UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

TOUCHPOINT PROJECTIONS INNOVATIONS, LLC, Plaintiff, v. **CLOUDFLARE, INC.,** Defendant.	**CASE NO. 2:24-cv-00343** **JURY TRIAL DEMANDED**

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Touchpoint Projection Innovations, LLC (hereinafter "Touchpoint"), by and through its undersigned attorneys, files this Complaint for Patent Infringement against Defendant Cloudflare, Inc. and alleges as follows.

NATURE OF ACTION

1. This is an action for infringement of United States Letters Patent No. 8,265,089 under the Patent Laws of the United States, 35 U.S.C. § 1, *et seq*[1].

THE PARTIES

2. Plaintiff Touchpoint is a limited liability company organized and existing under the laws of the State of Wyoming with its principal place of business at 1712 Pioneer Ave Suite 500, Cheyenne, Wyoming 82001. Touchpoint is in the business of licensing patented technology.

[1] The Patent-in-Suit does not expire until August 10, 2030, according to third party Google. *See* https://patents.google.com/patent/US8265089B2/en?oq=8265089, as last visited on May 2, 2024.

Touchpoint is the assignee of all right, title, and interest in United States Letters Patent No. 8,265,089.

3. On information and belief, Defendant Cloudflare, Inc. ("Defendant") has its headquarters in Austin, Texas, that directly and/or through its subsidiaries, affiliates, and agents, in the Eastern District of Texas.

JURISDICTION

4. The claims in this action arise under the Patent Laws of the United States, Title 35 of the United States Code. Accordingly, this Court has subject matter jurisdiction over the patent infringement claims in this action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

5. Defendant is subject to this Court's specific and general personal jurisdiction pursuant to the Texas Long Arm Statute, due at least to its substantial business conducted in this forum, directly and/or through one or more of its subsidiaries, affiliates, and/or intermediaries, including (i) having solicited business in the State of Texas, transacted business within the State of Texas, and/or attempted to derive financial benefit from residents of the State of Texas, including benefits directly related to the instant patent infringement causes of action set forth herein; (ii) having placed products and services into the stream of commerce throughout the United States and having been actively engaged in transacting business in Texas and in this District; and (iii) either alone or in conjunction with others, having committed acts of infringement within this District and/or induced others to commit acts of infringement within this District. Defendant has, directly and/or through a distribution network, purposefully and voluntarily placed infringing products and services in the stream of commerce knowing and expecting them to be purchased and used by consumers in Texas and in this District.

6. On information and belief, Defendant, directly and/or through one or more agent-subsidiaries, affiliates, and/or intermediaries, has advertised and continues to advertise (including through websites), used, offered to sell, sold, distributed, and/or induced the sale and/or use of infringing products and services in the United States and in this District. Defendant has, directly and/or through a distribution network, purposefully and voluntarily placed such products and services in the stream of commerce via established channels knowing and expecting them to be purchased and used by consumers in the United States and this District. Defendant has committed acts of direct infringement in Texas and/or committed indirect infringement based on acts of direct infringement by others in Texas and in this District, including Defendant's customer end-users.

7. On information and belief, Cloudflare's Insights is used in just the Plano area by at least 197 users, including Cinemark.com, plano.gov, disabilityover50.com, and many others as available, as last visited on May 2, 2024, at https://trends.builtwith.com/websitelist/Cloudflare-Insights/United-States/Texas/Plano.

Websites using Cloudflare Insights in Plano

Download a list of all 197 Current Cloudflare Insights Customers in Plano

Website	Location	Sales Revenue	Tech Spend	Social	Employees	Traffic
cinemark.com	United States		$2000+	20,000+	10,000+	High
justice-docs.tylerhost.net	United States		$10000+			Medium
arc.aiaa.org	United States		$5000+	2,000+		High
myfaithvotes.org	United States	$1k+	$1000+	5,000+	10+	-
funclub.livinglocurto.com	United States		$500+	5,000+		Medium
plano.gov	United States		$1000+	2,000+		Medium
qr.childrens.com	United States	$818k+	$10000+	10,000+	1,000+	Medium
letsgo.dreamtrips.com	United States		$2000+	10,000+		-
signazon.com	United States	$149k+	$250+	500+		Medium
iscsales.com	United States	$238k+	$1000+			Medium
prestonwood.org	United States		$1000+	5,000+		Medium
disabilityover50.com	United States		$250+			-
blog.armor.com	United States		$10000+	5,000+		Medium
give-a-con.vanillasoft.com	United States		$2000+	10,000+	10+	-
villagehealthpartners.com	United States		$100+			-

197 Results in this Full Report.We know of 1,688,036 live sites using Cloudflare Insights and 1,781,799 sites in total including historical. · Page 1 of 14

Figure 1 – Screenshot from website as last visited on May 2, 2024, at https://trends.builtwith.com/websitelist/Cloudflare-Insights/United-States/Texas/Plano.

