1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19	Brian A. E. Smith (SBN 188147) Alden KW Lee (SBN 257973) Jeffrey D. Chen (SBN 267837) Joseph J. Fraresso (SBN 289228) BARTKO, ZANKEL, BUNZEL, & MILLER One Embarcadero Center San Francisco, CA 94111 T: 415-956-1900 Email: bsmith@bzbm.com Email: jchen@bzbm.com Email: jchen@bzbm.com Email: jfraresso@bzbm.com Jonathan T. Suder (Pro Hac Vice To Be Filed) Corby R. Vowell (Pro Hac Vice To Be Filed) Pave R. Gunter (Pro Hac Vice To Be Filed) FRIEDMAN, SUDER & COOKE 604 East 4th Street, Suite 200 Fort Worth, TX 76102 T: 817-334-0400 F: 817-334-0401 jts@fsclaw.com vowell@fsclaw.com Michael F. Heim (Pro Hac Vice To Be Filed) Robert Allan Bullwinkel (Pro Hac Vice To Be Filed) HEIM, PAYNE & CHORUSH, LLP 1111 Bagby Street, Suite 2100 Houston, Texas 77002 T: 713-221-2000 F: 713-221-2021 mheim@hpcllp.com abullwinkel@hpcllp.com cfirst@hpcllp.com	led)		
20	Counsel for Plaintiff Packet Intelligence LLC			
21	UNITED STATES DISTRICT COURT			
22	NORTHERN DISTRICT OF CALIFORNIA			
23	PACKET INTELLIGENCE LLC,	Case No.		
24	Plaintiff,	PACKET INTELLIGENCE LLC'S		
25	V.	COMPLAINT FOR PATENT INFRINGEMENT		
26	JUNIPER NETWORKS, INC.,			
27	Defendant.	DEMAND FOR JURY TRIAL		
28				

2697.001/1426122.1 1 Case No.

1

4

5

6

7 8

9 10

11 12

13 14

16

17

15

18 19

21

20

23 24

26 27

28

25

PACKET INTELLIGENCE LLC ("Packet Intelligence" and "Plaintiff" herein) 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 JUNIPER NETWORKS, INC. ("Juniper" and "Defendant" herein).

I. THE PARTIES

- 1. Packet Intelligence LLC is a limited liability company existing under the laws of Texas since June 2012. Plaintiff maintains its principal place of business at 705B Mulberry Ave, Celebration, FL 34747.
- 2. Upon information and belief, Juniper Networks, Inc. is a Delaware Corporation, with a principal place of business at 1133 Innovation Way, Sunnyvale, CA 94089. Defendant may be served with process through its Registered Agent, CT Corporation System located at 818 Seventh Street, Suite 930, Los Angeles, CA 90017.

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 has sufficient minimum contacts with the Northern District of California 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 it 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 Northern District of California.
- 5. Further, Defendant makes or sells products that are and have been used, offered for sale, sold, and/or purchased in the Northern District of California. 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 Northern District of California.
- 6. 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.

2697.001/1426122.1 Case No.

III. THE PATENTS-IN-SUIT

- 7. 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.
- 8. 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. Mr. Dietz 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).
- 9. 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. 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.
- 10. 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.

- 11. 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.
- 12. 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.
- 13. 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.
- 14. 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.
- 15. 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.
- 16. 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.

- 17. 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.
- 18. 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 the Eastern District of Texas and one pending action in this District (*See Palo Alto Networks, Inc. v. Packet Intelligence LLC*, Civil Action No. 3:19-cv-02471-WHO). 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 the Eastern District of Texas:
 - 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)). The Court resolved post trial motions with final appealable orders on May 31, 2019 and June 5, 2019 and the case is currently on appeal to the Court of Appeals for the Federal Circuit;
 - 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));

- Two other actions involving the Asserted Patents are currently pending in the Eastern
 District of Texas as *Packet Intelligence LLC v. Nokia of America Corporation*, Civil
 Action No. 2:18-cv-00382-JRG and *Packet Intelligence LLC v. Ericsson Inc.*, Civil
 Action No. 2:18-cv-00381-JRG.
- 19. 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.
- 20. Defendant 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 January 18, 2019, at which time Packet Intelligence sent a notice letter alleging Defendant infringes the Asserted Patents.

