

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION**

PACSEC3, LLC,)	
Plaintiff,)	
)	Civil Action No. 6:20-CV-00914-ADA
v.)	
)	
NETSCOUT SYSTEMS, INC.,)	JURY TRIAL DEMANDED
Defendant.)	

PLAINTIFF’S FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT

PacSec3, LLC (“PacSec”) files this First Amended Complaint and demand for jury trial seeking relief from patent infringement of the claims of U.S. Patent Nos. 6,789,190 (“the ‘190 patent”); 7,047,564 (“the ‘564 patent”); and, 7,523,497 (“the ‘497 patent”) (collectively referred to as the “Patents-in-Suit”) by NetScout, Inc.

I. THE PARTIES

1. Plaintiff PacSec3, LLC is a Texas Limited Liability Company with its principal place of business located in Harris County, Texas.

2. On information and belief, NetScout, Inc. (“NetScout”). On information and belief, NETSCOUT sells and offers to sell products and services throughout Texas, including in this judicial district, and introduces products and services that perform infringing methods or processes into the stream of commerce knowing that they would be sold in Texas and this judicial district. NETSCOUT can be served with process through their registered agent, CT Corporation System, 155 Federal Street, Suite 700, Boston, MA 02110.

II. JURISDICTION AND VENUE

3. This Court has original subject-matter jurisdiction over the entire action pursuant to 28 U.S.C. §§ 1331 and 1338(a) because Plaintiff's claim arises under an Act of Congress relating to patents, namely, 35 U.S.C. § 271.

4. This Court also has original subject-matter jurisdiction over the entire action pursuant to 28 U.S.C. § 1332(a)(1) because Plaintiff is a limited liability company organized under the laws of the State of Texas and Defendant is a Massachusetts Corporation with a principal, physical place of business at 901 Mopac Expressway, South Barton Springs, Bldg. 1, Suite 300, Austin, Texas 78746. The matter in controversy exceeds the sum or value of \$75,000, exclusive of interest and costs.

5. This Court has personal jurisdiction over Defendant because: (i) Defendant is present within or has minimum contacts within the State of Texas and this judicial district; (ii) Defendant has purposefully availed itself of the privileges of conducting business in the State of Texas and in this judicial district; and (iii) Plaintiff's cause of action arises directly from Defendant's business contacts and other activities in the State of Texas and in this judicial district.

6. Venue is proper in this district under 28 U.S.C. §§ 1391(b) and 1400(b). Defendant has committed acts of infringement and has a regular and established place of business in this District, located at 901 Mopac Expressway, South Barton Springs, Bldg. 1, Suite 300, Austin, Texas 78746. Further, venue is proper because Defendant conducts substantial business in this forum, directly or through intermediaries, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct and/or deriving substantial revenue from goods and services provided to individuals in Texas and this District.

III. INFRINGEMENT

A. Infringement of the '190 Patent

7. On September 7, 2004, U.S. Patent No. 6,789,190 (“the ‘190 patent,” attached as Exhibit A) entitled “PACKET FLOODING DEFENSE SYSTEM,” was duly and legally issued by the U.S. Patent and Trademark Office. PacSec3, LLC owns the ‘190 patent by assignment.

8. The ‘190 patent relates to a novel and improved manner and system of defense to a data packet flood attack.

9. NETSCOUT offers for sale, sells and manufactures one or more firewall systems, including the Arbor Peakflow SP solution, that infringes one or more claims of the ‘190 patent, including one or more of claims 1-3, literally or under the doctrine of equivalents. Defendant put the inventions claimed by the ‘190 Patent into service (i.e., used them); but for Defendant’s actions, the claimed-inventions embodiments involving Defendant’s products and services would never have been put into service. Defendant’s acts complained of herein caused those claimed-invention embodiments as a whole to perform, and Defendant’s procurement of monetary and commercial benefit from it.