8. On information and belief, Defendant, directly or through its U.S.-based sales subsidiary, owns, maintains, and/or operates points-of-presence and/or edge computing sites throughout the United States, including in Texas and in this District, through which customer end-users can access Defendant's network, products, and services. On information and belief, Defendant's utilizes points-of-presence and/or edge computing sites in Texas are located at 6653 Pinecrest Drive, Plano, Texas 75024 and 1950 N Stemmons Freeway, Dallas, Texas 75207.

9. On information and belief, Defendant, alone and through the activities of at least its U.S.-based sales subsidiary, conducts business in the United States, including advertising, using, offering to sell, distributing, and selling infringing products in this District. Defendant, places infringing products and services into the stream of commerce via established channels knowing or understanding that such services would be offered for sale, sold, and/or used in the United States, including in the State of Texas. The exercise of jurisdiction over Defendant would therefore not offend the traditional notions of fair play and substantial justice.

10. Specific Jurisdiction is proper over Defendant under the Federal Circuit's test laid out in *SnapRays, LLC v. Lighting Def. Grp. LLC*, No. 2023-1184 (Fed. Cir. May 2, 2024).

11. Here, the Defendant (1) purposefully directed its activities at residents of the forum; (2) the claim arises out of or relates to the defendant's activities with the forum; and (3) the assertion of personal jurisdiction is reasonable and fair. On information and belief, Cloudflare reported in its Form S-1 filing that their technology was "used by, or for the benefit of, certain individuals or entities" that were blacklisted due to the United States economic and trade sanction regulations. Additionally, Defendant has a multitude of customers in this District using the infringing

technology as well as customers outside this District, including utilizing computing sites in Texas are located at 6653 Pinecrest Drive, Plano, Texas 75024 and 1950 N Stemmons Freeway, Dallas, Texas 75207, alleged on information and belief subject to verification with venue discovery if denied.

VENUE

12. Venue is proper in this judicial district under 28 U.S.C. § 1391(b) because of the actions of Defendant. *See SnapRays, LLC v. Lighting Def. Grp. LLC,* No. 2023-1184 (Fed. Cir. May 2, 2024).

13. Venue is proper in this judicial district under 28 U.S.C. § 1400(b) because Defendant ratifies businesses located within this district including the ones listed above through the direction and control implemented by Defendant over its users identified above.

THE PATENT IN SUIT

14. On September 11, 2012, United States Letters Patent No. 8,265,089 (hereinafter "the '089 Patent"), entitled "NETWORK GATEWAY WITH ENHANCED REQUESTING," was duly and legally issued by the United States Patent & Trademark Office. A copy of the '089 Patent is attached hereto as Exhibit 1.

15. The '089 Patent issued from U.S. Patent Application Number 12/636,955, which was filed on December 14, 2009. The inventors of the '089 Patent assigned all of their rights, title, and interest in and to the '089 Patent to Everis, Inc. and Everis, Inc. assigned its entire right, title, and interest in and to the '089 Patent to Touchpoint.

16. Touchpoint is the current and sole owner of all rights, title and interest in and to the ’089 Patent and, at a minimum, of all substantial rights in the ’089 Patent, including the exclusive right to enforce the patent and all rights to pursue past, present and future damages and to seek and obtain injunctive or any other relief for infringement of the ’089 Patent.

17. Upon information and belief, Defendant has had actual notice of the ’089 Patent and Defendant’s infringing activities since at least March 5, 2023.

Overview of the Technology

18. The ’089 Patent relates to communication networks for transmitting packets of data from a sender computer to a receiver computer. These data communication networks include a gateway connecting a connection-based wide area network (“WAN”) to a connectionless local area network (“LAN”).

