UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
TEXARKANA DIVISION

OPTIMORPHIX, INC., *Plaintiff,* v. **F5, INC.** *Defendant.*	**Civil Action No._________** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

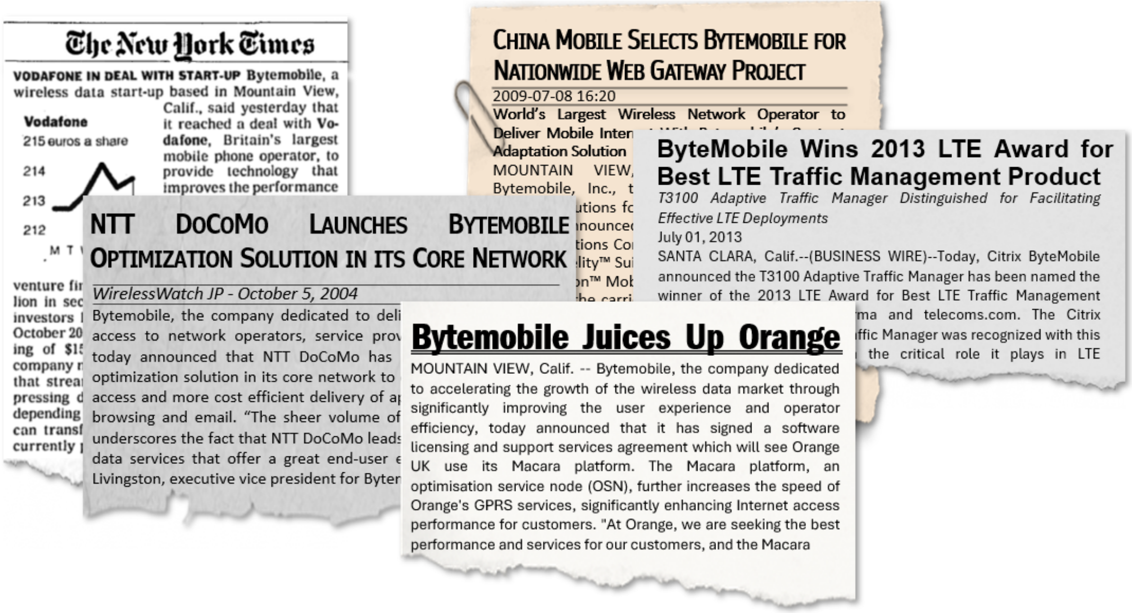
OptiMorphix, Inc. ("OptiMorphix" or "Plaintiff") brings this action and makes the following allegations of patent infringement relating to U.S. Patent Nos.: 7,099,273 (the "'273 patent"); 7,136,353 (the "'353 patent"); 7,586,871 (the "'871 patent"); 7,616,559 (the "'559 patent"); 8,429,169 (the "'169 patent"); 8,521,901 (the "'901 patent"); 9,936,040 (the "'040 patent"); and 10,264,093 (the "'093 patent") (collectively, the "patents-in-suit"). Defendant F5, Inc. ("F5" or "Defendant") infringes the patents-in-suit in violation of the patent laws of the United States of America, 35 U.S.C. § 1 *et seq*.

THE PARTIES

1. Plaintiff OptiMorphix, Inc. ("Plaintiff" or "OptiMorphix") is a Delaware corporation that holds a portfolio of over 250 patent assets that were developed at Citrix Systems, Inc. ("Citrix") and Bytemobile, Inc.

2. Bytemobile, Inc. ("Bytemobile") was a global leader in mobile internet solutions for network operators. The company was founded in 2000. Bytemobile's mission was to optimize video and web content services for mobile network operators to improve users' experiences while maximizing the efficiency of network infrastructure.

3. Bytemobile was established during a time when the mobile landscape was evolving rapidly. The advent of 3G technology, coupled with increasingly sophisticated smartphones, led to a surge in demand for data services. However, mobile networks at the time were not optimized to handle this influx, particularly for data-rich services like video streaming. Recognizing this opportunity, Bytemobile sought to create solutions that would enable network operators to deliver high-quality, consistent mobile data services. By 2011, Bytemobile was a "market leader in video and web optimization, with more than 125 cumulative operator deployments in 60 countries.[1]



The New York Times

VODAFONE IN DEAL WITH START-UP Bytemobile, a wireless data start-up based in Mountain View, Calif., said yesterday that it reached a deal with Vodafone, Britain's largest mobile phone operator, to provide technology that improves the performance

Vodafone
215 euros a share
214
213
212
M T

venture fir
lion in sec
investors
October 20
ing of $15
company r
that strea
pressing d
depending
can transf
currently

NTT DoCoMo Launches Bytemobile Optimization Solution in its Core Network

WirelessWatch JP - October 5, 2004

Bytemobile, the company dedicated to deli
access to network operators, service prov
today announced that NTT DoCoMo has
optimization solution in its core network to
access and more cost efficient delivery of ap
browsing and email. "The sheer volume of
underscores the fact that NTT DoCoMo leads
data services that offer a great end-user e
Livingston, executive vice president for Byten

China Mobile Selects Bytemobile for Nationwide Web Gateway Project

2009-07-08 16:20

World's Largest Wireless Network Operator to Deliver Mobile Inter
Adaptation Solution

MOUNTAIN VIEW,
Bytemobile, Inc., t
utions fo
nounced
tions Co
lity™ Su
on™ Mob
he carri

ByteMobile Wins 2013 LTE Award for Best LTE Traffic Management Product

T3100 Adaptive Traffic Manager Distinguished for Facilitating Effective LTE Deployments

July 01, 2013

SANTA CLARA, Calif.--(BUSINESS WIRE)--Today, Citrix ByteMobile announced the T3100 Adaptive Traffic Manager has been named the winner of the 2013 LTE Award for Best LTE Traffic Management
ma and telecoms.com. The Citrix
ffic Manager was recognized with this
the critical role it plays in LTE

Bytemobile Juices Up Orange

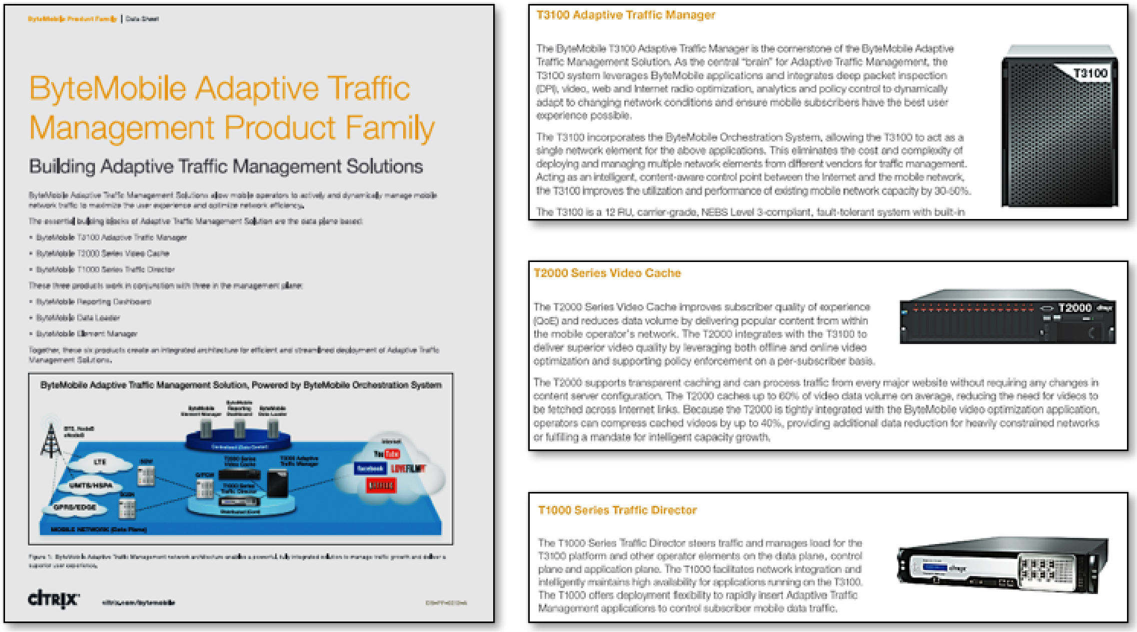
MOUNTAIN VIEW, Calif. -- Bytemobile, the company dedicated to accelerating the growth of the wireless data market through significantly improving the user experience and operator efficiency, today announced that it has signed a software licensing and support services agreement which will see Orange UK use its Macara platform. The Macara platform, an optimisation service node (OSN), further increases the speed of Orange's GPRS services, significantly enhancing Internet access performance for customers. "At Orange, we are seeking the best performance and services for our customers, and the Macara

