B.

13. 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 one patent assigned to Nokia Siemens Networks Oy.

14. 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 C.

15. 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.

16. 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 D.

17. 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.

18. 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 E.

19. 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.

20. Some or all of the '099, '725, '646, '751, and '789 Patents (referred to collectively as the "Asserted Patents" or the "Patents-in-Suit") have been asserted in several patent infringement litigations in this District. During the course of these District court litigations, claims of the Asserted Patents have withstood multiple validity challenges. The outcomes of those cases are indicative of the strength of the Asserted Patents. The following cases have been litigated in this District:

- *Packet Intelligence LLC v. Huawei Devices USA Inc.*, Civil Action No. 2:13-cv-00206-JRG (dismissed by stipulation of parties pursuant to settlement agreement);
- *Packet Intelligence LLC v. Cisco Systems, Inc.*, Civil Action No. 2:14-cv-00252-JRG (dismissed by agreed motion and order following settlement);
- *Packet Intelligence LLC v. Cisco Systems, Inc.*, Civil Action No. 2:14-cv-01122-JRG (consolidated with Civil Action No. 2:14-cv-00252-JRG);
- *Packet Intelligence LLC v. NetScout Systems, Inc. et al*, Civil Action No. 2:16-cv-00230-JRG (resulting in a jury verdict finding infringement of the asserted claims of the '725, '751, and '789 Patents and upholding validity of the same (Dkt. No. 237 at 3-4); applying the constructions entered in the Court's Claim Construction Order (Dkt. No. 66) and denying Defendant's Rule 52 motion challenging the validity of claims of the '725, '751, and '789 Patents under 35 U.S.C. 101 (Dkt. No. 298)); and,
- *Packet Intelligence LLC v. Sandvine Corporation and Sandvine Incorporated ULC*, Civil Action No. 2:16-cv-00147-JRG (resulting in a jury verdict of non-infringement of the asserted claims of the '725, '751, and '789 Patents; validity did not make it to the jury following denial of institution of Sandvine's Petitions for *inter partes* review

of the Asserted Patents and the Court's grant of Motion *in Limine* No. 4 (Dkt. No. 22)).

21. The validity of the asserted claims has been repeatedly upheld by the Patent Trial and Appeal Board ("the Board") through its denial of institution of six Petitions for *inter partes* review filed by defendants in the prior litigations. Institution was denied in each of these IPRs because the Board found that the respective Petitions did not establish a reasonable likelihood of success in invalidating the challenged claims, comprising several of which are now asserted in the present litigation. Requests for rehearing were similarly rejected by the Board.

22. Nokia has been aware of the status of these litigations and IPRs and of the existence and subject matter of the Asserted Patents since at least December 7, 2017, at which time Packet Intelligence responded to an electronic mail correspondence from Nokia's Senior IPR Licensing / Litigation Counsel requesting information about the Asserted Patents.

IV. BACKGROUND AND FACTS

23. The Asserted Patents are generally directed to systems and methods for classifying and monitoring network traffic as well as the use of state operations and state-of-the-flow analysis to accommodate classification and monitoring of network traffic. These innovative concepts enable classification of data packets passing through a network to provide detailed insight and information to network managers and operators. More specifically, the Asserted Patents disclose and claim improved techniques for monitoring network traffic through, among other things, categorizing network traffic into "conversational flows" – relating sequences of data packets exchanged in any direction over a network comprising multiple connections among network devices, which may be client or server devices, based on specific application activity. This was an improvement over conventional systems and methods for

classifying and monitoring network traffic based only on "connection flows" – data packets transmitted over a single network connection.

24. Traffic classification involves detecting the underlying protocols used within a data packet, as well as the applications or user activity responsible for generating network traffic. It also involves identifying the underlying protocols/applications of a flow along with recording traffic statistics. Such classification and monitoring provide network administrators with detailed information about their networks, which can be used to diagnose network problems, control bandwidth allocation, and ensure an appropriate quality of service for users.

25. Conventional network monitors categorized network transmissions into "connection flows." A connection flow refers to the packets involved in a single connection and relate to a negotiated transmission between specific addresses on two devices. A connection flow correlates to the source and destination IP address/port pairs used on both ends of the connection without inspecting the packet's payload deeper than the headers of the transport layer[1] containing port information. The problem with only tracking connection flows is that certain applications and protocols may generate multiple connections. In other words, a single application may spawn multiple connections for a single activity. For example, if user A wants to have a Skype call with user B, the Skype application may create multiple connections between computer A and B to conduct the call. There might be one connection which supplies setup information, a second connection for transmitting video information, and a third connection for transmitting audio information. Conventional network monitors would consider these three separate connections even though they originated from a single Skype call.