19. As described in the specification of the ‘089 patent, conventional types of data communication networks include: (i) connection-based networks; and (ii) connectionless networks. Often, but not necessarily, WANs are connectionless. Often, but not necessarily, LANs are connection based. Conventionally, a computer or set of computers, called a gateway, can be used to pass communications in both directions between a connectionless network and a connection-based network. Some conventional connection-oriented WAN protocols include SONET, ATM, and DSC. Two conventional connectionless protocols are TCP and UDP.

20. When data is sent from a sender computer to a receiver computer, it will conventionally go through a series of networks. For example, the data may be sent first through a connectionless LAN (the sender-side LAN), and then through a connection-oriented WAN, and then through another connectionless LAN (the receiver side LAN) before reaching the receiver computer. Along

the way, the data is generally bundled with other data as it travels away from the sender computer, and then unbundled again as it gets toward the receiver computer.

The Patented Invention

21. FIG. 1 of the '089 Patent shows a data communication system **100** including a connection-based network **102**; a gateway **103**; a first connectionless network **108**; a second connectionless network **110**; a third connectionless network **112**; and communicator computers **114**, **116**, **118**, **120**, **122**, **124**, **126**, and **128**. The gateway includes a gateway computer **104** and a rules database **106**. Generally speaking, all of the communicator computers can communicate with each other, in both directions, through the connectionless and connection-based networks. For purposes of the following discussion, communicator computer **114** (also referred to as the sender computer) sends a packet through the first connectionless network (which also may be referred to as the sender side connectionless network), then through the connection based network, then through the gateway computer, then through the third connectionless network (also called the receiver side connectionless network) and finally to communicator computer **126** (also referred to as the receiver computer).

22. As shown in FIG. 2 of the '089 Patent, the gateway computer **104** includes a gateway module **150**. The gateway module includes a de-encapsulation sub-module **160** and a packet send sub-module **162**.

23. Referring to FIGS. 1 and 2 of the '089 Patent, in the gateway module of the gateway computer, the de-encapsulation sub-module receives the MPDU from connection-based network **102** and removes the MPDU header in order to break the MPDU up into its constituent data packets (which each have their own data packet headers). As in conventional data communication systems, the de-encapsulation sub-module effectively discards the MPDU header

so that its network protocol data (for example, its low-level network protocol data) is lost. The packets are then sent to the packet send sub-module, and from there they are sent into the receiver side connectionless network **112**. It is noted that because these packets still have their packet headers, they still have some network protocol data (for example, high level network protocol data), which network protocol data is generally sufficient to get each packet navigated through the receiver side connectionless network and to its respective receiver computer.

24. An exemplary de-encapsulation is shown schematically in FIG. 6 of the '089 Patent. Beginning on the left-hand side of FIG. 6, prior to de-encapsulation, MPDU **401** contains three individual data packets **406**, **408**, **410** and MPDU header **404**. The MPDU header includes physical link layer network protocol data **412** and data link layer network protocol data **414**. The low-level network protocol data in the MPDU header was needed for the MPDU to navigate through the connection-based network **102** (see FIG. 1). In the de-encapsulation process illustrated in FIG. 6, de-encapsulation unbundles the three individual packets **406**, **408**, **410** so that they can be sent separately though other network(s), such as connectionless receiver side network **112**. Each of these three individual packets includes a packet header (with high-level network protocol information) and a packet payload. Hence, packet **406** can include: packet header **440** (including one or more of network layer network protocol data **450**, transport layer network protocol data **451**, session layer network protocol data **452**, presentation layer network protocol data **453,** and application layer network protocol data **454**); and packet payload **442**.

25. In the embodiment described above, the MPDU is structured for transmission by Synchronous optical networking (SONET) and is structured according to GR-253-CORE, specifically SONET Tx Rx protocol. Individual packets are preferably TCP/IP protocol packets

having a structure and packet header structured described at RFC 793 (TCP portion) and RFC 791 (IP portion).

26. Returning to FIG. 2, MPDU **401** is also sent to information dissector sub-module **170** for dissection. The equipment of the gateway can include a SONET Tx Rx optical interface (not separately shown) with a processor (not shown), which equipment provides information dissector module **170** with the raw data and processing power to perform its dissection of the MPDU as will now be described.

27. The various network protocol data and/or payload data characteristics are sent from the information dissector sub-module to protocol/data library **171** where it is retained for purposes of analysis and application of rules. A buffer memory may be used for temporary storage, which generally lasts at least long enough to implement and/or apply one or more rules.