Andrew Zipern, *Vodafone in Deal with Start-Up Bytemobile,* NYTimes at C4 (January 29, 2002) ("Bytemobile, a wireless data start-up . . . reached a deal with Vodafone, Britain's largest mobile phone operator"); *NTT DoCoMo Launches Bytemobile Optimization Solution in its Core Network,* WIRELESSWATCH IP (October 5, 2004) ("NTT DoCoMo has deployed Bytemobile's optimization solution in its core network"); *China Mobile Selects Bytemobile for Nationwide Web Gateway Project*, BUSINESS WIRE (July 8, 2009) ("A Bytemobile customer since 2004, CMCC has deployed its web optimization solutions"); *Bytemobile Juices Up Orange*, ESPICOM TELECOMMUNICATION NEWS (October 10, 2002) ("Orange customers will experience faster application performance and Web page downloads"); *ByteMobile Wins 2013 LTE Award for Best LTE Traffic Management Product*, MARKETSCREENER (July 1, 2013) ("ByteMobile technology has been deployed . . . in networks serving nearly two billion subscribers.").

[1] *Bytemobile: Importance of Video and Web Optimizations*, TELECOM REVIEW at 58 (2011); *see also Bytemobile Secures Its 36th Video Optimisation Win for MNO Deployment,* TOTAL TELECOM & TOTAL TELECOM MAGAZINE (March 21, 2011).

4. Bytemobile products, such as the Unison platform and the T3100 Adaptive Traffic Manager, were designed to optimize mobile data traffic in real-time, ensuring a high-quality mobile internet experience for end-users. This approach was groundbreaking at the time and set the stage for many of the mobile data optimization techniques used today.

5. Bytemobile's innovative technologies and customer-centric approach led to rapid growth and success. Bytemobile's innovative product portfolio included: the T3100 Adaptive Traffic Manager which was designed to handle high volumes of traffic efficiently and provide real-time optimization, compression, and management of mobile data; Bytemobile's T2000 Series Video Cache, which supported transparent caching of content; and Bytemobile's T1000 Series Traffic Director, which enabled traffic steering and load balancing for high availability of applications.



ByteMobile Product Family | Data Sheet

ByteMobile Adaptive Traffic Management Product Family

Building Adaptive Traffic Management Solutions

ByteMobile Adaptive Traffic Management Solutions allow mobile operators to actively and dynamically manage mobile network traffic to maximize the user experience and optimize network efficiency.

The essential building blocks of Adaptive Traffic Management Solution are the data plane based:

- ByteMobile T3100 Adaptive Traffic Manager
- ByteMobile T2000 Series Video Cache
- ByteMobile T1000 Series Traffic Director

These three products work in conjunction with three in the management plane:

- ByteMobile Reporting Dashboard
- ByteMobile Data Loader
- ByteMobile Element Manager

Together, these six products create an integrated architecture for efficient and streamlined deployment of Adaptive Traffic Management Solutions.

ByteMobile Adaptive Traffic Management Solution, Powered by ByteMobile Orchestration System

ByteMobile Element Manager
ByteMobile Reporting Dashboard
ByteMobile Data Loader
BTS, NodeB eNodeB
LTE
UMTS/HSPA
GPRS/EDGE
SGW
SGSN
GGSN
T2000 Series Video Cache
T3100 Adaptive Traffic Manager
T1000 Series Traffic Director
Internet
YouTube
facebook
LOVEFILM
NETFLIX
MOBILE NETWORK (Data Plane)

Figure 1: ByteMobile Adaptive Traffic Management network architecture enables a powerful, fully integrated solution to manage traffic growth and deliver a superior user experience.

citrix.com/bytemobile

T3100 Adaptive Traffic Manager

The ByteMobile T3100 Adaptive Traffic Manager is the cornerstone of the ByteMobile Adaptive Traffic Management Solution. As the central "brain" for Adaptive Traffic Management, the T3100 system leverages ByteMobile applications and integrates deep packet inspection (DPI), video, web and Internet radio optimization, analytics and policy control to dynamically adapt to changing network conditions and ensure mobile subscribers have the best user experience possible.

The T3100 incorporates the ByteMobile Orchestration System, allowing the T3100 to act as a single network element for the above applications. This eliminates the cost and complexity of deploying and managing multiple network elements from different vendors for traffic management. Acting as an intelligent, content-aware control point between the Internet and the mobile network, the T3100 improves the utilization and performance of existing mobile network capacity by 30-50%.

The T3100 is a 12 RU, carrier-grade, NEBS Level 3-compliant, fault-tolerant system with built-in

T2000 Series Video Cache

The T2000 Series Video Cache improves subscriber quality of experience (QoE) and reduces data volume by delivering popular content from within the mobile operator's network. The T2000 integrates with the T3100 to deliver superior video quality by leveraging both offline and online video optimization and supporting policy enforcement on a per-subscriber basis.

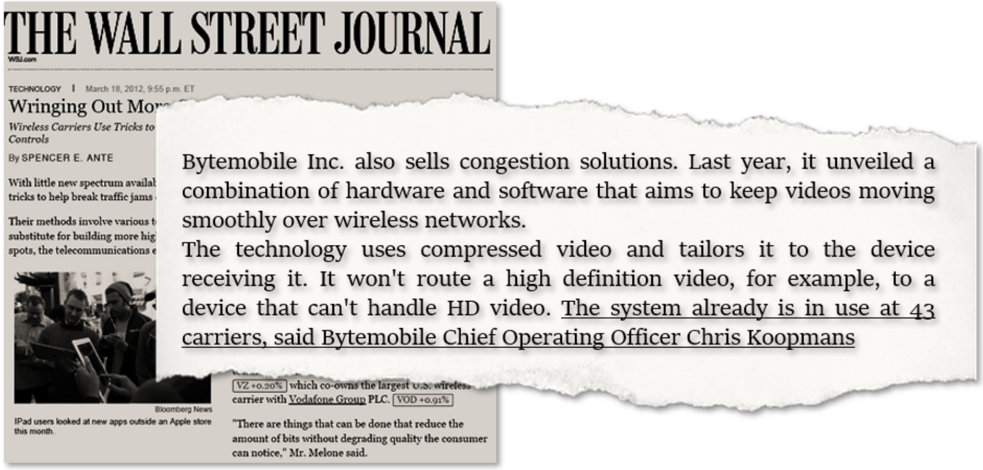
The T2000 supports transparent caching and can process traffic from every major website without requiring any changes in content server configuration. The T2000 caches up to 60% of video data volume on average, reducing the need for videos to be fetched across Internet links. Because the T2000 is tightly integrated with the ByteMobile video optimization application, operators can compress cached videos by up to 40%, providing additional data reduction for heavily constrained networks or fulfilling a mandate for intelligent capacity growth.