10. Support for the allegations of infringement may be found in the following preliminary table:

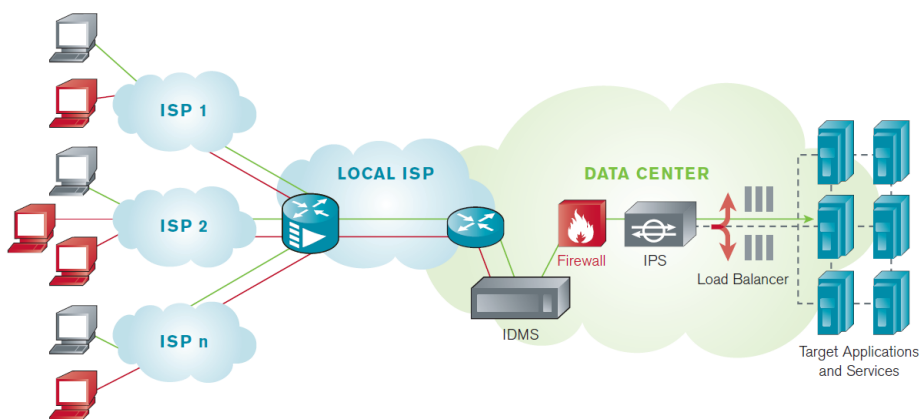
<u>Exemplary Claim language</u>	Arbor Networks Evidence
A packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said system comprising: at least	<p>In the case of DDoS attacks, Peakflow SP can detect many kinds of threats, such as bandwidth-consuming attacks (e.g., ICMP/UDP floods), connection-layer exhaustion attacks (e.g., TCP SYN floods) or attacks that target specific applications, such as HTTP, VoIP or DNS. In fact, since a majority of the world's Internet service providers use Peakflow SP, many consider it to be the de facto standard for carrier-grade DDoS attack detection and surgical mitigation.</p> <p>The Growing Threat of Application-Layer DDoS Attacks (Page 7)</p>

one firewall, said firewall comprising:

... hardware and software serving to control packet transmission between said network and a host computer connected to an internal network;

a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said system comprising: at least one firewall, said firewall comprising:

hardware and software serving to control packet transmission between said network and a host computer connected to an internal network;



Peakflow SP TMS in-line deployment

The Growing Threat of Application-Layer DDoS Attacks (page 10)

<p>... means for classifying data packets received at said firewall;...</p>	<p>In this case, the operator can use the "SIP request-limiting countermeasure" to limit the number of SIP request messages per second that are sent to the SIP proxy server. Once the operator enables this countermeasure, packets from IP addresses (called hosts) exceeding this rate are dropped and the hosts are blacklisted.</p> <p>The Growing Threat of Application-Layer DDoS Attacks (page 17)</p> <p>The reference describes means for classifying data packets received at said firewall [packets from IP addresses (called hosts) exceeding this rate are dropped and the hosts are blacklisted].</p>
<p>means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall;</p>	<p>The reference describes means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall</p> <p>The IDMS must have the ability to detect attacks using multiple techniques. These include statistical anomaly detection; detection of protocol violations or malformed packets; customizable thresholds or ability to detect security policy violations; and signatures of known or emerging threats that are based upon network behavioral patterns, not binary patterns in packets.</p> <p>The Growing Threat of Application-Layer DDoS Attacks (page 7)</p>
<p>means for said firewall to find information for packets it receives regarding the path by which said packets came to said firewall; and</p>	<p>In diversion/reinjection mode, TMS is deployed within the network and is not in-line of normal traffic flow. When a mitigation is initiated, a Border Gateway Protocol (BGP) route is announced, which must be preferred by the network, so that traffic matching the route is diverted through the TMS appliance. TMS then removes the attack traffic and good traffic is re-injected back into the normal network path for delivery to the customer/service.</p> <p>The Growing Threat of Application-Layer DDoS Attacks (page 9)</p>

<p>whereby, said firewall can use said information to allocate the transmission rate for each class in a desired way.</p>	<p>A unique feature of the decode display of Peakflow SP TMS (noticeable in the screen shot above) is the ability to see the source and destination country of each packet. This is useful information for attack mitigation. In fact, "GeoIP attack countermeasures" can be used to block or rate-limit traffic coming from specific countries.</p> <p>The Growing Threat of Application-Layer DDoS Attacks (page 15)</p>
---	---

These allegations of infringement are preliminary and are therefore subject to change.