28. As shown in FIGS. 2 and 4, module **172** applies one or more rules to the MPDU related data in protocol/data library **171** to determine whether any responsive reactions are appropriate depending upon the content of and/or patterns in the network protocol data and/or payload related data of an MPDU or a set of MPDUs. As shown by terminal T**1** in FIGS. 1 and 2, the module receives the applicable rule(s) from a database **106**. In FIG. 1, this database is shown to be a separate component from the gateway computer, but it may be: (i) contained within the gateway computer **103**; and/or (ii) distributed over many locations and/or components.

29. The rules database is generally a relational database that provides for network ID look-up based on international registration and is updated accordingly. The rules in the database may be entirely predetermined and/or they may be adaptively learned. Similarly, any parameter included in any rule may be entirely predetermined and/or may be adaptively scaled by learning. The rules

often, but not always, include at least some guidance as to the appropriate responsive reaction that is to occur when that rule is found to be met during the analysis process.

30. Referring to FIG. 4, the analysis process **200** starts at step S**10** where the MPDU (or set of MPDUs) is dissected for germane network protocol data and/or payload related data as explained above. Once it has been determined that this subject data is in place in the protocol/data library at step S**10**, processing proceeds to step S**12**. At the initial instance of step S**12**, a first rule is retrieved from rules database **106** (see FIG. 1), and processing proceeds to step S**14**. At step S**14**, the retrieved rule is applied to the subject data set. If the subject data set does not meet the rule, the processing proceeds to step S**18**. On the other hand, if the subject data set does meet the rule, then processing proceeds to step S**16**. At step S**18**, the module determines whether the rule that has just been applied at step S**14** is the last applicable rule from rules database **106**. If it is the last rule, then processing proceeds to step S**20**, which is the end of the analysis process for the subject data set. If it is not the last rule, then processing loops back to step S**12**, where the next rule is retrieved from rules database **106**. At step S**16**, because a rule has been found to have been met, responsive reaction processing is performed (see FIG. 2).

31. While some types of responsive reactions will be discussed in detail below, "responsive reaction" generally means that the performance of the data communication system is changed in some way because of the fact that some rule is met. The change in performance may be strictly informational, such as an alert to an administrator, and/or may be functional, such as preventing certain data transfers from occurring, such as when malicious data packets are blocked from passing from the gateway computer to the receiver side connectionless network, or limiting the rate at which such transfers occur. The change in performance may also prevent additional data

from being sent, as when a sender of suspicious packets is sent some kind of response in order to clarify and/or discourage the suspicious data communication activity.

32. A denial-of-service ("DoS") attack is an attempt to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the services of a host computer connected to a network. DoS attacks are typically accomplished by flooding the targeted machine/network resource with superfluous requests so as to overload the targeted machine/network resource and thereby prevent some (or all) legitimate requests from being fulfilled. DoS attacks can be broadly categorized into two major types: (i) bandwidth exhaustion, which concentrates on flooding a targeted uplink above its maximum capacity, so that legitimate traffic has no more available bandwidth; and (ii) server resource exhaustion, which primarily targets server resources and so tend not to be great in volume, but high in packet count.

33. 36. When an unusually large proportion of MPDUs originates from the same geographic and/or IP block location, this is frequently indicative of a malicious DoS attack. Consequently, a rule might, for example, check the physical layer network protocol data **412** (see FIG. 6) for a set of MPDUs received from the connection-oriented network to determine whether an unusually large proportion of the MPDUs were originating at the same geographic location. While higher level network protocol **450**, **451**, **452**, **453**, **454** (see FIG. 6) might be spoofed, it would be much more difficult, or impossible, to spoof the physical layer network protocol data **412** in regards of the geographic location at which the MPDUs entered the connection-oriented network (which is generally, but not necessarily, a WAN).

34. When an unusually high proportion of the set of MPDUs received from the connection-oriented network comes from the same geographic location set, the gateway will perform an appropriate responsive reaction, such as blocking the further transmission of offending packets,

and thereby thwart the DoS attack. Although some legitimate packets may be affected, along with the DoS attack packets, that has been recognized to be a small price to pay for preventing a DoS attack from shutting down the server computer which is the receiver computer.