T1000 Series Traffic Director

The T1000 Series Traffic Director steers traffic and manages load for the T3100 platform and other operator elements on the data plane, control plane and application plane. The T1000 facilitates network integration and intelligently maintains high availability for applications running on the T3100. The T1000 offers deployment flexibility to rapidly insert Adaptive Traffic Management applications to control subscriber mobile data traffic.

Bytemobile Adaptive Traffic Management Product Family, BYTEMOBILE DATA SHEET at 1-2 (2014).

6. Bytemobile's groundbreaking technologies also included products for data optimization. Bytemobile's data optimization solutions were designed to compress and accelerate data transfer. By reducing the size of data packets without compromising quality, these technologies allowed faster data transmission and minimized network congestion. Bytemobile also offered solutions to analyze and manage network traffic, allowing network operators to identify patterns, allocate bandwidth intelligently, and prioritize different types of content.



THE WALL STREET JOURNAL

WSJ.com

TECHNOLOGY | March 18, 2012, 9:55 p.m. ET

Wringing Out Mor

Wireless Carriers Use Tricks to
Controls

By SPENCER E. ANTE

With little new spectrum availa
tricks to help break traffic jams

Their methods involve various t
substitute for building more hig
spots, the telecommunications e

Bytemobile Inc. also sells congestion solutions. Last year, it unveiled a combination of hardware and software that aims to keep videos moving smoothly over wireless networks.

The technology uses compressed video and tailors it to the device receiving it. It won't route a high definition video, for example, to a device that can't handle HD video. The system already is in use at 43 carriers, said Bytemobile Chief Operating Officer Chris Koopmans

VZ +0.20% which co-owns the largest U.S. wireless carrier with Vodafone Group PLC. VOD +0.91%

"There are things that can be done that reduce the amount of bits without degrading quality the consumer can notice," Mr. Melone said.

Bloomberg News

IPad users looked at new apps outside an Apple store this month.

Spencer E. Ante, *Wringing Out More Capacity*, WALL STREET JOURNAL at B3 (March 19, 2012) (emphasis added).

7. In July 2012, Bytemobile was acquired by Citrix Systems, Inc. ("Citrix") for $435 million. Bytemobile "became part of [Citrix's] Enterprise division and extend[ed] [Citrix's] industry reach into the mobile and cloud markets."[2]

8. OptiMorphix owns a portfolio of patents developed at Bytemobile and later Citrix. Highlighting the importance of the patents-in-suit is the fact that the OptiMorphix's patent portfolio has been cited by over 4,800 U.S. and international patents and patent applications assigned to a wide variety of the largest companies operating in the networking, content delivery, and cloud computing fields. OptiMorphix's patents have been cited by companies such as:

[2] CITRIX SYSTEMS, INC. 2012 ANNUAL REPORT at 33 (2013).

- Amazon.com, Inc. (263 citing patents and applications)[3]
- Oracle (59 citing patents and applications)[4]
- Alphabet, Inc. (103 citing patents and applications)[5]
- Broadcom Ltd. (93 citing patents and applications)[6]
- Cisco Systems, Inc. (277 citing patents and applications)[7]
- Lumen Technologies, Inc. (77 citing patents and applications)[8]
- Intel Corporation (45 citing patents and applications)[9]
- Microsoft Corporation (150 citing patents and applications)[10]
- AT&T, Inc. (93 citing patents and applications)[11]
- Verizon Communications, Inc. (31 citing patents and applications)[12]
- Juniper Networks, Inc. (29 citing patents and applications)[13]

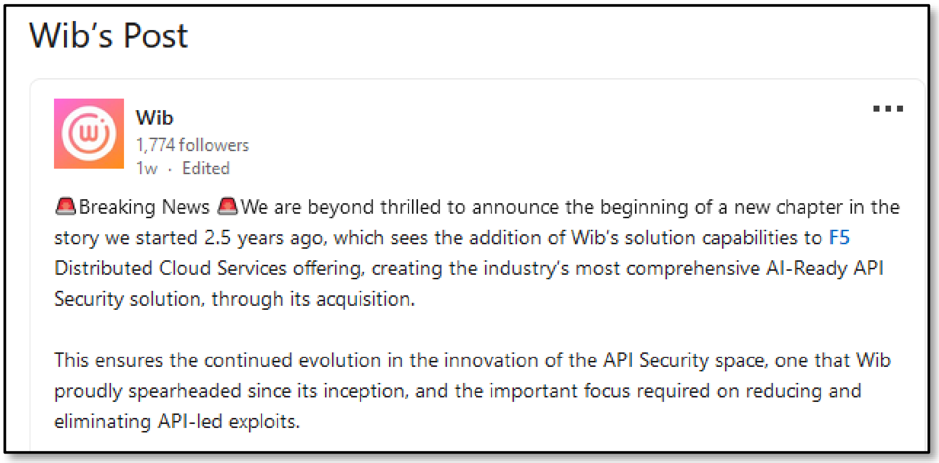
9. Defendant F5, Inc. ("F5") is a Washington corporation with its principal place of business at 801 5th Avenue, Seattle, Washington 98104.

10. F5 conducts business operations within the Eastern District of Texas where it sells, develops, and/or markets its products, including the accused products, including facilities at 18325 Waterview Parkway Dallas, Texas 75252, which is located in this District, in Collin County, Texas.

11. On February 7, 2024, F5 acquired Wib Security, which maintains its U.S. Headquarters in Collin County, Texas. Wib Security is registered with the Texas Comptroller of Public Accounts Sales & Use and lists its address as 12488 Eastline Road, Trenton, Texas, which is located in the Eastern District of Texas in Fannin County. News articles, blog postings, and social media postings from Wib Security and F5 executives all confirm that, as of the filing of this

[3] *See e.g.*, U.S. Patent Nos. 7,817,563; 9,384,204; 9,462,019; 11,343,551; and 11,394,620.
[4] *See e.g.,* U.S. Patent Nos. 7,475,402; 7,574,710; 8,589,610; 8,635,185; and 11,200,240.
[5] *See e.g.,* U.S. Patent Nos. 7,743,003; 8,458,327; 9,166,864; 9,665,617; and 10,733,376.
[6] *See e.g.,* U.S. Patent Nos. 7,636,323; 8,448,214; 9,083,986; 9,357,269; and 10,091,528.
[7] *See e.g.,* U.S. Patent Nos. 7,656,800; 7,930,734; 8,339,954; 9,350,822; and 10,284,484.
[8] *See e.g.,* U.S. Patent Nos. 7,519,353; 8,315,179; 8,989,002; 10,511,533; and 11,233,740.
[9] *See e.g.,* U.S. Patent Nos. 7,394,809; 7,408,932; 9,515,942; 9,923,821; and 10,644,961.
[10] *See e.g.,* U.S. Patent Nos. 8,248,944; 9,071,841; 9,852,118; 10,452,748; and 11,055,47.
[11] *See e.g.,* U.S. Patent Nos. 8,065,374; 8,429,302; 9,558,293; 9,800,638; and 10,491,645.
[12] *See e.g.,* U.S. Patent Nos. 8,149,706; 8,930,559; 9,253,231; 10,003,697; and 10,193,942.
[13] *See e.g.,* U.S. Patent Nos. 8,112,800; 8,509,071; 8,948,174; 9,407,726; and 11,228,631.