11. NETSCOUT has and continues to induce infringement. NETSCOUT has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., question and answer services on the Internet) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–3 of the ‘190 patent, literally or under the doctrine of equivalents. Moreover, NETSCOUT has known of the ‘190 patent and the technology underlying it from at least the date of issuance of the patent.

12. NETSCOUT has and continues to contributorily infringe. NETSCOUT has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., question and answer services on the Internet) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–3 of the ‘190 patent, literally or under the doctrine of equivalents. Moreover, NETSCOUT has known of the ‘190 patent and the technology underlying it from at least the date of issuance of the patent.

13. NETSCOUT has caused and will continue to cause PacSec3 damage by direct and indirect infringement of (including inducing infringement of) the claims of the '190 patent.

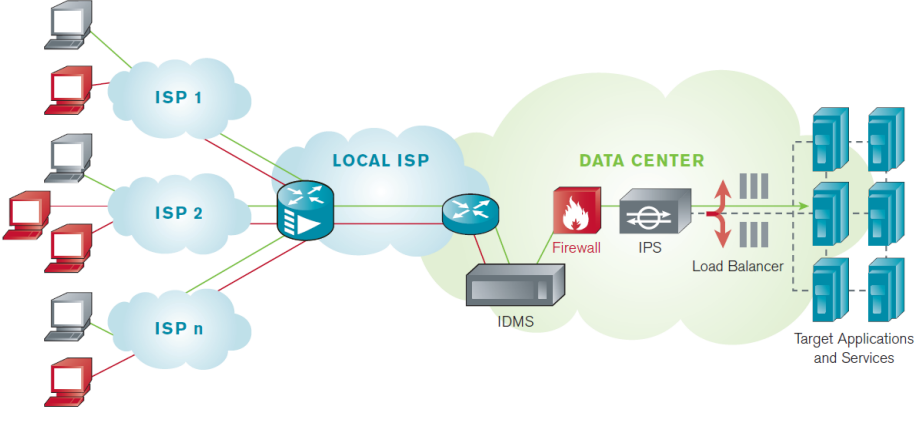
B. Infringement of the '564 Patent

14. On May 16, 2006, U.S. Patent No. 7,047,564 (“the ‘564 patent”, attached as Exhibit B) entitled “REVERSE FIREWALL PACKET TRANSMISSION CONTROL SYSTEM,” was duly and legally issued by the U.S. Patent and Trademark Office. PacSec3, LLC owns the ‘564 patent by assignment.

15. The ‘564 patent relates to a novel and improved manner and system of defense to a data packet flood attack.

16. NETSCOUT offers for sale, sells and manufactures one or more firewall systems, including the Arbor Peakflow SP solution, that infringes one or more claims of the ‘564 patent, including one or more of claims 1-6, literally or under the doctrine of equivalents. Defendant put the inventions claimed by the ‘564 Patent into service (i.e., used them); but for Defendant’s actions, the claimed-inventions embodiments involving Defendant’s products and services would never have been put into service. Defendant’s acts complained of herein caused those claimed-invention embodiments as a whole to perform, and Defendant’s procurement of monetary and commercial benefit from it.

17. Support for the allegations of infringement may be found in the following preliminary table:

<p><u>Exemplary Claim language</u></p>	<p>Arbor Networks Evidence</p>
<p>A packet transmission control system for managing traffic between at least two data networks, each of said networks comprising a plurality of host computers, communication lines and transmitted data packets, said system comprising:</p>	<p>Arbor Networks: Peakflow SP TMS has a packet transmission control system for managing traffic between at least two data networks, each of said networks comprising a plurality of host computers, communication lines and transmitted data packets.</p>
<p>at least one firewall, said firewall comprising:</p> <p>hardware and software providing a non-redundant connection between said networks and serving to control packet transmission between said networks;</p>	 <p><i>Peakflow SP TMS in-line deployment</i></p> <p>The Growing Threat of Application-Layer DDoS Attacks (page 10)</p>
<p>means for classifying data packets received at said firewall</p>	