35. In the context of the internet, the traditional borders of nation states have diminished significance. The notion of geographic locations, however, is currently tied to IP block assignments law, RFC 1174 and the Internet Assigned Numbers Authority (IANA). For example, with technologies such as "bot armies," a DoS attack may come from a number of infected computers that may or may not be in the same country, such as where the source computers executing the attack have been infected with malicious code that came from visiting a web site. Consequently, a geographic area may be targeted by rule-based analysis, and these geographically oriented rules may be based, for example, on IANA assignments.

The Claims are Directed to Patentable Subject Matter

36. The inventions claimed in the '089 Patent include "[a] computer communication network system comprising: a source computer, an MPDU aggregating module, a connection-based network, a gateway, a receiver-side connectionless network, and a receiver computer . . .."

The claims are directed to a solving an existing problem with data communication in conventional computer networks

37. The inventions claimed in the '089 patent are directed to a specific way of selectively transmitting data packets across a network which involves the steps of collecting network protocol data from an MPDU, applying one or more stored rules to that collected data, and transmitting (or not transmitting) the DUs from that MPDU based on the application of the rule(s) to the collected network protocol data. This is a substantial improvement over data transmission in conventional networks.

38. More specifically, the inventions claimed in the '089 patent are directed to solving a problem specifically arising in the realm of computer technology, *viz.* DoS attacks. The invention claimed in the '089 patent solves this problem by, *inter alia*, having the gateway collect network protocol data from an MPDU, apply one or more stored rules to the collected data, and then transmit (or not transmit) the DUs from that MPDU based on the application of the rule(s) to the collected data.

39. Early DoS attacks generally involved only a single source computer, and so could be readily blocked once the IP address of the source computer was identified. By the early part of this century, however, attackers were using multiple computers for DoS attacks (*i.e.*, DoS attacks) and so such preventative measures were no longer effective.

40. Early DoS attacks frequently resulted in a complete shutdown of a website or network. In 2007, for example, Russia-based attackers launched a series of DoS attacks against Estonian public and private sector organizations in response to the Estonian government's removal of a Soviet war monument from its capital. For three weeks, threat actors targeted state and commercial websites, ranging from foreign and defense ministries to banks and media outlets, by overloading their bandwidth and flooding their servers with junk traffic, rendering them inaccessible to the public. In order to mitigate the onslaught, Estonia was forced to close its digital borders and block all international web traffic for a period of time.

41. Prior to the development of the inventions claimed in the '089 patent, attempts to mitigate against DoS attacks included routing all incoming traffic through a "scrubbing center" (a centralized data cleansing station where traffic is analyzed and malicious traffic is removed). This attempted solution, however, necessarily slowed down packet transmission to the receiving computer.

42. Other attempts to mitigate against DoS attacks included the development of content distribution networks (also known as content delivery networks), or CDNs, which sought to reduce the ability of an attacker to flood a particular server by spreading content out amongst multiple servers (*i.e.*, a "horizontal" distribution of the attack surface area). Such a solution, however, proved to be quite expensive as more and more servers were required for a CDN.

The claimed inventions provide unconventional technological solutions to problems with conventional computer systems and networks

43. The inventions claimed in the '089 patent are directed to a novel way of selectively transmitting data packets across a network. As described above, the inventions claimed in the '089 patent are direct to systems and methods data communication that involve collecting network protocol data from an MPDU, applying one or more stored rules to that collected data, and transmitting (or not transmitting) the DUs from that MPDU based on the application of the rule(s) to the collected network protocol data.

44. One component of the inventive system is a gateway between the connection-based network (*i.e.* the internet) and the connectionless network. This particular gateway performs certain specified functions, some of which are performed by gateways in conventional network systems. These "conventional" functions include: receiving the first MPDU from the WAN; disaggregating the first MPDU into a plurality of smaller data units (DUs); and communicating the DUs to the LAN.

45. The gateway between the connection-based network (*i.e.* the internet) and the connectionless network in the claimed system, however, also performs certain additional functions which are not performed by gateways in conventional network systems. These additional, unconventional functions include: collecting selected network protocol data from the MPDU; applying a rule to the collected selected network protocol data; and selectively making a responsive

reaction based, at least in part, upon the application of the rule to the collected selected network protocol data. The selected network protocol data from the MPDU that is collected and utilized by the gateway in the claimed system is discarded and lost by gateways in conventional systems.

46. The gateway in the claimed system uses the collected selected network protocol data to determine, *inter alia*, whether to communicate the DUs from the MPDU to the LAN. The ability to selectively communicate DUs to the LAN based on the collected selected network protocol data enables the gateway in the claimed system to counter DoS attacks, particularly DoS attacks.