Complaint, F5 has purchased Wib Security and is conducting business and maintaining a presence in this District. Wib Security posted on LinkedIn: "We are beyond thrilled to announce the beginning of a new chapter in the story we started 2.5 years ago, which sees the addition of Wib's solution capabilities <u>to F5 Distributed Cloud Services offering</u>, creating the industry's most comprehensive AI-Ready API Security solution, <u>through its acquisition</u>."[14]



Wib's Post

Wib
1,774 followers
1w · Edited

🚨Breaking News 🚨We are beyond thrilled to announce the beginning of a new chapter in the story we started 2.5 years ago, which sees the addition of Wib's solution capabilities to F5 Distributed Cloud Services offering, creating the industry's most comprehensive AI-Ready API Security solution, through its acquisition.

This ensures the continued evolution in the innovation of the API Security space, one that Wib proudly spearheaded since its inception, and the important focus required on reducing and eliminating API-led exploits.

LinkedIn Wib Security Posting, LINKEDIN.COM WEBPAGE (dated February 2024), available at: www.linkedin.com/posts/wibsecurity_wib-api-apisecurity-activity-7161460906969743360-IqK5?

> Cybersecurity startup Wib, which has developed an API security platform, <u>has been acquired by U.S. cyber giant F5</u>. The companies did not reveal the value of the acquisition, but it is estimated to be in the region of tens of millions of dollars.

API Security Startup Wib Acquired By F5 For Tens Of Millions Of Dollars, CTECH BY CALCALLIST.COM (February 11, 2024), available at: ttps://www.calcalistech.com/ctechnews/article/rjoixtuj6 (emphasis added).

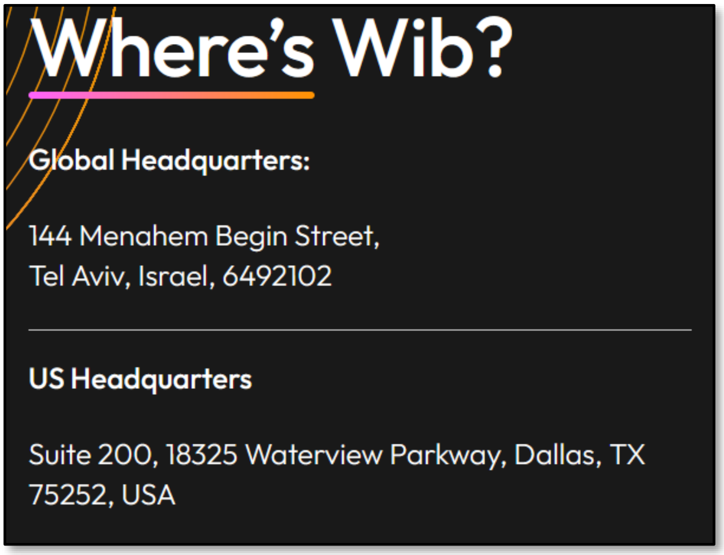
> F5 also took to AppWorld 2024 to announce that it had acquired Israel-based API security provider Wib for an undisclosed sum. The company's vulnerability detection and observability in application development processes is also now

[14] *LinkedIn Wib Security Posting,* LINKEDIN.COM WEBPAGE (dated February 2024), available at: ww.linkedin.com/posts/wibsecurity_wib-api-apisecurity-activity-7161460906969743360-IqK5? (emphasis added).

included in F5's enhanced Distributed Cloud Platform.

F5 Ups Application Security With Enhanced Distributed Cloud Services Platform, AI Assistant, CRN.COM WEBSITE (February 14, 2024), ttps://www.crn.com/news/networking/2024/f5-ups-application-security-with-enhanced-distributed-cloud-services-platform-ai-assistant

12. As of the filing of this Complaint, the Wib Security website directs and identifies to users that it is continuing to do business and is located in the Eastern District of Texas.



Where's Wib?

Global Headquarters:

144 Menahem Begin Street,
Tel Aviv, Israel, 6492102

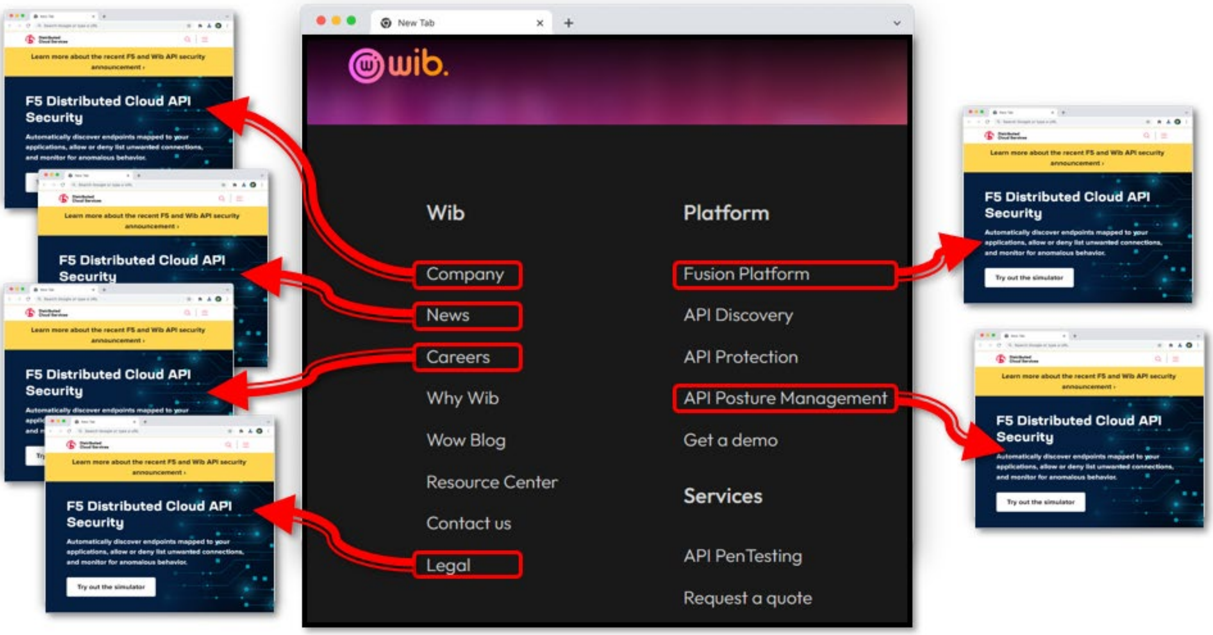
US Headquarters

Suite 200, 18325 Waterview Parkway, Dallas, TX
75252, USA

WIB SECURITY WEBSITE, CONTACT US PAGE, available at: https://wib.com/contact-us/ (image captured February 21, 2024).

13. F5 is now conducting the business of F5 through Wib Security, including but not limited to Wib Security's former (and F5's current) regular and established place of business within this District.

14. For example, numerous links on the Wib Security website redirect users to the F5 website. Specifically, visitors to Wib.com are redirected to the F5 website when they click links for "Company," "News," "Careers," "Legal," "Fusion Platform," and "API Posture Management."