[1] The functionality underlying network communications is often viewed in terms of conceptual layers, such as those defined in the 7 Layer OSI Model. *See* OSI Model, https://en.wikipedia.org/wiki/OSI_model (visited July 27, 2018). Several different protocol options may be available at each layer to accomplish specific tasks needed by the layer above it.

26. The Asserted Patents improved upon these conventional network monitoring systems and methods by categorizing network transmissions into "conversational flows" rather than merely in "connection flows." Unlike connection flow, conversational flow is the sequence of packets that are exchanged in any direction as a result of a particular activity—for instance, the running of an application on a server as requested by a client—which may include multiple connections, transmissions, or exchanges in either direction between the participants in the conversation. This addressed the problem of disjointed flows in network communications through "virtually concatenating," or linking, all related conversational exchanges.

27. "Conversational flows" are identified through parsing and analyzing data packets at deeper layers to extract information used to classify each data packet, determining whether it belongs to an existing conversational flow or is part of a new conversational flow. This is accomplished, in part, by populating a parsing/extraction operations memory and a state patterns/operations and database with machine operations that implement programmable rules and instructions for inspecting packets to identify patterns forming conversational flows.

28. Network traffic is inspected for pattern recognition to determine protocol types and headers for each protocol layer. Extracted packet information is compared to stored data corresponding to prior network transmissions to determine whether a current transmission belongs to a known flow comprising previously inspected transmissions. Extracted data may also be used to determine the different states, state transitions, and/or state operations to be performed corresponding to a conversational flow to aid in predicting and/or identifying subsequent transmissions within a conversational flow and/or to determine the termination of a conversational flow. One of the many advantages of the invention is properly analyzing the

packets exchanged between a client and a server and maintaining information relevant to the current state of each of these conversational flows.

29. Classifying transmissions in the context of conversational flows provides several benefits over conventional network monitoring systems and methods, including accommodation of: more flexible and effective stateful firewall operations to permit network operators greater flexibility in configuring network security policies; more robust understanding of the quality of service ("QoS") and bandwidth usage of a multiple connection flow application whereby certain network traffic could be excluded from data usage limits, bandwidth throttling may be applied to specific applications or services, and access to certain web browser applications may be restricted at specified times; and, eavesdropping or lawful interception, by cloning all of the traffic of a conversational flow, which allows another user on the network, or elsewhere, to read the content exchanged over the network without the knowledge of the original recipient.

V. THE ACCUSED PRODUCTS

30. The "Accused Products" include Nokia products, such as routers and Ethernet switches, running the Service Router Operating System ("SR OS") and providing Nokia's Application Assurance feature. These products include, but are not limited to: (1) 7705 Service Aggregation Router ("7705 SAR"), (2) 7450 Ethernet Service Switch ("7450 ESS"), (3) 7750 Service Router ("7750 SR") (4) 7950 Extensible Routing System ("7950 ERS" and "7950 XRX-XC"), and (5) Virtualized Service Router ("VSR").

31. The Application Assurance feature of the Accused Products allows inspection of packets at layers 3-7 of the OSI model to allow identification of a protocol associated with the packet and to determine the particular application associated with the packet. Nokia's documentation describes this capability as shown below:

3.2.2.2 Application Identification

Application identification means there is sufficient flow information to provide the network operator with a view to the underlying nature and value of the content. Application ID does not include:

- Anti-virus signatures per IPS/UTM.
- Content inspection (e-mail, text, picture, or video images). The payload data content of flows is typically not examined as part of the application identification.

