

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

<b>PACSEC3, LLC,</b>	)	
<b>Plaintiff,</b>	)	
	)	<b>Civil Action No. 6:22-cv-00129</b>
<b>v.</b>	)	
	)	
<b>CLOUDFLARE, INC.,</b>	)	<b>JURY TRIAL DEMANDED</b>
<b>Defendant.</b>	)	

**PLAINTIFF’S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT**

PacSec3, LLC (“PacSec”) files this Original Complaint and demand for jury trial seeking relief from patent infringement of the claims of U.S. Patent No. 7,523,497 (“the ‘497 patent”) (referred to as the “Patent-in-Suit”) by Cloudflare, Inc. (“Cloudflare”).

**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, Cloudflare is a corporation organized under the laws of the State of Delaware with a regular and established place of business at 106 East 6th Street, Suites 350 and 400, Austin, TX 78701. On information and belief, CLOUDFLARE 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. CLOUDFLARE can be served with process through their registered agent Registered Agent Solutions, Inc., Corporate Center One, 5301 Southwest Parkway, Suite 400, Austin, TX 78735 or wherever they may be found.

**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 Patent, namely, 35 U.S.C. § 271.

4. 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.

5. 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. 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 OF THE '497 PATNET**

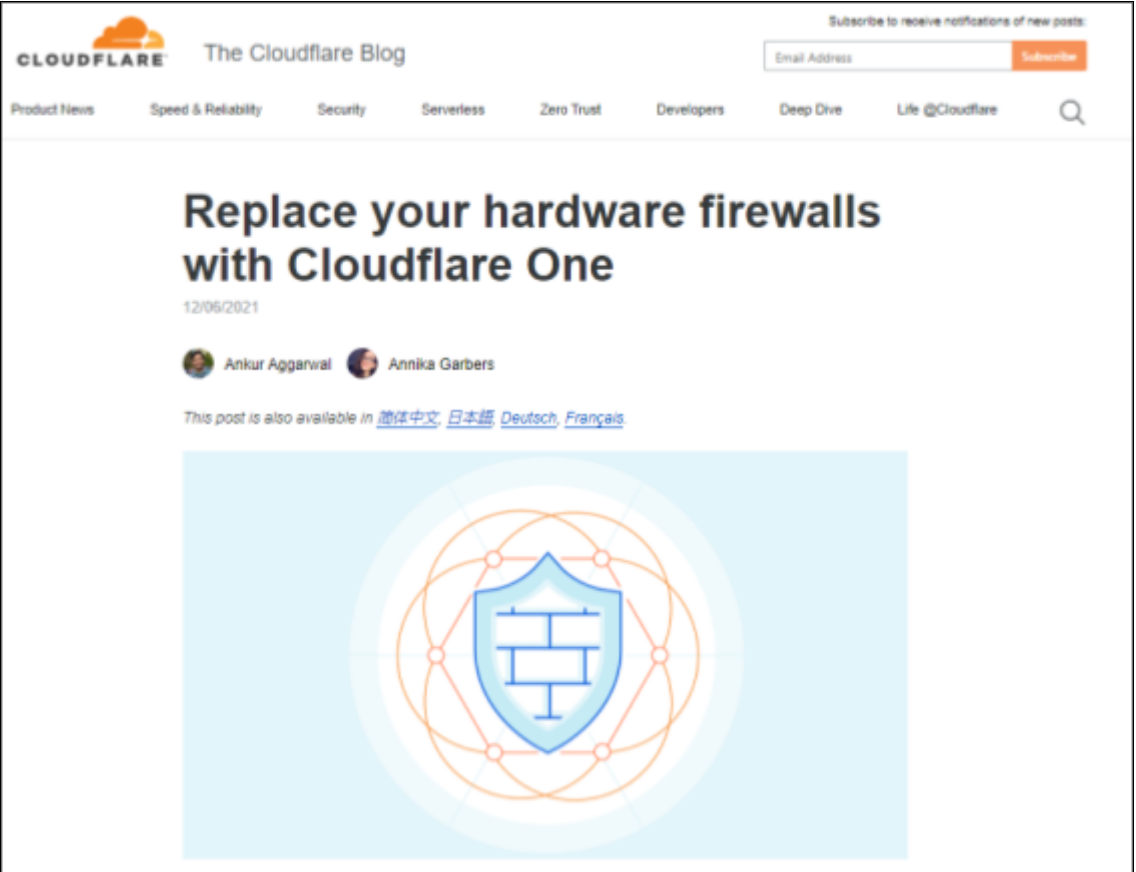
6. On April 21, 2009, U.S. Patent No. 7,523,497 ("the '497 patent", included as an attachment) entitled "PACKET FLOODING DEFENSE SYSTEM," was duly and legally issued by the U.S. Patent and Trademark Office. PacSec3, LLC owns the '497 patent by assignment.