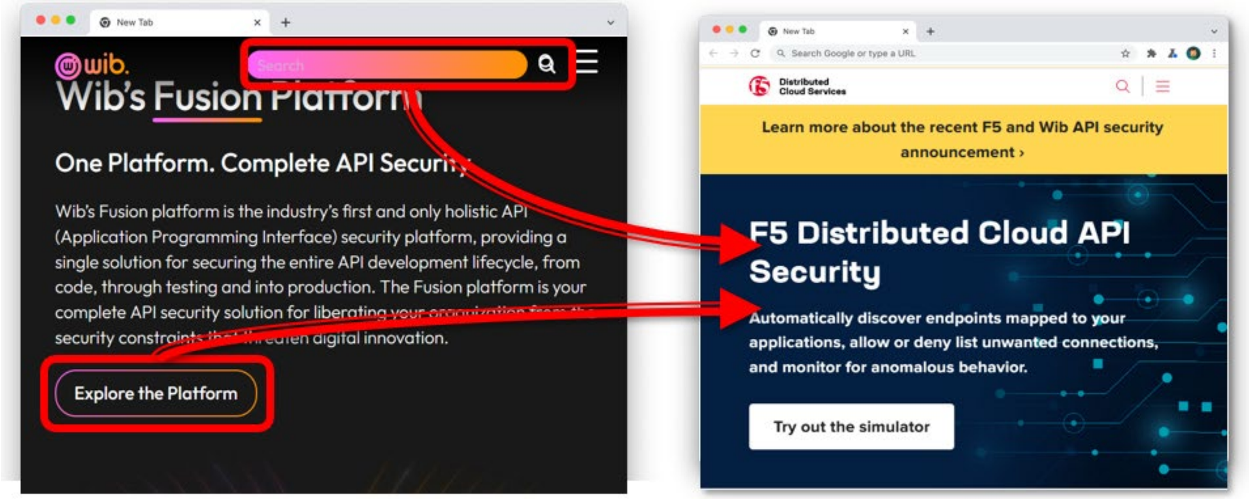
Learn more about the recent F5 and Wib API security announcement ›

F5 Distributed Cloud API Security

Automatically discover endpoints mapped to your applications, allow or deny list unwanted connections, and monitor for anomalous behavior.

WIB SECURITY WEBSITE, available at: https://wib.com/(image captured February 21, 2024); F5 WEBSITE, API-SECURITY WEBPAGE, available at: https://www.f5.com/cloud/products/api-security (image captured February 21, 2024) (showing the webpage that appears as of February 21, 2024 when the "Search jobs" link is clicked from the immediately preceding Wib Security webpage).

15. As a further example of F5 conducting its business through Wib Security, all queries to the Wib Security website are redirected to the F5 website. As of February 21, 2024, if a visitor to the Wib Security website clicks on the magnifying glass icon on the homepage to search the site and enters any query into the search functionality, the visitor will be redirected to the F5 website.



wib.

Wib's Fusion Platform

One Platform. Complete API Security

Wib's Fusion platform is the industry's first and only holistic API (Application Programming Interface) security platform, providing a single solution for securing the entire API development lifecycle, from code, through testing and into production. The Fusion platform is your complete API security solution for liberating your organization from the security constraints that threaten digital innovation.

Explore the Platform

Distributed Cloud Services

Learn more about the recent F5 and Wib API security announcement ›

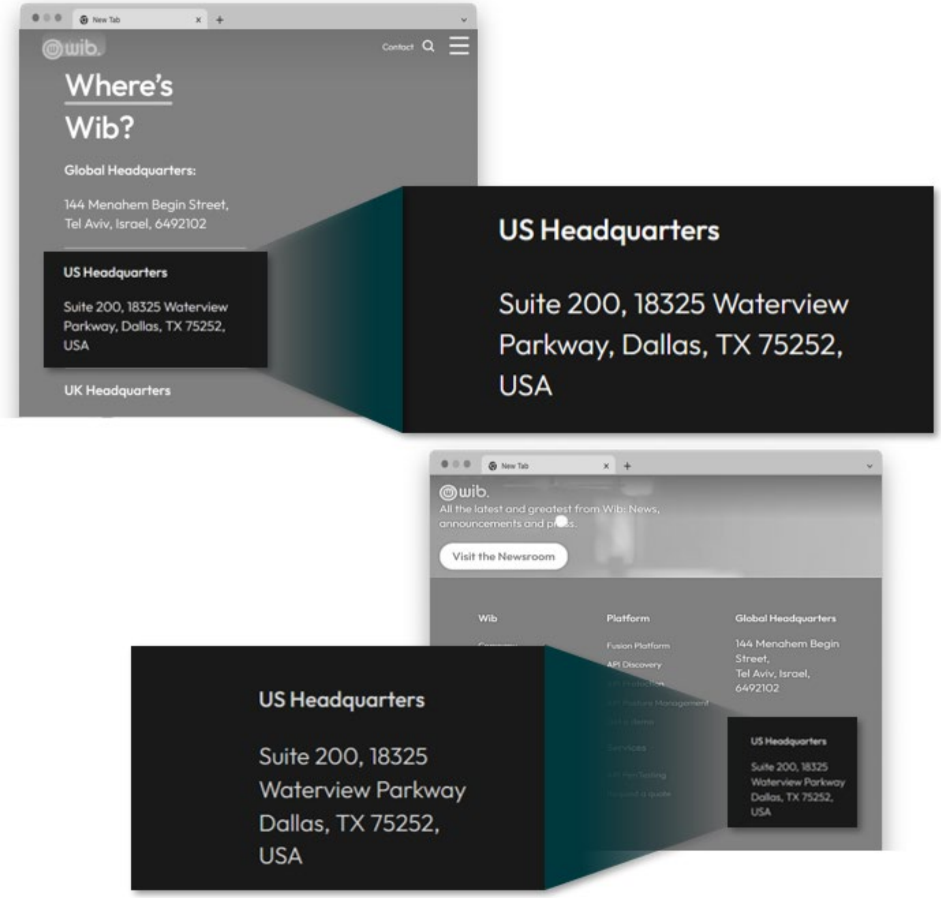
F5 Distributed Cloud API Security

Automatically discover endpoints mapped to your applications, allow or deny list unwanted connections, and monitor for anomalous behavior.

Try out the simulator

WIB SECURITY WEBSITE, HOME PAGE, available at: https://wib.com/ (image captured February 21, 2024) (searching "wib" in the search functionality on the Wib Security home page or clicking on "Explore the Platform"); F5 WEBSITE, API-SECURITY WEBPAGE, available at: https://www.f5.com/cloud/products/api-security (image captured February 21, 2024) (showing the webpage that comes up after searching "wib" in the search functionality of the Wib Security home page shown in the images above).

16. F5 continues to engage in business in the Eastern District of Texas. The following are two screenshots of web pages maintained by F5 following its acquisition of Wib Security, listing its U.S. Headquarters as located at 18325 Waterview Parkway Dallas, Texas 75252 (located within the Eastern District of Texas).



Where's Wib?

Global Headquarters:

144 Menahem Begin Street,
Tel Aviv, Israel, 6492102

US Headquarters

Suite 200, 18325 Waterview Parkway, Dallas, TX 75252, USA

UK Headquarters

US Headquarters

Suite 200, 18325 Waterview Parkway, Dallas, TX 75252, USA

All the latest and greatest from Wib: News, announcements and press.