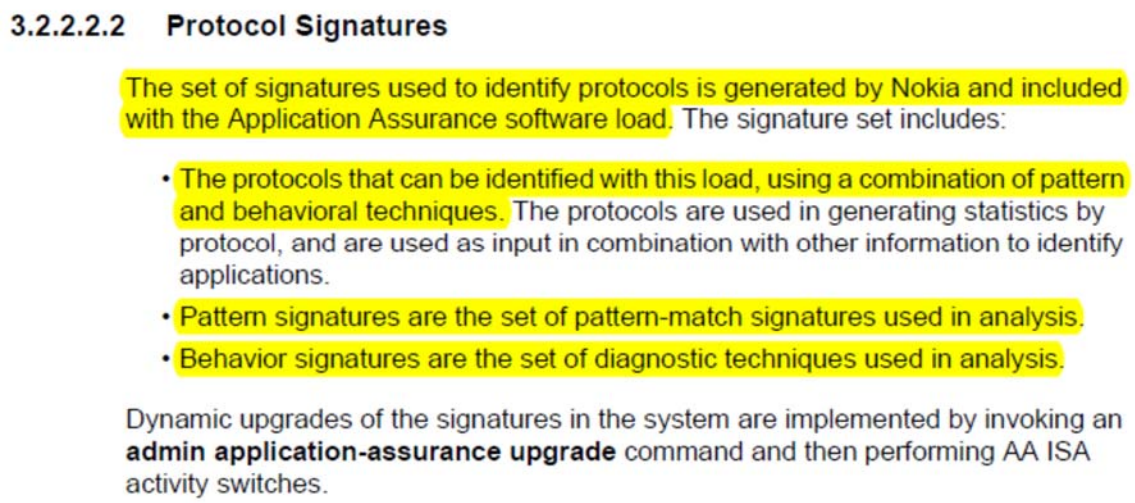
Application Assurance can identify and measure non-encrypted IP traffic flows using any available information from Layer 2 to Layer 7, and encrypted IP traffic flows using heuristic techniques.

Application Assurance attempts to positively identify the protocols and applications for flows based on a pattern signature observation of the setup and initial packets in a flow. The system correlates control and data flows belonging to the same application. In parallel, statistical and behavioral techniques are also used to identify the application. Until identified, the flow will not have a known application and will be treated according to the default policies (AQP policies defined using all or any ASO characteristics, subscriber Id and traffic direction as match criteria) for traffic for that AA subscriber, app-profile and direction (packets will be forwarded unless an action is configured otherwise). If the identification beyond OSI Layer 2is not successful, the flow will be flagged as an unknown protocol type, (for example unknown_tcp or unknown_udp). The unknown traffic is handled as part of all application statistics and policy, including generation of stats on the volume of unknown traffic.

See "Multiservice Integrated Service Adapter Guide Release 15.0.R1" or "Adapter Guide", at p. 80, which can be found at the URL: https://infoproducts.alcatel-lucent.com/cgi-bin/dbaccessfilename.cgi/3HE13637AAAATQZZA01_V1_7450%20ESS%207750%20SR%20and%20VSR%20Multiservice%20Integrated%20Service%20Adapter%20Guide%20R15.1.R1.pdf

32. As described above, the Accused Products correlate control and data flows belonging to the same application. This correlation of flows identifies a packet as being part of a particular conversational flow and ultimately associated with a particular application. The Accused Products use what Nokia calls Protocol Signatures and Application Filters in this analysis. Protocol Signatures include pattern signatures and behavioral techniques used in

determining a protocol associated with a particular packet and are described in Nokia's documentation shown below:



3.2.2.2.2 Protocol Signatures

The set of signatures used to identify protocols is generated by Nokia and included with the Application Assurance software load. The signature set includes:

- The protocols that can be identified with this load, using a combination of pattern and behavioral techniques. The protocols are used in generating statistics by protocol, and are used as input in combination with other information to identify applications.
- Pattern signatures are the set of pattern-match signatures used in analysis.
- Behavior signatures are the set of diagnostic techniques used in analysis.

Dynamic upgrades of the signatures in the system are implemented by invoking an **admin application-assurance upgrade** command and then performing AA ISA activity switches.

See Adapter Guide, at p. 83

33. The Application Filters used in the Accused Products are described as a numbered rule entry that defines the use of Protocol Signatures and other information to define a particular application. The Accused Products use Application Filters to analyze information obtained from the incoming packets to determine whether a packet is associated with a particular application. Nokia documentation further describes the Application Filters used in the Accused Products as follows:

3.2.2.2.9 Application Filters

Application filters (app-filter) are provided as an indirection between protocols and applications to allow the addition of variable parameters (port number, IP addresses, and so on) into an application definition. An application filter is a numbered rule entry that defines the use of protocol signatures and other criteria to define an application. Multiple rules can be used to define what constitutes an application but each rule will map to only one application definition.

The system concept of application filters is analogous to IP filters. Match of a flow to multiple rules is possible and is resolved by picking the rule with the lowest entry number that matches. A flow will only ever be assigned to one application.