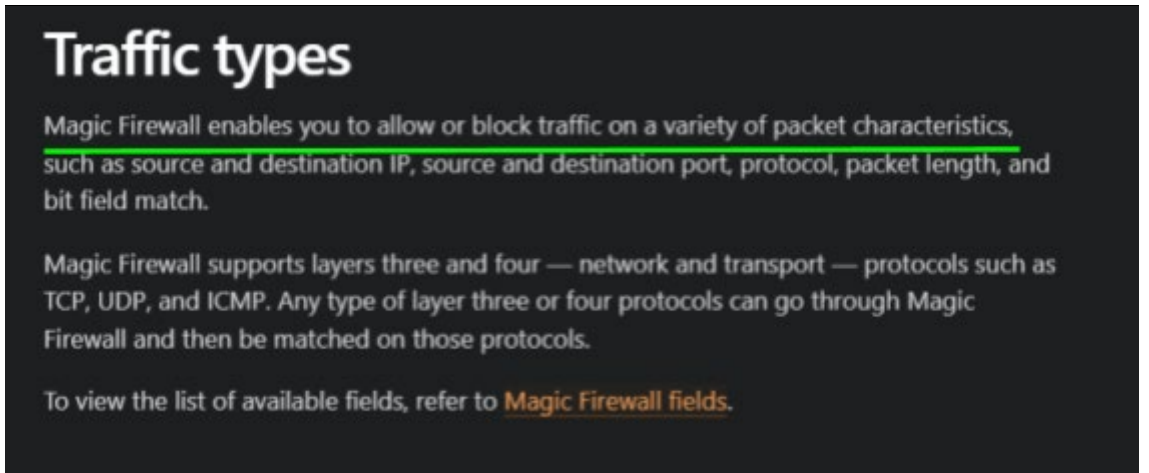
7. The '497 patent relates to a novel and improved manner and system of defense to a data packet flood attack.

8. CLOUDFLARE offers for sale, sells and manufactures one or more firewall systems 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.

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

US7523497 B2 Claim 7	Cloudflare One
<p>7. 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>The screenshot shows the Cloudflare Blog interface. At the top, there's a navigation bar with the Cloudflare logo, 'The Cloudflare Blog' title, a subscribe form, and various category links like 'Product News', 'Speed &amp; Reliability', 'Security', 'Serverless', 'Zero Trust', 'Developers', 'Deep Dive', and 'Life @Cloudflare'. The main content area features a large heading 'Replace your hardware firewalls with Cloudflare One' with a date of '12/06/2021'. Below the title are the authors' names, 'Ankur Aggarwal' and 'Annika Garbers', and a note that the post is available in multiple languages: 'This post is also available in 简体中文, 日本語, Deutsch, Français'. The central image is a light blue square containing a circular graphic with a shield in the center, symbolizing network security.</p>

	<p>Cloudflare One has a packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets.</p> <p>The reference includes subject matter disclosed by the claims of the patent after the priority date. "In November of 2009, Cloudflare closed its Series A financing with Ray Rothrock, from Venrock, and Carl Ledbetter, from Pelion Venture Partners." <a href="https://www.cloudflare.com/our-story/">https://www.cloudflare.com/our-story/</a></p> <p>The venue of the company is:</p> <p>McAllen, TX, United States - (MFE) <a href="https://blog.cloudflare.com/mcallen/">https://blog.cloudflare.com/mcallen/</a></p> <p>Houston, TX, United States - (IAH) <a href="https://blog.cloudflare.com/usa-expansion/">https://blog.cloudflare.com/usa-expansion/</a></p> <p>Dallas, TX, United States - (DFW) <a href="https://www.cloudflarestatus.com/">https://www.cloudflarestatus.com/</a></p>
<b>US7523497 B2 Claim 7</b>	<b>Cloudflare One</b>
<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 routed to said computer;</p>	 <p>The screenshot shows a dark-themed document titled "Traffic types". The text describes the Magic Firewall's ability to allow or block traffic based on various packet characteristics, including source and destination IP, port, protocol, packet length, and bit field match. It also mentions that Magic Firewall supports layers three and four (network and transport) protocols like TCP, UDP, and ICMP. A link is provided to view the list of available fields: "Magic Firewall fields".</p> <p><a href="https://developers.cloudflare.com/magic-firewall/about/traffic-types">https://developers.cloudflare.com/magic-firewall/about/traffic-types</a></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; said path comprising all routers in said network via which said packets are routed to said computer.</p>