<p>related to the consumption of at least one resource;</p>	<p>In this case, the operator can use the "SIP request-limiting countermeasure" to limit the number of SIP request messages per second that are sent to the SIP proxy server. Once the operator enables this countermeasure, packets from IP addresses (called hosts) exceeding this rate are dropped and the hosts are blacklisted.</p> <p>The Growing Threat of Application-Layer DDoS Attacks (page 17)</p> <p>The reference describes means for classifying data packets received at said firewall [packets from IP addresses (called hosts) exceeding this rate are dropped and the hosts are blacklisted].</p>
<p>means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall;</p>	<p>The reference describes means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall</p> <p>The IDMS must have the ability to detect attacks using multiple techniques. These include statistical anomaly detection; detection of protocol violations or malformed packets; customizable thresholds or ability to detect security policy violations; and signatures of known or emerging threats that are based upon network behavioral patterns, not binary patterns in packets.</p> <p>The Growing Threat of Application-Layer DDoS Attacks (page 7)</p>
<p>means for limiting the transmission rate from the firewall to the maximum acceptable transmission rate for each class of data packet; and</p>	<p>A unique feature of the decode display of Peakflow SP TMS (noticeable in the screen shot above) is the ability to see the source and destination country of each packet. This is useful information for attack mitigation. In fact, "GeoIP attack countermeasures" can be used to block or rate-limit traffic coming from specific countries.</p> <p>The Growing Threat of Application-Layer DDoS Attacks (page 15)</p> <p>The reference describes means for limiting the transmission rate from the firewall to the maximum acceptable transmission rate for each class of data packet ["GeoIP attack countermeasures" can be used to block or rate-limit traffic coming from specific countries].</p>

<p>whereby, packet flooding and other over usage type distributed denial of service attacks cannot be effectively launched through said non-redundant connection.</p>	<p>In the case of DDoS attacks, Peakflow SP can detect many kinds of threats, such as bandwidth-consuming attacks (e.g., ICMP/UDP floods), connection-layer exhaustion attacks (e.g., TCP SYN floods) or attacks that target specific applications, such as HTTP, VoIP or DNS. In fact, since a majority of the world's Internet service providers use Peakflow SP, many consider it to be the de facto standard for carrier-grade DDoS attack detection and surgical mitigation.</p> <p>The Growing Threat of Application-Layer DDoS Attacks (Page 7)</p> <p>The reference describes packet flooding and other over usage type distributed denial of service attacks cannot be effectively launched through said non-redundant connection</p>
---	---

These allegations of infringement are preliminary and are therefore subject to change.

18. NETSCOUT has and continues to induce infringement. NETSCOUT has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., question and answer services on the Internet) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–6 of the '564 patent, literally or under the doctrine of equivalents. Moreover, NETSCOUT has known of the '564 patent and the technology underlying it from at least the date of issuance of the patent.

19. NETSCOUT has and continues to contributorily infringe. NETSCOUT has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., question and answer services on the Internet) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–6 of the '564 patent, literally or under

the doctrine of equivalents. Moreover, NETSCOUT has known of the '564 patent and the technology underlying it from at least the date of issuance of the patent.

20. NETSCOUT has caused and will continue to cause PacSec3 damage by direct and indirect infringement of (including inducing infringement of) the claims of the '564 patent.

