IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTICT OF TEXAS
TYLER DIVISION

SELECTIVE SIGNALS, LLC,
 	
                                   Plaintiff,
 	
      v.
 	
ROHDE & SCHWARZ USA, INC.
 	
                                   Defendant.
	Case No. _____
	
	JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

This is an action for patent infringement in which Selective Signals, LLC ("Selective" or "Plaintiff") makes the following allegations against Rohde & Schwarz USA, Inc. ("Rohde" or "Defendant").

NATURE OF THE ACTION

1.   This is a patent infringement action to stop Defendant's infringement of United States Patent No. 8,111,629 ("the '629 Patent") ("the Patent-in-Suit").

PARTIES

2.   Plaintiff Selective Signals, LLC is a Texas limited liability company with its principal place of business at 211 E. Tyler St., Suite 600-A, Longview, TX 75601.

3.   On information and belief, Rohde & Schwarz USA, Inc. is a corporation, with its principal place of business at 6821 Benjamin Franklin Drive, Columbia, MD 21046.   On information and belief, Rohde may be served via its registered agent, Corporation Service Company DBA CSC-Lawyers Incorporating Service Company at 211 E. 7th St. Suite 620, Austin, TX 78701.

JURISDICTION AND VENUE

4.   The Court has personal jurisdiction over Defendant, including because Defendant has minimum contacts within the State of Texas; Defendant has purposely availed itself of the privileges of conducting business in the State of Texas; Defendant regularly conducts business within the State of Texas; and Selective's cause of action arises directly from Defendant's business contacts and other activities in the State of Texas.

5.   More specifically, Defendant, directly and/or through its intermediaries, makes, distributes, imports, offers for sale, sells, advertises and/or uses, including the accused products identified herein that practice the claimed method of the Patent-in-Suit in the State of Texas. Defendant has committed patent infringement in the State of Texas and solicits customers in the State of Texas. Defendant has paying customers who are residents of the State of Texas and who purchase and/or use Defendant's infringing products in the State of Texas. Further, Defendant has an interactive website that is accessible from the State of Texas.

5.   Venue is proper in this district under 28 U.S.C. §§ 1391(c) and 1400(b). On information and belief, Defendant has transacted business in this district, and has committed acts of patent infringement in this district.

6.   More specifically, Defendant, directly and/or through its intermediaries, makes, distributes, imports, offers for sale, sells, advertises and/or uses, devices including the Accused Systems identified herein, that practice the claimed method of the Patent-in-Suit in the State of Texas. Defendant has committed patent infringement in the State of Texas and solicits customers in the State of Texas. Defendant has paying customers who are residents of the State of Texas and who purchase and/or use Defendant's infringing products in the State of Texas.

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 8,111,629

7.   Plaintiff is the owner by assignment of the '629 Patent entitled "Media Session Identification Method for IP Network" – including all rights to recover for past and future acts of infringement. The '629 Patent issued on February 7, 2012. A true and correct copy of the '629 Patent is attached as Exhibit A.

8.   Infringement by Defendant includes, without limitation, making, distributing, importing, offering for sale, selling, advertising, and/or using, without limitation methods of identifying session type (collectively referred to hereinafter as "Defendant's devices performing the Accused Methods") infringing at least claim 15 of the '629 Patent. Defendant's devices performing the Accused Methods offer significant enhancements for network health and security for homes or businesses. Network security appliances, like Defendant's devices performing the Accused Methods, must analyze ever-increasing amounts of network traffic and do so without noticeably increasing latency. Rather than holding traffic for approval, it must be able to scan a flow of data packets to determine what they're probably doing, even if they are encrypted or piggybacking on other data streams. This is essential for both preventing potentially damaging activity, such as network intrusions, or the spread of a malware infection, and businesses also have the added concern of preventing certain types of programs or network sessions from occurring, either for security purposes or just to ensure their workforce stays productive. Today many network security appliances, including next generation firewalls, utilize methods for identifying session types such as those previously claimed by the '629 Patent.

9.   Defendant makes and sells products that utilize the method of identifying session type of the '629 Patent. These devices performing the Accused Methods include, for example

and without limitation, Defendant's R&S network security appliances and gateprotect network security appliances. A detailed claim chart is incorporated herein by reference and attached at Exhibit B.

10.   Each of Defendant's devices performing the Accused Methods are designed to perform the first step, "obtaining passing packets of respectively unknown sessions and unknown session types." Defendant's devices that perform the Accused Methods obtain passing packets to provide "deep packet inspection, behavioral, heuristic and statistical analysis - to reliably detect network protocols and applications and extract metadata in realtime." Said devices must obtain packets as packet preparation is a per-packet based operation." *See, e.g.,* https://cybersecurity.rohde-schwarz.com/sites/default/files/download/rs-cybersecurity_solution_guide_pace2_web.pdf at Exhibit B.

.