<b>US7523497 B2 Claim 7</b>	<b>Cloudflare One</b>
classifying data packets received at said host computer into wanted data packets and unwanted data packets by path;	<div data-bbox="396 275 1479 527" style="border: 1px solid red; padding: 10px;"> <p>We built flowtrackd, which runs autonomously on each server at our network's edge. <u>flowtrackd is able to classify the state of TCP flows by analyzing only the ingress traffic, and then drops, challenges, or rate-limits attack packets that do not correspond to an existing flow.</u></p> </div> <p><a href="https://blog.cloudflare.com/beat-an-acoustics-inspired-ddos-attack/">https://blog.cloudflare.com/beat-an-acoustics-inspired-ddos-attack/</a>  The reference describes classifying data packets received at said host computer into wanted data packets and unwanted data packets by path.</p>
<b>US7523497 B2 Claim 7</b>	<b>Cloudflare One</b>
associating a maximum acceptable processing rate with each class of data packet received at said host computer; and	<div data-bbox="396 1125 1479 1556" style="border: 1px solid orange; padding: 10px;"> <p><b>Overview</b></p> <p>Cloudflare <b>Rate Limiting</b> automatically identifies and mitigates excessive request rates for <u>specific URLs or for an entire domain</u>. Request rates are calculated locally for individual Cloudflare data centers. The most common uses for <b>Rate Limiting</b> are <b>DDoS</b> protection, <b>Brute-force attack</b> protection, and to limit access to forum searches, API calls, or resources that involve database-intensive operations at your origin.</p> <p>Once an individual IPv4 address or IPv6 /64 IP range exceeds a rule threshold, further requests to the origin web server are blocked with an HTTP 429 response that includes a <b>Retry-After</b> header to indicate when the client can resume sending requests.</p> </div> <p><a href="https://support.cloudflare.com/hc/en-us/articles/115001635128-Configuring-Cloudflare-Rate-Limiting">https://support.cloudflare.com/hc/en-us/articles/115001635128-Configuring-Cloudflare-Rate-Limiting</a>  The reference describes associating a maximum acceptable processing rate with each class of data packet received at said host computer.</p>

<b>US7523497 B2 Claim 7</b>	<b>Cloudflare One</b>
<p>allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets.</p>	<div data-bbox="394 342 1505 762"> <p><b>Overview</b></p> <p>Cloudflare <b>Rate Limiting</b> automatically identifies and mitigates excessive request rates for specific URLs or for an entire domain. Request rates are calculated locally for individual Cloudflare data centers. The most common uses for <b>Rate Limiting</b> are <b>DDoS</b> protection, <b>Brute-force attack</b> protection, and to limit access to forum searches, API calls, or resources that involve database-intensive operations at your origin.</p> <p>Once an individual IPv4 address or IPv6 /64 IP range exceeds a rule threshold, further requests to the origin web server are blocked with an HTTP 429 response that includes a <b>Retry-After</b> header to indicate when the client can resume sending requests.</p> </div> <p><a href="https://support.cloudflare.com/hc/en-us/articles/115001635128-Configuring-Cloudflare-Rate-Limiting">https://support.cloudflare.com/hc/en-us/articles/115001635128-Configuring-Cloudflare-Rate-Limiting</a></p> <div data-bbox="394 856 1505 1287"> <p><b>Overview</b></p> <p>Cloudflare <b>Rate Limiting</b> automatically identifies and mitigates excessive request rates for specific URLs or for an entire domain. Request rates are calculated locally for individual Cloudflare data centers. The most common uses for <b>Rate Limiting</b> are <b>DDoS</b> protection, <b>Brute-force attack</b> protection, and to limit access to forum searches, API calls, or resources that involve database-intensive operations at your origin.</p> <p>Once an individual IPv4 address or IPv6 /64 IP range exceeds a rule threshold, further requests to the origin web server are blocked with an HTTP 429 response that includes a <b>Retry-After</b> header to indicate when the client can resume sending requests.</p> </div> <p><a href="https://support.cloudflare.com/hc/en-us/articles/115001635128-Configuring-Cloudflare-Rate-Limiting">https://support.cloudflare.com/hc/en-us/articles/115001635128-Configuring-Cloudflare-Rate-Limiting</a></p> <p>The reference describes allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets..</p>

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

10. CLOUDFLARE has and continues to induce infringement. CLOUDFLARE 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., DDOS protection systems) 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, CLOUDFLARE has known of the ‘497 patent and the technology underlying it from at least the filing date of the lawsuit.<sup>1</sup> For clarity, direct infringement is previously alleged in this complaint.

11. CLOUDFLARE has and continues to contributorily infringe. CLOUDFLARE 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., DDOS protection systems) 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. Further, there are no substantial noninfringing uses for Defendant’s products and services. Moreover, CLOUDFLARE has known of the ‘497 patent and the technology underlying it from at least the filing date of the lawsuit.<sup>2</sup> For clarity, direct infringement is previously alleged in this complaint.

12. CLOUDFLARE 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 DDOS protection systems;

---

<sup>1</sup> Plaintiff reserves the right to amend if discovery reveals an earlier date of knowledge.

<sup>2</sup> Plaintiff reserves the right to amend if discovery reveals an earlier date of knowledge.

- b. award PacSec3 damages in an amount sufficient to compensate it for Defendant's infringement of the Patent-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 (if) 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 Patent-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*