Global Headquarters

144 Menahem Begin Street,
Tel Aviv, Israel,
6492102

US Headquarters

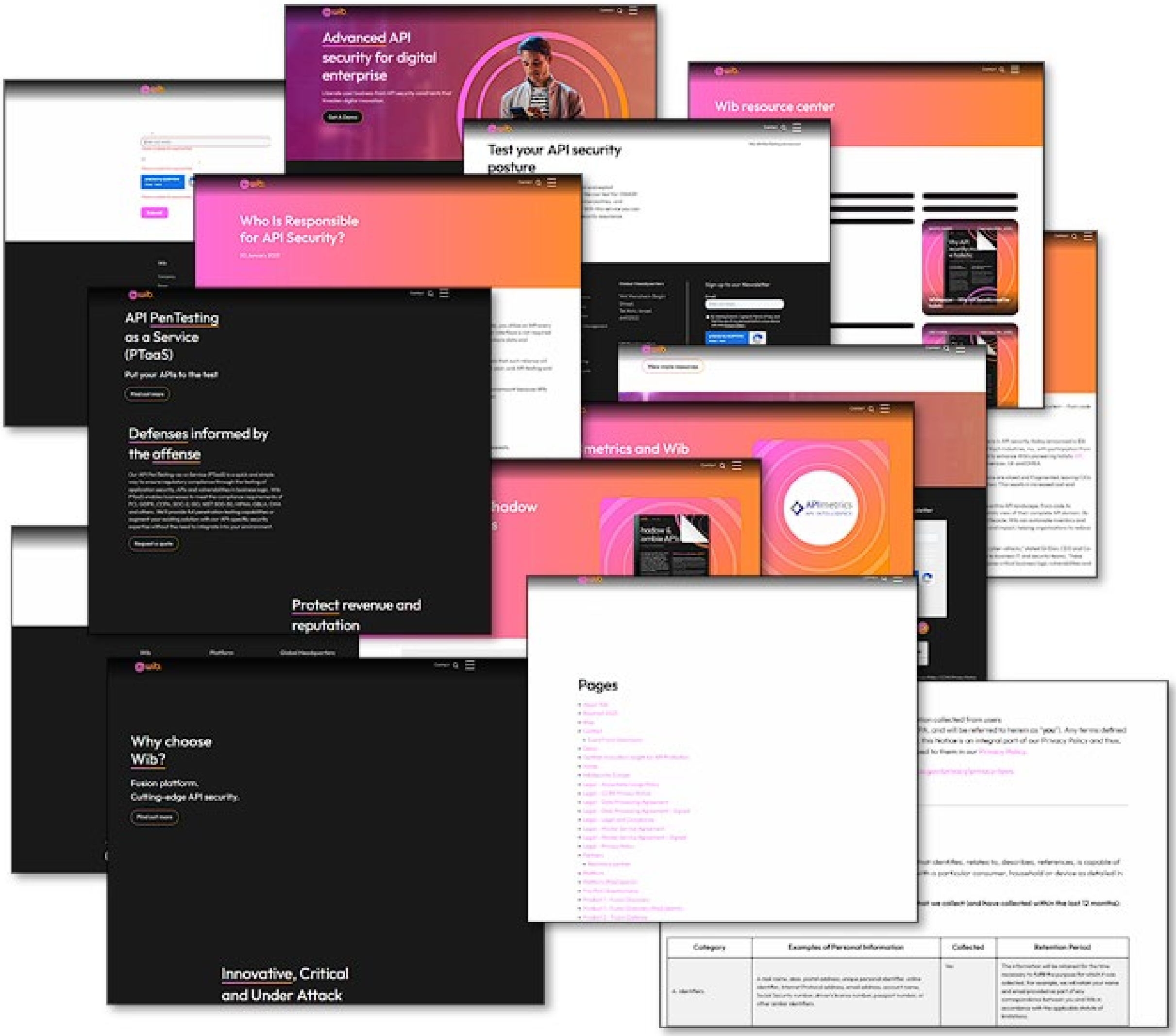
Suite 200, 18325
Waterview Parkway
Dallas, TX 75252,
USA

US Headquarters

Suite 200, 18325
Waterview Parkway
Dallas, TX 75252,
USA

Contact Us | Wib API Security, WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/contact-us/ and *Wib Resource Archive,* WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/resource-center/ (annotation added).

17. The following are selected screenshots of the 33 separate web pages maintained by F5 following its acquisition of Wib Security identifying its U.S. Headquarters as located at 18325 Waterview Parkway Dallas, Texas 75252 (located within the Eastern District of Texas).


Advanced API security for digital enterprise
Wib resource center
Test your API security posture
Who Is Responsible for API Security?
API PenTesting as a Service (PTaaS)
Put your APIs to the test
Defenses informed by the offense
Protect revenue and reputation
metrics and Wib
APImetrics
Pages
Why choose Wib?
Fusion platform. Cutting-edge API security.
Innovative, Critical and Under Attack
Category
Examples of Personal Information
Collected
Retention Period

See e,g., Securing APIs through the lens of NIST | Wib WOW Blog, WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/blog/; *Fusion Defense - Holistic API Security - Wib,* WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/fusion-defense/; *Wib News - APImetrics Partner with Wib Security,* WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/news/; *API Security Posture Management | Wib Fusion Analysis,* WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/fusion-analysis/; *Contact Us | Wib API Security,* WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/contact-us/; *Wib API Security Services*, WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/services/; *Wib: API Security Solutions | Protecting The Digital Economy*, WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/; *API security company Wib raise $16m investment,* WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/news/; *Wib Resource Archive,* WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/resource-center/; *Legal and compliance - Wib*, WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/legal-and-compliance/; *Gartner Innovation Insight for API Protection - Wib*, WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/gartner-innovation-insight-for-api-protection/; *Secure a Fusion platform demo - Wib,* WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/demo/; *Use Cases - Cryptocurrency - Wib*, WIB.COM WEBSITE (last visited February 21, 2024), available at:

https://wib.com/resources/; *Wib Partners*, WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/partners/; *Who is responsible for API security? - Wib,* WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/blog/; *Use Cases - Shadow & Zombie APIs - Wib*, WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/resources/; *API Pentesting As A Service | Put Your APIs To The Test,* WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/services/; *Why choose Wib for API security*, WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/why-wib/; *Legal – CCPA Privacy Notice - Wib,* WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/ccpa-notice/; *Use Cases - BOLA Attacks - Wib,* WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/resources/; *Coinbase API Security Nightmare - Wib,* WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/blog/; *API Pen Testing Request - Wib,* WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/services/; *Wib Brand Guidelines,* WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/our-brand/; *Wib Use Cases - Resource Center*, WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/resources-categories/use-cases/; *Wib News - Wib Launch API Risk Management Module*, WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/news/; *Wib API Security Webinars*, WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/api-security-webinars/; *Wib News - Wib Launch API Security Compliance Module,* WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/news/; *Wib Achieves Industry Recognition Following Record Year*, WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/news/; *WOW Blog - API Security Blog - Wib,* WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/wow-blog/; *API Documentation & Discovery Tool | Wib Fusion Discovery,* WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/fusion-discovery/; *Wib Signs Kite Distribution as First Distribution Partner in ...,* WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/news/; and *Sitemap - Wib,* WIB.COM WEBSITE (last visited February 21, 2024), available at: https://wib.com/sitemap/.

JURISDICTION AND VENUE

18. This action arises under the patent laws of the United States, Title 35 of the United States Code. Accordingly, this Court has exclusive subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

19. This Court has personal jurisdiction over F5 in this action because F5 has committed acts within the Eastern District of Texas giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over F5 would not offend traditional notions of fair play and substantial justice. Defendant F5, directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the patents-in-suit. Moreover, F5 is registered to

do business in the State of Texas, has offices and facilities in the State of Texas, and actively directs its activities to customers located in the State of Texas.