47. The inventive system, which includes an embodiment of the inventive gateway, is exemplified by claim 1 of the '089 patent, which is directed to:

> A computer communication network system comprising: a source computer, an MPDU aggregating module, a connection-based network, a gateway, a receiver-side connectionless network, and a receiver computer, wherein:
>
> the source computer is structured, and/or data-communication-connected to send a first packet, with the first packet including destination information indicating that it is intended to be sent to and received by the receiver computer;
>
> the MPDU aggregating module is structured, programmed and/or data-communication-connected to receive the first packet from the source computer and to aggregate it into a first MPDU, where the first MPDU is in a form and format suitable to be communicated over the connection-based network;
>
> the connection-based network is structured, programmed and/or data-communication-connected to receive the first MPDU from the MPDU aggregating module and to communicate it to the gateway in a connection-based manner;
>
> the gateway is structured, programmed and/or data-communication-connected to receive the first MPDU from the connection-based network, to disaggregate the first MPDU into a plurality of smaller data units (DUs) including a first DU at least partially constituted by the first packet, and to selectively communicate the first DU to the receiver-side connectionless network;
>
> the receiver-side connectionless network is structured, programmed and/or data-communication-connected to receive the first DU from the gateway on condition that it was selectively communicated by the gateway, and to communicate at least the first

> data packet portion of the first DU to the receiver computer in a connectionless manner;
>
> the gateway is structured, programmed and/or data-communication-connected to collect selected network protocol data from the first MPDU, with the selected network protocol data including at least some network protocol data included in the first MPDU and not included in any of the plurality of DUs, and with the selected network protocol data relating exclusively to network protocols and including no data from any data payload(s) which may be present in the MPDU;
>
> the gateway is further structured, programmed and/or data-communication-connected to apply a first rule to the selected network protocol data that has been collected by the gateway; and
>
> the gateway is further structured, programmed and/or data-communication-connected to selectively make a responsive reaction based, at least in part, upon the application of the first rule applied by the gateway to the selected network protocol data.

Claim 1 of the ’089 patent.

The claims are not directed to an abstract idea or law of nature

48. The claims of the ‘089 patent are not directed to an abstract idea or law of nature.

Claim 7 of the ‘089 patent is directed to a gateway computer comprising a non-transient software storage device with the following software encoded therein: a gateway module and an enhanced requesting module. As would be known and recognized by person of ordinary skill in the art (“POSITA”), a gateway computer is a real, tangible, physical device, as is a non-transient software storage device.

49. Claim 1 of the ’089 patent is directed to a computer communication network system comprising: a source computer, an MPDU aggregating module, a connection-based network, a gateway, a receiver-side connectionless network, and a receiver computer. As would be known and recognized by a POSITA, all of the elements of the claim—the source and receiver computers, the MPDU aggregating module, the gateway, and the connection-based and connectionless networks--are all real, tangible, physical devices.

50. Claim 20 of the ’089 patent is directed to method of communicating data units in a computer network. Packet transmission is not a law of nature and the specific way in which data units are communicated according to the claimed method, *i.e.*, by collecting certain network protocol, applying a rule from a database to that data, and then routing the packet based on the application of that rule (or rules) to the collected network protocol data, is not abstract.

The claims do not preempt their field

51. The claims of the ‘089 patent do not merely recite a generic way of routing incoming traffic to a receiver-side connectionless network and, ultimately, to a receiver computer. Rather, the claimed inventions are directed to a specific way of defending against DoS attacks by collecting a particular set of data and then using that data to determine how to route the incoming traffic by applying one or more rules from a database.

52. Alternative ways exist and are known for routing incoming traffic to defend against DoS attacks. Prior to the inventions claimed in the ‘089 patent, for example, CDNs were developed as a means of defending against DoS attacks, as was the procedure of scrubbing all incoming traffic. U.S. Patent No. 7,020,783, for example, discloses a data communication network that includes a system (**201**, **203**, **212**) for handling DoS attacks. U.S. Patents Nos. 7,849,504 and 7,404,206 disclose security enhanced network devices, and methods, that help prevent traffic spoofing and maintain information that identifies the source(s) of traffic.