IV. BACKGROUND AND FACTS

21. 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.

- 1 | 2 | 3 | 4 | 5 | 6 |

- 22. 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.
- 23. 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 layer¹ 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.
- 24. 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

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.

addressed the problem of disjointed flows in network communications through "virtually concatenating," or linking, all related conversational exchanges.

- 25. "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.
- 26. 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.
- 27. 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

28. The "Accused Products" include Defendant's products, such as gateway and firewall						
products that include the Application Identification feature, and/or the Juniper Application Aware						
feature or other similar functionality. These products include, but are not limited to: SRX Series						
Gateway and/or Firewall products both physical and virtual/containerized platforms (including but						
not limited to SRX100, SRX110, SRX210, SRX220, SRX240, SRX300, SRX320, SRX340,						
SRX550, SRX650, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800,						
vSRX, and cSRX), the Juniper MX Series routers including both physical and virtual platforms						
(including but not limited to virtual MX (vMX), MX5. MX10, MX40, MX80, MX104, MX150,						
MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX 10008, and						
MX10016), and the NFX Series Network Services Platform products both physical and virtual						
platforms (including but not limited to NFX150 and NFX250) and any predecessor or successor						
models.						

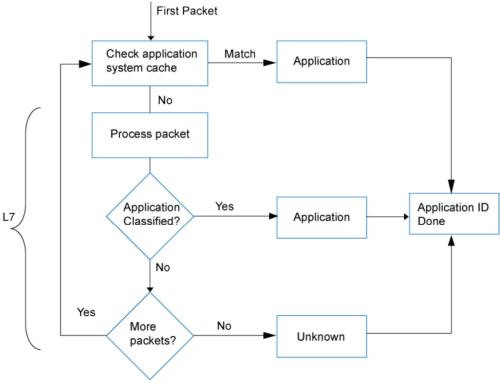
29. The Application Identification and Application Aware features of the Accused Products allow inspection of packets at layers 3-7 of the OSI model to allow identification of a protocol associated with the packet and to determine the particular application associated with the packet. Defendant's documentation describes this capability as shown below:

1 Junos OS Next-Generation Application Identification Next-generation application identification builds on the legacy application identification 2 functionality and provides more effective detection capabilities for evasive applications such as Skype, BitTorrent, and Tor. 3 Junos OS application identification recognizes Web-based and other applications and 4 protocols at different network layers using characteristics other than port number. 5 Applications are identified by using a protocol bundle containing application signatures and parsing information. The identification is based on protocol parsing and decoding 6 and session management. 7 The detection mechanism has its own data feed and constructs to identify applications. 8 The following features are supported in application identification: 9 · Support for protocols and applications, including video streaming, peer-to-peer communication, social networking, and messaging 10 · Identification of services within applications 11 Ability to distinguish actions launched within an application (such as login, browse, chat, and file transfer) 12 Support for all versions of protocols and application decoders and dynamic updates 13 of decoders 14 · Support for encrypted and compressed traffic and most complex tunneling protocols Ability to identify all protocols from Layer 3 to Layer 7 and above Layer 7 15 16 17 See "Junos OS – Application Security Feature Guide for Security Devices," at p. 28. 18 30. A flow chart of the process by which the Accused Products identify the application 19 that corresponds to a packet is shown below in the excerpt from Defendant's documentation: 20 21 22 23 24 25 26 27 28

Application Identification Match Sequence

Figure 1 on page 29 shows the sequence in which mapping techniques are applied and how the application is determined.

Figure 1: Mapping Sequence



See "Junos OS – Application Security Feature Guide for Security Devices," at p. 29.