20. Venue is proper in this District under 28 U.S.C. §§ 1391(b)-(d) and 1400(b). Defendant F5 has offices in the State of Texas, has transacted business in the Eastern District of Texas and has committed acts of direct and indirect infringement in the Eastern District of Texas.

21. F5 has a regular and established place of business in this District and has committed acts of infringement in this District. F5 has a permanent office location at 18325 Waterview Parkway Dallas, Texas 75252, both of which are located within this District. F5 employs full-time personnel such as sales personnel and engineers in this District, including in Collin County, Texas. F5 has also committed acts of infringement in this District by commercializing, marketing, selling, distributing, testing, and servicing certain Accused Products.

22. This Court has personal jurisdiction over F5. F5 has conducted and does conduct business within the State of Texas. F5, directly or through subsidiaries or intermediaries (including distributors, retailers, and others), ships, distributes, makes, uses, offers for sale, sells, imports, and/or advertises (including by providing an interactive web page) its products and/or services in the United States and the Eastern District of Texas and/or contributes to and actively induces its customers to ship, distribute, make, use, offer for sale, sell, import, and/or advertise (including the provision of an interactive web page) infringing products and/or services in the United States and the Eastern District of Texas. F5, directly and through subsidiaries or intermediaries (including distributors, retailers, and others), has purposefully and voluntarily placed one or more of its infringing products and/or services, as described below, into the stream of commerce with the expectation that those products will be purchased and used by customers and/or consumers in the Eastern District of Texas. These infringing products and/or services have been and continue to be

made, used, sold, offered for sale, purchased, and/or imported by customers and/or consumers in the Eastern District of Texas. F5 has committed acts of patent infringement within the Eastern District of Texas. F5 interacts with customers in Texas, including through visits to customer sites in Texas. Through these interactions and visits, F5 directly infringes the patents-in-suit. F5 also interacts with customers who sell the Accused Products into Texas, knowing that these customers will sell the Accused Products into Texas, either directly or through intermediaries.

23. F5 has minimum contacts with this District such that the maintenance of this action within this District would not offend traditional notions of fair play and substantial justice. Thus, the Court therefore has both general and specific personal jurisdiction over F5.

THE ASSERTED PATENTS

U.S. PATENT NO. 7,099,273

24. U.S. Patent No. 7,099,273 (the "'273 patent") entitled, *Data Transport Acceleration and Management Within a Network Communication System,* was filed on January 29, 2002. The '273 patent is subject to a 35 U.S.C. § 154(b) term extension of 1,021 days. The '273 patent claims priority to U.S. Provisional Patent Application No. 60/309,212 filed on July 31, 2001, and U.S. Provisional Patent Application No. 60/283,542 filed on April 12, 2001. A true and correct copy of the '273 patent is attached hereto as Exhibit 1.

25. The '273 patent has been in full force and effect since its issuance. OptiMorphix, Inc. owns by assignment the entire right, title, and interest in and to the '273 patent.

26. The technologies disclosed in the '273 patent improve the efficiency and speed of data transmission within network communication systems. The '273 patent introduces methods and apparatuses that enhance data transport, especially in environments where network conditions

are variable or unpredictable and “provide systems and method for data transport acceleration and management within a network communication system.” ‘273 patent, col. 3:31-33.

27. The ‘273 patent is directed to solving the problem of inefficient data transport within network communication systems. This inefficiency can lead to poor utilization of network resources, increased latency, and reduced overall performance.

28. The ‘273 patent identifies the shortcomings of the prior art. Specifically, the specification describes that traditional methods of data transport in network communication systems often fail to efficiently manage and accelerate data transport, especially in environments with variable or unpredictable network conditions. These methods may not adequately handle network congestion, leading to poor utilization of network resources, increased latency, and reduced overall performance. “This bursty nature of data transmission may under-utilize the available bandwidth on the downlink channel, and may cause some applications requiring a steady flow of data, such as audio or video, to experience unusually poor performance.” ‘273 patent, col. 2:1-6.

29. The ‘273 patent identifies several shortcomings of the prior art, particularly in the context of the Transport Control Protocol (TCP) which is commonly used in modern data communication networks. The patent specification describes that:

> Many of the problems associated with conventional TCP architectures stem from the flow control, congestion control and error recovery mechanisms used to control transmission of data over a communication network.

‘273 patent, col. 1:38-41.

30. Conventional TCP architectures assume that the network employs symmetric communication channels that enable data packets and acknowledgements to be equally spaced in time. This assumption often does not hold true in networks that employ asymmetric uplink and downlink channels, such as wireless communication networks. Bursty data transmission might

result in the inefficient use of the available bandwidth on the downlink channel, leading to suboptimal performance in applications that need a consistent data flow, such as those involving audio or video.

31. Another shortcoming identified is that conventional TCP architectures react to both random loss and network congestion by significantly and repeatedly reducing the congestion window, which can lead to significant and potentially unjustified deterioration in data throughput. This is particularly problematic in wireless and other bandwidth constrained networks where random packet loss due to fading, temporary degradation in signal quality, signal handoffs or large propagation delays occur with relatively high frequency.

32. The ‘273 patent also points out that conventional TCP congestion control mechanisms tend to exhibit sub-optimal performance during initialization of data connections over reduced-bandwidth channels, such as wireless links. When a connection is initiated, the congestion control mechanism aggressively increases the size of the congestion window until it senses a data packet loss. This process may adversely impact other connections that share the same reduced-bandwidth channel as the connection being initialized attempts to maximize its data throughput without regard of the other pre-existing connections. This can lead to inefficient use of resources with decreased overall throughput.

33. The ‘273 patent teaches the use of various techniques to accelerate and manage data transport in network communication systems. These techniques include the use of congestion control mechanisms, timers, and other methods to optimize data transmission. By implementing these techniques, the patent aims to improve the efficiency of data transport, particularly in environments with variable or unpredictable network conditions. This can lead to better utilization of network resources, reduced latency, and improved overall performance. The inventions

disclosed in the ‘273 patent provide significant benefits and improvements to the function of the hardware in a computer network.

34. The ‘273 patent family has been cited by 1,466 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies and research institutions have cited the ‘273 patent family as relevant prior art:

- Cisco Technology, Inc.
- Qualcomm Incorporated
- International Business Machines Corporation
- Intel Corporation
- Microsoft Corporation
- Broadcom Corporation
- Google Inc.
- F5 Networks, Inc.
- Adobe Systems Incorporated
- Apple Inc.
- Lumen Technologies, Inc
- Oracle Corporation
- Amazon.com, Inc.

U.S. PATENT NO. 7,136,353

35. U.S. Patent No. 7,136,353 (the "‘353 patent") entitled, *Quality of Service Management for Multiple Connections Within a Network Communication System*, was filed on May 17, 2002. The ‘353 patent claims priority to Provisional Application No. 60/309,212, filed on July 31, 2001 and Provisional Application No. 60/291,825, filed on May 18, 2001. The ‘353 patent is subject to a 35 U.S.C. § 154(b) term extension of 945 days. A true and correct copy of the ‘353 patent is attached hereto as Exhibit 2.

36. The ‘353 patent has been in full force and effect since its issuance. OptiMorphix, Inc. owns by assignment the entire right, title, and interest in and to the ‘353 patent.