53. Even with respect to the more specific selective transmission of data units to a receiver-side connectionless network, a POSITA knows and understands other ways to determine how to communicate data units to the receiver-side network than collecting certain network protocol, applying a rule from a database to that data, and then routing the data unit based on the application of that rule (or rules) to the collected network protocol data. U.S. Patent No. 6,990,531, for

example, discloses other systems and methods for prioritizing data traffic over a shared bandwidth connection. U.S. Patent No. 7,856,012 also discloses alternative systems and methods for facilitating communication of data in a network, which includes receiving a block of data, selecting a selected rule from a set of available rules, processing the block of data, and prioritizing the block of data.

The claimed method could not be performed mentally or by hand

54. Data transfer across the internet typically takes place at speeds up to 10 Tbps (10 terabits per second). Given that volume of data packets, a POSITA would know and understand that the claimed method of communicating data units in a computer network could not possibly be performed mentally or by hand.

DEFENDANT'S ACCUSED INSTRUMENTALITIES

55. On information and belief, Cloudflare connects customer end-users to the internet (a connection-based network). Data packets (MPDUs) being sent to a customer end-user enter the network through an edge router (a gateway) by Cloudflare.

56. On information and belief, Defendant uses, sells, and/or offers for sale cybersecurity services, including DoS protection services (the "Accused Services"). **Exhibit 2**.

57. Cloudflare provides the end-to-end internet whereby connectionless LAN autonomous systems connect to BGP WAN edge routers for the connection-based pathway and encapsulation framing across the WAN to mitigate DDoS. It distributes traffic (data unit) across the network and chooses a fast, efficient route to deliver the traffic.

FIRST CAUSE OF ACTION
(Direct Infringement of the '089 Patent)

58. Touchpoint hereby repeats and re-alleges the allegations contained in paragraphs above as if fully set forth herein.

59. The ’089 Patent is presumed valid under 35 U.S.C. § 282.

60. Touchpoint has complied with the requirements of 35 U.S.C. § 287 as have all prior owners of the ’089 Patent.

61. The Accused Instrumentalities and Accused Services are covered by one or more claims of the ’089 Patent and therefore infringe the ’089 Patent. A claim chart attached as **Exhibit 2** identifies specifically how each element of each asserted claim of the ’089 Patent is practiced by the Accused Instrumentalities and/or the Accused Services.

62. The Accused Instrumentalities infringes, for example, Claim 1 of the ’089 Patent, either literally or under the doctrine of equivalents, because the Accused Instrumentalities receives packets from the internet through an edge router which disaggregates each packet into data units, collects network protocol data from the packet, and then transmits (or does not transmit) the data units that were contained in that packet based upon the application of one or more rules to the network protocol data.

63. The Accused Services infringe, for example, claim 20 of the ’089 Patent, either literally or under the doctrine of equivalents, because Defendant’s DoS Protection solution receives packets from the internet, disaggregates those packets into data units, collects network protocol data from the packets, and then transmits (or does not transmit) the data units from each packet based upon the application of one or more rules to the network protocol data collected from that packet.

64. Defendant’s direct infringement of the ’089 Patent has injured and continues to injure Touchpoint and Touchpoint is entitled to recover damages adequate to compensate for that infringement in an amount to be proven at trial, but not less than a reasonable royalty.

65. Despite Defendant's knowledge of the '089 Patent and its infringing activities, Defendant has continued to use, sell, and/or offer for sale products and services falling within the scope of one or more claims of the '089 Patent, without authority from Touchpoint.

66. Even after becoming aware of its direct infringement of the '089 Patent, on information and belief, Defendant has made no effort to alter its services or otherwise attempt to design around the claims of the '089 Patent in order to avoid infringement. These actions demonstrate Defendant's blatant and egregious disregard for Touchpoint's patent rights.

67. As a result of Defendant's unlawful activities, Touchpoint has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Defendant's continued direct infringement of the '089 Patent causes harm to Touchpoint in the form of loss of goodwill, damage to reputation, loss of business opportunities, lost profits, inadequacy of monetary damages, and/or direct and indirect competition. Monetary damages are insufficient to compensate Touchpoint for these harms. Accordingly, Touchpoint is entitled to preliminary and permanent injunctive relief.

SECOND CAUSE OF ACTION
(Indirect Infringement of the '089 Patent)

68. Touchpoint hereby repeats and re-alleges the allegations contained in paragraphs above as if fully set forth herein.

69. Defendant's customer end-users directly infringe the claims of the '089 patent, including at least claim 1 due to their use of Accused Instrumentalities and/or Accused Services in their normal and customary way in this District.

