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

SELECTIVE SIGNALS, LLC, **Plaintiff,** **v.** **WATCHGUARD TECHNOLOGIES, 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 Watchguard Technologies, Inc. ("Watchguard" 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, Watchguard Technologies, Inc. is a corporation, with its principal place of business at 505 Fifth Avenue South, suite 500, Seattle, WA 98104. On information and belief, Watchguard may be served via its registered agent, SLG Registered Agent LLC at 315 5th Avenue, Suite 1000, Seattle, WA 98104.

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 Fireware XTM Network Security Appliances and Firebox

Network Security Appliances including the T Series and M Series. 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 perform both "Stateful packet inspection" and "deep packet inspection." *See, e.g.*, https://www.watchguard.com/docs/datasheet/wg_firebox_m200-m300_ds.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 to enable security services including "Intrusion Prevention Service (IPS)," "Reputation Enabled Defense Service (RED)", "Spamblocker," "Gateway Antivirus (GAV)," "Webblocker URL Filtering," "Application Control," "APT Blocker," and "Data Loss Prevention (DLP)." *See, e.g.*, https://p.widencdn.net/vm1roi/Brochure_Total_Security 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 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 to enable security services including "Intrusion Prevention

Service (IPS)," "Reputation Enabled Defense Service (RED)", "Spamblocker," "Gateway Antivirus (GAV)," "Webblocker URL Filtering," "Application Control," "APT Blocker," and "Data Loss Prevention (DLP)." *See, e.g.*, https://p.widencdn.net/vm1roi/Brochure_Total_Security 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 enables the session to be used to "Easily and quickly enforce granular policies per user, group, and schedule." Defendant's devices that perform the Accused Methods are designed to "Quickly and easily select to allow, block, or restrict access to applications based on a user's department, job function, and time of day" granularly, with "the ability to block sub-functions within applications, including file transfers, media and chat functions, and peer-to-peer connections." In addition, "Get real-time and historical visibility into the applications being used on your network, including top applications, categories, and user-specific data." *See, e.g.*, http://www.watchguard.com/wgrd-products/security-services/application-control 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. For example, even if traffic is encrypted, Defendant's devices that perform the Accused Methods decrypt the transmission to "scan the data, perform any needed security functions, and then we re-encrypt the

data before it exits the box." This scanning and security functions includes the ability to "filter and block on a whole range of characteristics (e.g., based on strict interpretation of a protocol standard; based on character strings; based on regular expressions; based on denying URLs that contain .EXE; and more" to grant "full security screening and logic on the HTTPS packet, but does not open it up to prying human eyes." This also enables the devices to "intercept and inspect VoIP-related protocols such as H.323 and Session Initiation Protocol (SIP)" "to reduce your exposure to VoIP-related risk." *See, e.g.*, http://www.watchguard.com/docs/whitepaper/wg_xtm_advantages_wp.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 Application described *supra*, which enables Defendant's devices that perform the Accused Methods to not only provide control over specific applications, but also identify and "block sub-functions within applications" such as "file transfers, media and chat functions, and peer-to-peer connections." *See, e.g.*, http://www.watchguard.com/wgrd-products/security-services/application-control 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