31. The flow chart shows several decision points during the processing of a packet in the Application Identification feature. The Accused Products can be used to implement one or more of the AppSecure models, such as AppTrack, AppFW, AppQoS, AppDoS, and IPS. For instance, AppQoS can be used to implement Quality of Service ("QOS") policies that are applied to packets 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.

VI. PATENT INFRINGEMENT (U.S. Patent No. 6,651,099)

- 32. Packet Intelligence realleges paragraphs 1 through 31 as though fully set forth herein.
- 33. 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.

- 34. 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 date of the notice letter sent by Packet Intelligence on January 18, 2019, 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.
- 35. 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.
- 36. As of the time Defendant first had notice of the '099 Patent, at least as early as January 18, 2019, 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.

VII. PATENT INFRINGEMENT (U.S. Patent No. 6,665,725)

3

2

4

5 6

7

8

9 10 11

12

13

14

15 16

17

18 19

20 21

22 23

24

25 26

- 37. Packet Intelligence realleges paragraphs 1 through 31 as though fully set forth herein.
- 38. 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.
- 39. 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, at least as early as January 18, 2019, 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.
- 40. 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.
- 41. As of the time Defendant first had notice of the '725 Patent, at least as early as January 18, 2019, Defendant has continued with its infringement despite the objectively high likelihood that its actions constitute infringement 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.

3

VIII. PATENT INFRINGEMENT (U.S. Patent No. 6,771,646)

4 5 42. Packet Intelligence realleges paragraphs 1 through 31 as though fully set forth herein.

6

7

8

9

43. 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.

As of the time Defendant first had notice of Plaintiff's allegations of infringement of

10

11

12

13

14

15

16

17

44.

one or more claims of the '646 Patent by Defendant, which is no later than the January 18, 2019, 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

1819202122

23

24

25

States.

45. 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.

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

26

27

28

46. As of the time Defendant first had notice of the '646 Patent, at least as early as January 18, 2019 2017, Defendant has continued with its infringement despite the objectively high

1 | 1 | 2 | 6 | 3 | I | 4 | I | 5 | i i

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.

IX. PATENT INFRINGEMENT (U.S. Patent No. 6,839,751)

- 47. Packet Intelligence realleges paragraphs 1 through 31 as though fully set forth herein.
- 48. 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.
- 49. 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 January 18, 2109, 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.
- 50. 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.

51. As of the time Defendant first had notice of the '751 Patent, at least as early as January 18, 2019, 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.

X. PATENT INFRINGEMENT (U.S. Patent No. 6,954,789)

- 52. Packet Intelligence realleges paragraphs 1 through 31 as though fully set forth herein.
- 53. 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.
- 54. 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.

55. 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.

56. As of the time Defendant first had notice of the '789 Patent, at least as early as January 18, 2019, 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

57. 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 Patents-in-Suit, and/or judgment in favor of Packet Intelligence that one or more of the claims of the Patents-in-Suit have been directly infringed by others and indirectly infringed by Defendant, to the extent Defendant induced or contributed to such direct infringement by others;
- B. An order permanently enjoining 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 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

1	pursuant to 35 U.S.C. § 284, together with prejudgment and post-judgment interest, in ar		
2	amount to be determined at trial;		
3	D.	A judgment declaring this case exceptional under 35 U.S.C. § 285 and	
4	awarding Packet Intelligence its attorneys' fees;		
5	E.	An award of prejudgment and post-judgment interest to the full extent	
6	permitted by controlling law; and,		
7	F.	An award of costs and any further relief as the Court may deem just and	
8	proper to Packet Intelligence.		
9			
10	DATED: August 13	, 2019	BARTKO ZANKEL BUNZEL & MILLER A Professional Law Corporation
11			11 Trolessional Law Corporation
12			D
13			By: /s/ Brian A.E. Smith Brian A. E. Smith
14			Counsel for Plaintiff Packet Intelligence LLC
15			
16			
17			
18			
1920			
21			
22			
23			
24			
25			
26			
27			
28			