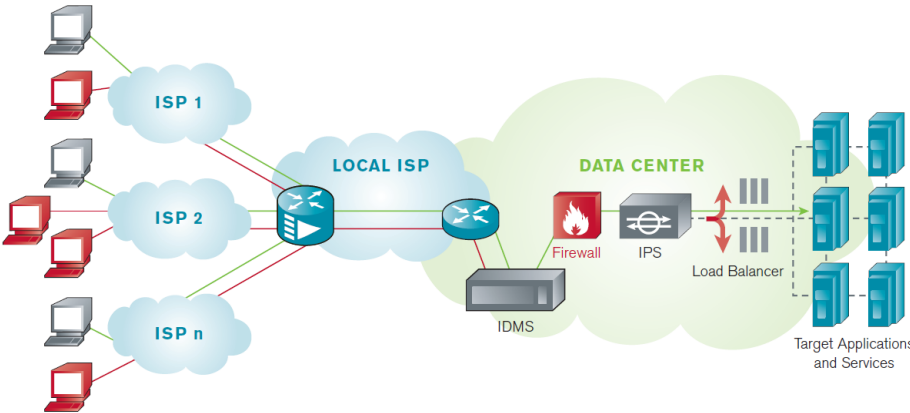
C. Infringement of the '497 Patent

21. On April 21, 2009, U.S. Patent No. 7,523,497 ("the '497 patent", attached as Exhibit C) entitled "PACKET FLOODING DEFENSE SYSTEM," was duly and legally issued by the U.S. Patent and Trademark Office. PacSec3, LLC owns the '497 patent by assignment.

22. The '497 patent relates to a novel and improved manner and system of defense to a data packet flood attack.

23. NETSCOUT offers for sale, sells and manufactures one or more firewall systems, including the Arbor Peakflow SP solution, that infringes one or more claims of the '497 patent, including one or more of claims 1-18, literally or under the doctrine of equivalents. Defendant put the inventions claimed by the '497 Patent into service (i.e., used them); but for Defendant's actions, the claimed-inventions embodiments involving Defendant's products and services would never have been put into service. Defendant's acts complained of herein caused those claimed-invention embodiments as a whole to perform, and Defendant's procurement of monetary and commercial benefit from it.

24. Support for the allegations of infringement may be found in the following preliminary table:

<p><u>Exemplary Claim language</u></p>	<p>Arbor Networks Evidence</p>
<p>A method of providing packet flooding defense for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said method comprising the steps of:</p>	<p>In the case of DDoS attacks, Peakflow SP can detect many kinds of threats, such as bandwidth-consuming attacks (e.g., ICMP/UDP floods), connection-layer exhaustion attacks (e.g., TCP SYN floods) or attacks that target specific applications, such as HTTP, VoIP or DNS. In fact, since a majority of the world's Internet service providers use Peakflow SP, many consider it to be the de facto standard for carrier-grade DDoS attack detection and surgical mitigation.</p> <p>The Growing Threat of Application-Layer DDoS Attacks (Page 7)</p>  <p><i>Peakflow SP TMS in-line deployment</i></p> <p>The Growing Threat of Application-Layer DDoS Attacks (page 10)</p>
<p>determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer; said path comprising all routers in said network via which said packets are</p>	<p>The Arbor Peakflow SP solution is a network-wide infrastructure security and traffic monitoring platform. By leveraging IP flow data (i.e., NetFlow, sFlow, etc.) and information from deep packet inspection (DPI), Peakflow SP provides pervasive and cost-effective network and application-layer visibility. As Peakflow SP gathers this information, it learns normal traffic and routing behavior across hundreds of routers and thousands of interfaces, and correlates the traffic patterns with the topology data to build logical data models. Armed with this information, Peakflow SP notifies network operations staff of significant changes to the network (a.k.a. network anomalies)—regardless of whether they are due to misconfiguration, equipment failure or a DDoS attack.</p>