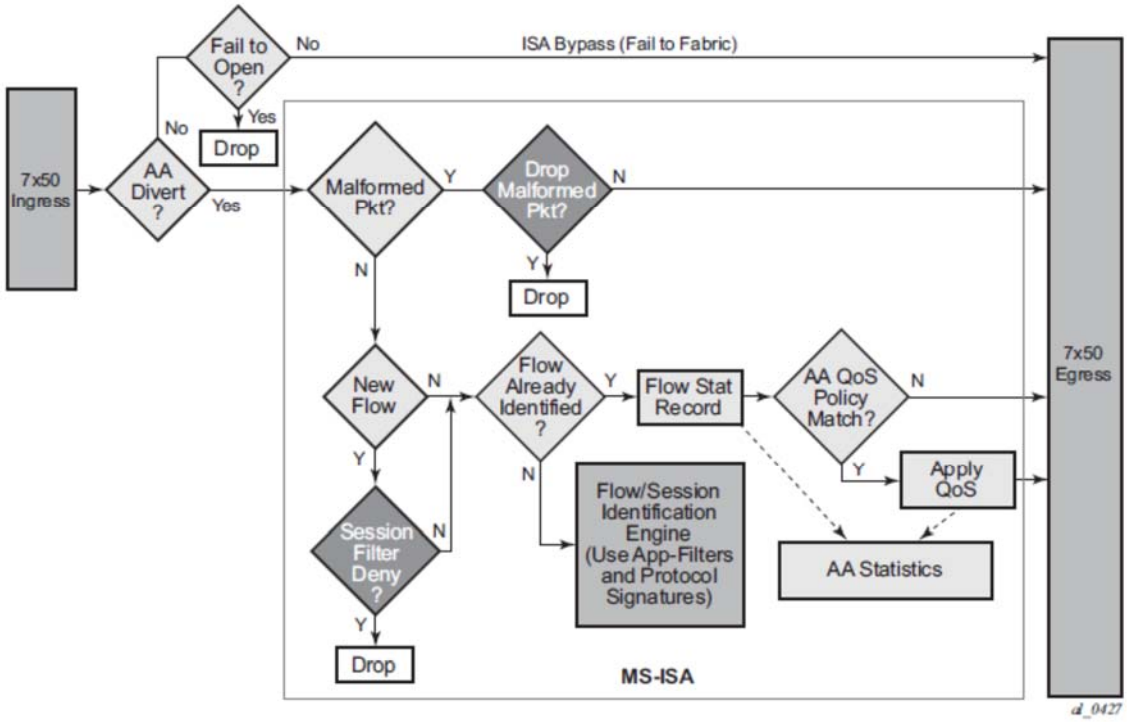
The following criteria can be assigned to an application filter rule entry:

- Unique entry ID number
- Application name
- Flow setup direction
- Server IP address (or server IP filter list)
- HTTP port (or HTTP port list) used by HTTP proxies
- Server port (or server port list)
- Protocol signature
- IP protocol number
- String matches against Layer 5+ protocol header fields (for example, a string expression against HTTP header fields)

See Adapter Guide, at p. 87.

34. The Accused Products use Protocol Signatures and Application Filters as part of the process shown in the flow chart below to process incoming packets.

Figure 13 **Application Assurance High Level Functional Components**



See Adapter Guide, at p. 56.

35. The flow chart shows several decision points during the processing of a packet in the Application Assurance feature. The Accused Products determine if a packet is part of a new flow or part of an existing flow that has already been identified. If the packet is part of a new flow, a Flow/Session Identification engine uses the Protocol Signatures and Application Filters to determine the type of protocols used in the packet and the application to which the packet relates. The flow chart also shows that other Quality of Service ("QOS") policies may be applied to the packet based on the application that is identified. A network operator using the Accused Products can set QOS policies that can limit the bandwidth for certain applications during peak

hours or prioritize packets associated with applications requiring more bandwidth, e.g., streaming video.

COUNT I
PATENT INFRINGEMENT
U.S. Patent No. 6,651,099

36. Packet Intelligence realleges paragraphs 1 through 35 as though fully set forth herein.

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

38. As of the time Defendant first had notice of Plaintiff’s allegations of infringement of one or more claims of the ’099 Patent by Defendant, which is no later than the filing date of this complaint, 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). Defendant has induced, caused, urged, encouraged, aided and abetted its direct and indirect customers to make, use, sell, offer for sale and/or import one or more of the Accused Products, and thus indirectly infringes at least claim 1 of the ’099 Patent. Defendant has done so by acts including but not limited to (1) selling such products including features that—when used or resold—infringe, either literally or under the doctrine of equivalents, the ’099 Patent; (2) marketing the infringing capabilities of such products; and (3) providing instructions, technical support, and other support and encouragement for the use of such products, including at least the documents referenced above. Such conduct by Defendant was intended to and actually did result in direct infringement by

Defendant's direct and indirect customers, including the making, using, selling, offering for sale and/or importation of the Accused Products in the United States.