70. Defendant indirectly infringes by inducing infringement of the claims of the '089 Patent by aiding and abetting consumer end-users to use the Accused Instrumentalities and/or the Accused Services in their normal and customary way in the United States and in this District and

by contributing to infringement of the claims of the ’089 Patent by supplying components and providing instructions to consumer end-users for using those components in practicing the method claimed in claim 20 of the ’089 Patent, if infringement contentions are amended to include this claim.

71. Defendant aids and abets consumer end-users in infringing the claims of the ’089 Patent with the knowledge of, and the specific intent to cause, the acts of direct infringement performed by these consumer end-users. On information and belief, despite having knowledge of the ’089 Patent, Defendant has been and will continue to use, sell, and/or offer to sell the Accused Instrumentalities and/or Accused Services directly and through the actions of others controlled by Defendant.

72. Defendant’s indirect infringement of the ’089 Patent has injured and continues to injure Touchpoint and Touchpoint is entitled to recover damages adequate to compensate for that infringement in an amount to be proven at trial, but not less than a reasonable royalty.

73. Despite Defendant’s knowledge of the ’089 Patent and its infringing activities and the infringing activities of consumer end-users of Defendant’s Accused Instrumentalities and/or Accused Services, Defendant has continued to use, sell, and/or offer for sale products and services falling within the scope of one or more claims of the ’089 Patent, without authority from Touchpoint.

74. Even after becoming aware of its indirect infringement of the ’089 Patent, on information and belief, Defendant has made no effort to alter its services or otherwise attempt to design around the claims of the ’089 Patent in order to avoid infringement. These actions demonstrate Defendant’s blatant and egregious disregard for Touchpoint’s patent rights.

75. As a result of Defendant's unlawful activities, Touchpoint has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Defendant's continued indirect infringement of the '089 Patent causes harm to Touchpoint in the form of loss of goodwill, damage to reputation, loss of business opportunities, lost profits, inadequacy of monetary damages, and/or direct and indirect competition. Monetary damages are insufficient to compensate Touchpoint for these harms. Accordingly, Touchpoint is entitled to preliminary and permanent injunctive relief.

PRAYER FOR RELIEF

Wherefore, Touchpoint respectfully prays this Court enter judgment in its favor on each and every Claim for Relief and award to Touchpoint relief, including, but not limited to, the following:

A. Entry of judgment in favor of Touchpoint, and against Defendant, on each and every Claim in this Complaint;

B. Entry of judgment in favor of Touchpoint, and against Defendant, that Defendant has directly infringed the claims of the '089 Patent;

C. Entry of judgment in favor of Touchpoint, and against Defendant, that Defendant has indirectly infringed the claims of the '089 Patent by inducing the infringement thereof and/or contributing to the infringement thereof;

D. Entry of judgment in favor of Touchpoint, and against Defendant, that this case is an exceptional case and awarding Touchpoint its reasonable attorney fees and costs pursuant to 35 U.S.C. § 285 and any other applicable statutes, laws, and/or rules; and

E. Entry of preliminary and permanent injunctions against Defendant, and its officers, directors, principals, agents, sales representatives, servants, employees, successors, assigns,

affiliates, divisions, subsidiaries, and all those acting in concert or participation with them, from directly infringing, inducing infringement and/or contributing to the infringement of any claim of the '089 Patent.

F. A determination that Touchpoint is the prevailing party and therefore entitled to its taxable costs; and

G. Entry of judgment in favor of Touchpoint, and against Defendant, awarding Touchpoint such other relief the Court deems just, equitable, and proper.

DEMAND FOR A JURY TRIAL

Touchpoint requests a trial by jury, under Rule 38 of the Federal Rules of Civil Procedure, for all issues so triable.

Dated: May 8, 2024

Respectfully Submitted,

/s/ Randall Garteiser

Christopher A. Honea
Texas Bar No. 24059967
chonea@ghiplaw.com
Randall Garteiser
Texas Bar No. 24038912
rgarteiser@ghiplaw.com
M. Scott Fuller
Texas Bar No. 24036607
rgarteiser@ghiplaw.com
GARTEISER HONEA, PLLC
119 W. Ferguson Street
Tyler, Texas 75702
Telephone: (903) 705-7420
Facsimile: (903) 405-3999

COUNSEL FOR PLAINTIFF