11.   Defendant's devices that perform the Accused Methods are designed to perform the second step, "obtaining traffic packet characteristics of said passing packets of respectively unknown session types."   Defendant's devices that perform the Accused Methods obtain passing packets then determine its characteristics. This enables Defendant's devices that perform the Accused Methods to monitor data signatures, protocols, data content, source and destination addresses and behavior through "deep packet inspection, behavioral, heuristic and statistical analysis - to reliably detect network protocols and applications and extract metadata in realtime." Traffic packet characteristics are obtained in at least the "Packet Classification" stage, which "provides the protocol and application detection results" using "a high number of different protocol and application detections," and the "Packet Decoding" stage which "provides advanced metadata." *See, e.g.*, https://cybersecurity.rohde-schwarz.com/sites/default/files/download/rs-cybersecurity_solution_guide_pace2_web.pdf at Exhibit B.

12.   Defendant's devices that perform the Accused Methods are designed to perform the third step, "comparing said obtained packets with each other using respectively obtained traffic packet characteristics." Defendant's devices that perform the Accused Methods compare obtained packets with each other using the characteristics to help determine, for example, the application. "behavioral, heuristic and statistical analysis," used "to reliably detect network protocols and applications and extract metadata in realtime" all require that Defendant's devices that perform the Accused Methods must capture and compare multiple packets to perform these comparative functions. Further, if Defendant's devices that perform the Accused Methods determine there is insufficient information for the comparison, "The engine will buffer out-of-order packets until the missing packets arrive or a specific timeout occurs. With the help of packet reordering, the detection classification rate will be improved."

See, e.g., https://cybersecurity.rohde-schwarz.com/sites/default/files/download/rs-cybersecurity_solution_guide_pace2_web.pdf at Exhibit B.

13.   Defendant's devices that perform the Accused Methods are designed to perform the fourth step, "grouping together those packets having similar values of said traffic packet characteristics into a presumed session." Defendant's devices that perform the Accused Methods automatically group together packets that have similar values of traffic packet characteristics (i.e., same application, same protocol and same user) to a session. This is evidenced by the fact that Defendant's devices that perform the Accused Methods include a "re-ordering engine" that "will buffer out-of-order packets until the missing packets arrive or a specific timeout occurs." Grouping these packets into a presumed session, "With the help of packet reordering," ensures that "the detection classification rate will be improved." This grouping is done by gathering "flow information" to create a "state buffer" which is "maintained for every subscriber. In most

situations, a subscriber is identified by an internal IP address." *See, e.g.,* https://cybersecurity.rohde-schwarz.com/sites/default/files/download/rs-cybersecurity_solution_guide_pace2_web.pdf at Exhibit B.

14. Defendant's devices that perform the Accused Methods are designed to perform the fifth step, "analyzing said grouped packets of said presumed session for session characteristics." Defendant's devices that perform the Accused Methods analyze grouped packets of said presumed session to determine session characteristics. Defendant's devices that perform the Accused Methods "inspects and analyzes network data in realtime, providing accurate detection of today's most popular applications with the ability to extract metadata and application attributes from the network traffic. Different technologies such as deep packet inspection (DPI), behavioral, heuristic and statistical analysis are used to analyze the IP packet in order to determine the protocol and application and other application based attributes of the traffic." *See, e.g.*, https://cybersecurity.rohde-schwarz.com/sites/default/files/download/rs-cybersecurity_solution_guide_pace2_web.pdf at Exhibit B.

15. Defendant's devices that perform the Accused Methods are designed to perform the final step, "using said session characteristics to identify a session type of said presumed session." Defendant's devices that perform the Accused Methods use the session characteristics to determine a session type. In addition to the ability to determine the protocol and application described *supra*, Defendant's devices that perform the Accused Methods can also determine the "Application Attributes." Once classification has been performed, Metadata (e.g., "volume of traffic," "identifiers … that can be used to implement strong security rules," the "used codec," and "usage") can be meaningfully extracted, dependent on the session type, for use in security

analysis. *See, e.g.*, https://cybersecurity.rohde-schwarz.com/sites/default/files/download/rs-cybersecurity_solution_guide_pace2_web.pdf at Exhibit B.

16.   Defendant is thus liable for infringement of the '629 Patent under 35 U.S.C. §271.

17.   Each of Defendant's aforesaid activities has been without authority and/or license from Selective.

18.   Selective is entitled to recover from Defendant the damages sustained by Selective as a result of Defendant's wrongful acts in an amount subject to proof at trial, which by law cannot be less than a reasonable royalty, together with interest and costs as fixed by this court under 35 U.S.C. § 284.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court enter a judgment:

1.   In favor of Plaintiff that Defendant has infringed the '629 Patent;

2.   Requiring Defendant to pay Plaintiff its damages, costs, expenses, and prejudgment and post-judgment interest for Defendant's infringement of the '629 Patent as provided under 35 U.S.C. § 284; and

3.   Granting Plaintiff any and all other relief to which Plaintiff may show itself to be entitled.

DEMAND FOR JURY TRIAL

Plaintiff, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

Dated: January 31, 2017   Respectfully submitted,

/s/ Todd Y. Brandt
Todd Y. Brandt
State Bar No. 24027051
BRANDT LAW FIRM
222 N. Fredonia Street
Longview, Texas 75606
Telephone: (903) 212-3130
Facsimile: (903) 753-6761
tbrandt@thebrandtlawfirm.com

Attorneys for Selective Signals, LLC