39. Defendant's infringement of the '099 Patent has damaged Packet Intelligence, and 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.

40. As of the time Defendant first had notice of the '099 Patent, at least as early as December 2017, 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 Defendant has no good faith belief that it does not infringe the '099 Patent, at least Defendant's continued 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.

COUNT II
PATENT INFRINGEMENT
U.S. Patent No. 6,665,725

41. Packet Intelligence realleges paragraphs 1 through 35 as though fully set forth herein.

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

43. As of the time Defendant first had notice of Plaintiff's allegations of infringement of one or more claims of the '725 Patent by Defendant, 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). Defendant has induced, caused, urged, encouraged, aided and abetted its direct and indirect customers to make, use, sell, offer for sale and/or import one or more of the Accused Products, and thus indirectly infringes at least claim 17 of the '725 Patent. Defendant has done so by acts including but not limited to (1) selling such products including features that—when used or resold—infringe, either literally or under the doctrine of equivalents, the '725 Patent; (2) marketing the infringing capabilities of such products; and (3) providing instructions, technical support, and other support and encouragement for the use of such products, including at least the documents referenced above. Such conduct by Defendant was intended to and actually did result in direct infringement by Defendant's direct and indirect customers, including the making, using, selling, offering for sale and/or importation of the Accused Products in the United States.

44. Defendant's infringement of the '725 Patent has damaged Packet Intelligence, and 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.

45. As of the time Defendant first had notice of the '725 Patent, at least as early as December 2017, 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 Defendant has no good faith belief that it does not infringe the '725 Patent, at least Defendant's continued 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.

COUNT III
PATENT INFRINGEMENT
U.S. Patent No. 6,771,646

46. Packet Intelligence realleges paragraphs 1 through 35 as though fully set forth herein.

47. Defendant has infringed directly and continues to infringe directly, either literally or under the doctrine of equivalents, at least claim 7 of the ’646 Patent by its manufacture, sale, offer for sale, and use of any one or more of the Accused Products. Defendant is therefore liable for infringement of the ’646 Patent pursuant to 35 U.S.C. § 271.

48. As of the time Defendant first had notice of Plaintiff’s allegations of infringement of one or more claims of the ’646 Patent by Defendant, which is no later than the filing date of this complaint, 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). Defendant has induced, caused, urged, encouraged, aided and abetted its direct and indirect customers to make, use, sell, offer for sale and/or import one or more of the Accused Products, and thus indirectly infringes at least claim 7 of the ’646 Patent. Defendant has done so by acts including but not limited to (1) selling such products including features that—when used or resold—infringe, either literally or under the doctrine of equivalents, the ’646 Patent; (2) marketing the infringing capabilities of such products; and (3) providing instructions, technical support, and other support and encouragement for the use of such products, including at least the documents referenced above. Such conduct by Defendant was intended to and actually did result in direct infringement by Defendant’s direct and indirect customers, including the making, using, selling, offering for sale and/or importation of the Accused Products in the United States.

49. Defendant’s infringement of the ’646 Patent has damaged Packet Intelligence, and 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.

50. As of the time Defendant first had notice of the ’646 Patent, at least as early as December 2017, 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 Defendant has no good faith belief that it does not infringe the ’646 Patent, at least Defendant’s continued 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.

COUNT IV
PATENT INFRINGEMENT
U.S. Patent No. 6,839,751

51. Packet Intelligence realleges paragraphs 1 through 35 as though fully set forth herein.

52. Defendant has infringed directly and continues to infringe directly, either literally or under the doctrine of equivalents, at least claim 17 of the ‘751 Patent by its manufacture, sale, offer for sale, and use of any one or more of the Accused Products. Defendant is therefore liable for infringement of the ‘751 Patent pursuant to 35 U.S.C. § 271.