<p>routed to said computer;</p>	<p>The reference describes determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer</p>
<p>classifying data packets received at said host computer into wanted data packets and unwanted data packets by path;</p>	<p>The reference describes classifying data packets received at said host computer into wanted data packets and unwanted data packets by path</p> <p>In this case, the operator can use the "SIP request-limiting countermeasure" to limit the number of SIP request messages per second that are sent to the SIP proxy server. Once the operator enables this countermeasure, packets from IP addresses (called hosts) exceeding this rate are dropped and the hosts are blacklisted.</p> <p>The Growing Threat of Application-Layer DDoS Attacks (page 17)</p>
<p>associating a maximum acceptable processing rate with each class of data packet received at said host computer; and</p>	<p>A unique feature of the decode display of Peakflow SP TMS (noticeable in the screen shot above) is the ability to see the source and destination country of each packet. This is useful information for attack mitigation. In fact, "GeolP attack countermeasures" can be used to block or rate-limit traffic coming from specific countries.</p> <p>The Growing Threat of Application-Layer DDoS Attacks (page 15)</p> <p>The reference describes associating a maximum acceptable processing rate with each class of data packet received at said host computer</p>
<p>allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets.</p>	<p>A unique feature of the decode display of Peakflow SP TMS (noticeable in the screen shot above) is the ability to see the source and destination country of each packet. This is useful information for attack mitigation. In fact, "GeolP attack countermeasures" can be used to block or rate-limit traffic coming from specific countries.</p> <p>The Growing Threat of Application-Layer DDoS Attacks (page 15)</p>

These allegations of infringement are preliminary and are therefore subject to change.

25. NETSCOUT has and continues to induce infringement. NETSCOUT has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., question and answer services on the Internet) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–18 of the ‘497 patent, literally or under the doctrine of equivalents. Moreover, NETSCOUT has known of the ‘497 patent and the technology underlying it from at least the date of issuance of the patent.

26. NETSCOUT has and continues to contributorily infringe. NETSCOUT has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., question and answer services on the Internet) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–18 of the ‘497 patent, literally or under the doctrine of equivalents. Moreover, NETSCOUT has known of the ‘497 patent and the technology underlying it from at least the date of issuance of the patent.

27. NETSCOUT has caused and will continue to cause PacSec3 damage by direct and indirect infringement of (including inducing infringement of) the claims of the ‘497 patent.

IV. JURY DEMAND

PacSec3 hereby requests a trial by jury on issues so triable by right.

V. PRAYER FOR RELIEF

WHEREFORE, PacSec3 prays for relief as follows:

- a. enter judgment that Defendant has infringed the claims of the '190 patent, the '564 patent and the '497 patent through selling, offering for sale, manufacturing, and inducing others to infringe by using and instructing to use at least the Arbor Peakflow SP solution, and perhaps other firewall systems;
- b. award PacSec3 damages in an amount sufficient to compensate it for Defendant's infringement of the Patents-in-Suit in an amount no less than a reasonable royalty or lost profits, together with pre-judgment and post-judgment interest and costs under 35 U.S.C. § 284;
- c. award PacSec3 an accounting for acts of infringement not presented at trial and an award by the Court of additional damage for any such acts of infringement;
- d. declare this case to be "exceptional" under 35 U.S.C. § 285 and award PacSec3 its attorneys' fees, expenses, and costs incurred in this action;
- e. declare Defendant's infringement to be willful and treble the damages, including attorneys' fees, expenses, and costs incurred in this action and an increase in the damage award pursuant to 35 U.S.C. § 284;
- f. a decree addressing future infringement that either (i) awards a permanent injunction enjoining Defendant and its agents, servants, employees, affiliates, divisions, and subsidiaries, and those in association with Defendant from infringing the claims of the Patents-in-Suit, or (ii) awards damages for future infringement in lieu of an injunction in an amount consistent with the fact that for future infringement the Defendant will be an adjudicated infringer of a valid patent, and trebles that amount in view of the fact that the future infringement will be willful as a matter of law; and
- g. award PacSec3 such other and further relief as this Court deems just and proper.

Respectfully submitted,

Ramey & Schwaller, LLP

/s/William P. Ramey
William P. Ramey, III
Texas Bar No. 24027643
5020 Montrose Blvd., Suite 800
Houston, Texas 77006
(713) 426-3923 (telephone)
(832) 900-4941 (fax)
wramey@rameyfirm.com

Attorneys for PacSec3, LLC

CERTIFICATE OF SERVICE

Pursuant to the Federal Rules of Civil Procedure, I hereby certify that all counsel of record who have appeared in this case are being served on this day of January 5, 2021, with a copy of the foregoing via the Court's CM/ECF.

/s/ William P. Ramey, III
William P. Ramey, III