1  Brian A. E. Smith (SBN 188147)
   Alden KW Lee (SBN 257973)
2  Jeffrey D. Chen (SBN 267837)
   Joseph J. Fraresso (SBN 289228)
3  BARTKO, ZANKEL, BUNZEL, & MILLER
   One Embarcadero Center
4  San Francisco, CA 94111
   T: 415-956-1900
5  Email: bsmith@bzbm.com
   Email: alee@bzbm.com
6  Email: jchen@bzbm.com
   Email: jfraresso@bzbm.com
7
   Jonathan T. Suder (*Pro Hac Vice*)
8  Corby R. Vowell (*Pro Hac Vice*)
   Dave R. Gunter (*Pro Hac Vice*)
9  FRIEDMAN, SUDER & COOKE
   604 East 4th Street, Suite 200
10 Fort Worth, TX 76102
   T: 817-334-0400
11 F: 817-334-0401
   jts@fsclaw.com
12 vowell@fsclaw.com
   gunter@fsclaw.com
13
   Michael F. Heim (*Pro Hac Vice*)
14 R. Allan Bullwinkel (*Pro Hac Vice*)
   Christopher M. First (*Pro Hac Vice*)
15 HEIM, PAYNE & CHORUSH, LLP
   1111 Bagby Street, Suite 2100
16 Houston, Texas 77002
   T: 713-221-2000
17 F: 713-221-2021
   mheim@hpcllp.com
18 abullwinkel@hpcllp.com
   cfirst@hpcllp.com
19
   *Counsel for Plaintiff, Packet Intelligence LLC*

20
21                UNITED STATES DISTRICT COURT
               NORTHERN DISTRICT OF CALIFORNIA
                   SAN FRANCISCO DIVISION
22

23 PACKET INTELLIGENCE LLC,          Case No. 3:19-cv-04741-WHO

24           Plaintiff,              **PACKET INTELLIGENCE LLC'S
                                     DISCLOSURE OF ASSERTED CLAIMS
25        v.                         AND INFRINGEMENT CONTENTIONS
                                     TO JUNIPER NETWORKS, INC.**
26 JUNIPER NETWORKS, INC.,

27           Defendant.

28

PACKET INTELLIGENCE LLC ("Packet Intelligence") hereby provides its disclosure of asserted claims and infringement contentions. Packet Intelligence expressly reserves the right to supplement its contentions based on additional information obtained in discovery and/or the Court's claim construction.

**1.     3-1 Disclosure of Asserted Claims and Infringement Contentions**

**(a)     Each claim of each patent in suit that is allegedly infringed by each opposing party, including for each claim the applicable statutory subsections of 35 U.S.C. §271 asserted;**

Based on presently available information, Packet Intelligence contends that Juniper Network, Inc. ("Juniper") directly infringes under 35 U.S.C. §271(a) at least the following claims:

- Claims 1, 2, 4, and 5 of U.S. Patent No. 6,651,099.

- Claims 10, 12, 13, 16, and 17 of U.S. Patent No. 6,665,725;

- Claims 1, 2, 3, 7, 16, and 18 of U.S. Patent No. 6,771,646;

- Claims 1, 2, 5, 10, 14, and 15 of U.S. Patent No. 6,839,751;

- Claims 1, 2, 13, 14, 15, 16, 17, 19, 20, 31, 33, 34, 42, 44, 48, and 49 of U.S. Patent No. 6,954,789;

Based on presently available information, Packet Intelligence contends that Juniper induces and/or has induced its customers to directly infringe under 35 U.S.C. §271(b) at least the following claims:

- Claims 1, 2, 4, and 5 of U.S. Patent No. 6,651,099.

- Claims 10, 12, 13, 16, and 17 of U.S. Patent No. 6,665,725;

- Claims 1, 2, 3, 7, 16, and 18 of U.S. Patent No. 6,771,646;

- Claims 1, 2, 5, 10, 14, and 15 of U.S. Patent No. 6,839,751;

- Claims 1, 2, 13, 14, 15, 16, 17, 19, 20, 31, 33, 34, 42, 44, 48, and 49 of U.S. Patent No. 6,954,789;

**(b)** **Separately for each asserted claim, each accused apparatus, product, device, process, method, act, or other instrumentality ("Accused Instrumentality") of each opposing party of which the party is aware. This identification shall be as specific as possible. Each product, device, and apparatus shall be identified by name or model number, if known. Each method or process shall be identified by name, if known, or by any product, device, or apparatus which, when used, allegedly results in the practice of the claimed method or process;**

Based on presently available information, Packet Intelligence accuses the following products of infringing the Asserted Claims listed above:

The "Accused Products" include all Juniper products, such as firewall, router, and/or switch products, that include the Application Identification or Application Aware features, as well as any other Juniper products with the same or similar functionality. These products include the Juniper NFX Series Network Services Platform (including but not limited to *e.g.*, NFX150, NFX250, NFX350), the Juniper SRX Series Next Generation Firewall (NGFW) (including but not limited to *e.g.*, vSRX, cSRX, SRX100, SRX110, SRX210, SRX220, SRX240, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550, SRX550 HM, SRX650, SRX1400, SRX1500, SRX3400, SRX3600, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800 and other SRX Series products that provide similar functionality) including both physical and virtual/containerized platforms, the Juniper MX Series routers including both physical and virtual platforms (including but not limited to *e.g.*, vMX, MX5. MX10, MX40, MX80, MX104, MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003), the Juniper EX Ethernet Switches (including but not limited to *e.g.*, EX9200, EX9200-VC, EX9251, EX9253), Juniper T Series products (including but not limited to *e.g.*, T640, T1600, TX Matrix, TX Matrix Plus), Juniper M Series products (including but not limited to *e.g.*, M120, M320), and any predecessor or successor models, all of which support or supported the Application Identification (APPID) and/or Application Aware (AppAware) features, and any other Juniper products with similar packet-based traffic classification and processing technology or other products classifying and relating packet-based traffic flows with each other, including using information from one or more of layers 5-7 (session, presentation, and/or application layers) of the OSI model to do so.

**(c)** **A chart identifying specifically where and how each limitation of each asserted claim is found within each Accused Instrumentality, including for each limitation that such party contends is governed by 35 U.S.C. § 112(6), the**

1    **identity of the structure(s), act(s), or material(s) in the Accused Instrumentality**
     **that performs the claimed function.**

2

3         The Accused Products practice the Asserted Claims as shown in the claim charts attached

4    hereto as Exhibits A-E. Any citations to publicly available documentation in the attached claim

5    charts are exemplary and not exhaustive, as are the examples provided of the ways in which the

6    Accused Products satisfy the elements of each of the Asserted Claims. Moreover, any and all

7    citations or references to publicly available documentation should be understood to encompass any

8    and all prior versions that incorporate the same or similar functionality, as well as any similar or

9    derivative products which Packet Intelligence has been unable to discover from publicly available

10   information to this point.

11        **(d)**    **For each claim which is alleged to have been indirectly infringed, an**
                     **identification of any direct infringement and a description of the acts of the**
                     **alleged indirect infringer that contribute to or are inducing that direct**
12                   **infringement. Insofar as alleged direct infringement is based on joint acts of**
                     **multiple parties, the role of each such party in the direct infringement must be**
13                   **described.**

14        Packet Intelligence contends that Juniper has induced infringement of each of the Asserted

15   Claims by instructing, causing, urging, and/or encouraging its customers to make, use, sell, offer for

16   sale and/or import the Accused Products. For example, Juniper's customers of the Accused Products

17   in the United States include at least:

18        • Aston Martin

19        • Gap Inc.

20        • Dartmouth

21        • The Ricoh Group

22        • Rackspace

23        • Iron Mountain

24        • Dedicated.com

25        • City of Fairlawn, Ohio

26        • Linode

27        • Gamesys Group

28        • Intelsat

- Blackberry

- University of Louisiana, Monroe

See also: https://www.juniper.net/us/en/company/case-studies-customer-success/#Sort=featured. Juniper has induced infringement 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 Patents-in-Suit; (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.

Juniper provides documentation to its customers describing how to install, implement, and use the Junos operating system and Application Identification feature in an infringing manner on the Accused Products which is specific evidence of Juniper's intent to encourage infringement of the Patents-in-Suit. For example, Juniper provides the following documents:

- Junos OS Application Security User Guide for Security Devices
  See: https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/security/security-application-identification.pdf

- Junos OS Application Aware Services Interfaces Features Guide for Routing Devices
  See: https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/services-interfaces/application-aware-access-list.pdf

- Junos OS Intrusion Detection and Prevention User Guide
  See: https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/security/security-idp-policy.pdf

Additional Junos OS and Application Identification technical documentation that Juniper provides to its customers can be found at https://www.juniper.net/documentation/product/en_US/junos-os

Juniper has had knowledge of the Patents-in-Suit and Packet Intelligence's infringement allegations related to the accused products since at least as early as January 18, 2019. As of the time Juniper first had notice of the Packet Intelligence's infringement allegations, Juniper has continued with its infringement despite an objectively high likelihood that its actions constitute infringement

# DOCKET ALARM

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

### LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

### FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

### E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.