53. As of the time Defendant first had notice of Plaintiff’s allegations of infringement of one or more claims of the ’751 Patent by Defendant, which is no later than the filing date of this complaint, 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). Defendant has induced, caused, urged, encouraged, aided and abetted its direct and indirect customers to make, use, sell, offer for sale and/or import one or more of the Accused Products, and thus indirectly infringes at least claim 17 of the ‘751 Patent. Defendant has done so by acts including but not limited to (1) selling such products including features that—when used or resold—infringe, either literally or

under the doctrine of equivalents, the '751 Patent; (2) marketing the infringing capabilities of such products; and (3) providing instructions, technical support, and other support and encouragement for the use of such products, including at least the documents referenced above. Such conduct by Defendant was intended to and actually did result in direct infringement by Defendant's direct and indirect customers, including the making, using, selling, offering for sale and/or importation of the Accused Products in the United States.

54. Defendant's infringement of the '751 Patent has damaged Packet Intelligence, and 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.

55. As of the time Defendant first had notice of the '751 Patent, at least as early as December 2017, 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 Defendant has no good faith belief that it does not infringe the '751 Patent, at least Defendant's continued 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.

COUNT V
PATENT INFRINGEMENT
U.S. Patent No. 6,954,789

56. Packet Intelligence realleges paragraphs 1 through 35 as though fully set forth herein.

57. Defendant has infringed directly and continues to infringe directly, either literally or under the doctrine of equivalents, at least claim 19 of the '789 Patent by its manufacture, sale,

offer for sale, and use of any one or more of the Accused Products. Defendant is therefore liable for infringement of the '789 Patent pursuant to 35 U.S.C. § 271.

58. As of the time Defendant first had notice of Plaintiff's allegations of infringement of one or more claims of the '789 Patent by Defendant, which is no later than the filing date of this complaint, 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). Defendant has induced, caused, urged, encouraged, aided and abetted its direct and indirect customers to make, use, sell, offer for sale and/or import one or more of the Accused Products, and thus indirectly infringes at least claim 19 of the '789 Patent. Defendant has done so by acts including but not limited to (1) selling such products including features that—when used or resold—infringe, either literally or under the doctrine of equivalents, the '789 Patent; (2) marketing the infringing capabilities of such products; and (3) providing instructions, technical support, and other support and encouragement for the use of such products, including at least the documents referenced above. Such conduct by Defendant was intended to and actually did result in direct infringement by Defendant's direct and indirect customers, including the making, using, selling, offering for sale and/or importation of the Accused Products in the United States.

59. Defendant's infringement of the '789 Patent has damaged Packet Intelligence, and 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.

60. As of the time Defendant first had notice of the '789 Patent, at least as early as December 2017, 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 Defendant has no good faith belief that it does not infringe the '789 Patent, at

least Defendant's continued 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

61. 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 Defendant has, either literally or under the doctrine of equivalents, directly infringed and is directly infringing one or more of the claims of the Asserted Patents, and/or judgment in favor of Packet Intelligence that one or more of the claims of the Asserted Patents have been directly infringed by others and indirectly infringed by Defendant, to the extent Defendant induced such direct infringement by others;

B. An order permanently enjoining the Defendant, its respective officers, agents, employees, and those acting in privity with it, from further direct and/or indirect infringement of one or more claims of the Asserted Patents, or, alternatively, an award of an ongoing royalty for Defendant's post-judgment infringement of the asserted claims of the Asserted Patents in an amount to be determined at trial;

C. An award of damages to Packet Intelligence arising out of Defendant's infringement of one or more claims of the Asserted 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. A judgment declaring this case exceptional under 35 U.S.C. § 285 and awarding Packet Intelligence its attorneys' fees;

E. An award of prejudgment and post-judgment interest to the full extent permitted by controlling law; and,

F. An award of costs and any further relief as the Court may deem just and proper to Packet Intelligence.

Dated: August 30, 2018

Respectfully submitted,

/s/ *Jonathan T. Suder by permission Claire Henry*

Jonathan T. Suder
State Bar No. 19463350
Corby R. Vowell
State Bar No. 24031621
Dave R. Gunter
State Bar No. 24074334
FRIEDMAN, SUDER & COOKE
604 East 4th Street, Suite 200
Fort Worth, TX 76102
817-334-0400
Fax: 817-334-0401
vowell@fsclaw.com
jts@fsclaw.com
gunter@fsclaw.com

T. John Ward, Jr.
Texas State Bar No. 00794818
E-mail: jw@wsfirm.com
Claire Abernathy Henry
Texas State Bar No. 24053063
E-mail: claire@wsfirm.com
WARD, SMITH & HILL, PLLC
PO Box 1231
Longview, Texas 75606
(903) 757-6400 (telephone)
(903) 757-2323 (facsimile)

ATTORNEYS FOR PLAINTIFF PACKET INTELLIGENCE, LLC