37. The ‘353 patent primarily relates to managing the quality of service (QoS) in a network communication system, especially focusing on multiple connections between a sender

and a receiver. It introduces a methodology where a host-level transmission rate is allocated among multiple connections based on a ratio of a weight associated with each connection and the sum of the weights associated with the connections. This approach aims to optimize the transmission of data packets, particularly in environments where multiple connections to the same host might compete for bandwidth, ensuring efficient utilization and prioritization of data transmission.

38. The ‘353 patent is directed to solving the problem of efficiently managing multiple connections in a network communication system to optimize data packet transmission and improve the quality of service. It addresses issues related to the allocation of transmission rates among multiple connections, selective transmission of data packets, and ensuring that higher priority connections are allocated a more significant portion of the available transmission rate than lower priority connections.

39. The ‘353 patent identifies shortcomings in the prior art. Specifically, the specification describes that conventional Transport Control Protocol (TCP) architectures, which were primarily designed for reliable, sequenced transmission of non-real-time data streams over high-bandwidth wireline channels, tend to exhibit sub-optimal performance when employed in environments with different or incompatible characteristics, such as wireless networks. Traditional TCP architectures face issues related to flow control, congestion control, and error recovery mechanisms, especially in scenarios involving multiple connections between a sender and a receiver, leading to inefficient use of resources and decreased overall throughput.

40. The inventions disclosed in the ‘353 patent provide significant benefits and improvements to the function of the hardware in a computer network by ensuring that data transmission across multiple connections is managed efficiently and prioritized according to the

significance of each connection. The methodology ensures that higher priority connections are allocated more bandwidth, reducing bursty data transmissions and ensuring that data is transmitted at a rate that the communication channel can support, thereby optimizing the utilization of network resources and enhancing the overall quality of service.

41. The invention taught by the ’353 patent solves discrete, technological problems associated with computer systems; specifically, it addresses the technical challenges related to managing and optimizing data packet transmission across multiple connections in a network communication system. It provides a systematic approach to allocate transmission rates, manage data packet transmission, and prioritize connections, ensuring efficient utilization of network resources and improved quality of service.

42. The technologies taught in the ‘353 patent constitute an improvement in computer network technology by introducing a systematic and efficient methodology to manage multiple connections in a network communication system. The teachings in the ‘353 patent provide a mechanism to allocate transmission rates among connections, selectively transmit data packets, and prioritize connections based on associated weights, ensuring that higher priority connections are allocated a more significant portion of the available transmission rate, thereby optimizing data transmission and enhancing the quality of service in network communication systems.

43. The ‘353 patent family has been cited by 1,469 United States and international patents and patent applications as relevant prior art. Specifically, 77 United States and international patents and patent applications have cited the ‘353 patent itself as relevant prior art. The following companies and research institutions have cited the ‘353 patent as relevant prior art:

- Broadcom Limited
- Cisco Systems, Inc.
- CommScope, Inc.
- Intel Corporation

- Interdigital, Inc.
- Lumen Technologies, Inc
- Microsoft Corporation
- NEC Corporation
- NetApp Inc.
- Nokia Corporation
- Oracle Corporation
- Panasonic Corporation
- Rensselaer Polytechnic Institute
- Samsung Electronics Co., Ltd.
- Telefonaktiebolaget Lm

U.S. PATENT NO. 7,586,871

44. U.S. Patent No. 7,586,871 (the "'871 patent") entitled, *Platform and Method for Providing Data Services in a Communication Network*, was filed on January 11, 2006. The '871 patent claims priority to U.S. Application Ser. No. 10/061,953, which was filed on February 2, 2002, which claims the benefit of U.S. Provisional Applications No. 60/292,564, which was filed on May 22, 2001, and No. 60/293,756, which was filed on May 25, 2001. The '871 patent also claims the benefit of U.S. Provisional Application No. 60/654,730, which was filed on February 18, 2005. The '871 patent is subject to a 35 U.S.C. § 154(b) term extension of 748 days. A true and correct copy of the '871 patent is attached hereto as Exhibit 3.

45. The '871 patent has been in full force and effect since its issuance. OptiMorphix, Inc. owns by assignment the entire right, title, and interest in and to the '871 patent.

46. The '871 patent generally relates to a communication node and corresponding method for processing data communications passing through the node between a first data network and a second data network. The method includes detecting an event associated with data communication arriving at the node from the first data network, determining whether the data communication is to be suspended for service at the node based on the detected event, and processing suspended data communication based on information in the data communication. The

patent also covers the detection of return data communication arriving at the node from the second data network in response to the processed data communication from the first data network. The detected return data communication is allowed to pass through the node without processing the detected return data communication.

47. The ‘871 patent is directed to solving the problem of efficiently providing data services, such as content filtering, in a communication network. This includes the ability to determine whether a packet flow should be suspended for filtering a content request based on packet flow characteristics detected at the layers implemented in hardware, without the need for assistance from higher layers in the architecture implemented in software.

48. The ‘871 patent teaches the use of a communication node that processes data communication between two networks. This node detects an event associated with data communication from the first network, determines whether the data communication should be suspended for service at the node based on the detected event, and processes suspended data communication based on information in the data communication. The ‘871 patent also teaches the detection of return data communication from the second network in response to the processed data communication from the first network, allowing this return data communication to pass through the node without further processing. This approach allows for more efficient processing of data communication, reducing the need to inspect every packet in a flow and avoiding the need to terminate or establish a communication session associated with the data communication.

49. The inventions disclosed in the ‘871 patent provide significant benefits and improvements to the function of the hardware in a computer network. Specifically, the inventions taught by the ‘871 patent can determine whether a packet flow should be suspended for filtering a content request based on packet flow characteristics detected at the layers implemented in

hardware. This improves the efficiency and scalability of content filtering and other services, particularly for mobile data networks that carry delay-sensitive traffic such as voice or video streaming traffic.

50. The ‘871 patent family has been cited by 962 United States and international patents and patent applications as relevant prior art. 166 United States and international patents and patent applications have cited the ‘871 patent itself as relevant prior art. The following companies and research institutions have cited the ‘871 patent as relevant prior art:

- A10 Networks, Inc.
- Thoma Bravo, LLC
- AT&T, Inc.
- NEC Corporation
- Nokia Corporation
- Cisco Systems, Inc.
- Juniper Networks, Inc.
- Fujitsu Limited

U.S. PATENT NO. 7,616,559

51. U.S. Patent No. 7,616,559 (the "‘559 patent") entitled, *Multi-Link Network Architecture, Including Security, In Seamless Roaming Communications Systems And Methods*, was filed on September 2, 2004. The ‘559 patent claims priority to Provisional Application No. 60/499,648, which was filed on September 3, 2003. The ‘559 patent is subject to a 35 U.S.C. § 154(b) term extension of 638 days. A true and correct copy of the ‘559 patent is attached hereto as Exhibit 4.

52. The ‘559 patent has been in full force and effect since its issuance. OptiMorphix, Inc. owns by assignment the entire right, title, and interest in and to the ‘559 patent.

53. The ‘559 patent generally relates to a communications system that provides secure communications of information over multiple communication links. This system includes a client

device, a server device, and at least one communication channels, elements, modes, and links for connecting the devices for communication of information between them. The system includes a link detector for determining the existence and usability of the communication links for communication of the information, a pathfinder for selecting one or more of the communication links for communication of at least some of the information, a link handover for switching to the selected one or more communication links for communication of the information or portion thereof, and an auto reconnector for re-connecting to detected and selected one or more communication links for communication of the information or portions of it in the event that any communication is hindered, terminated, or upset.

54. The '559 patent is directed to solving the problem of ensuring secure and reliable communication over multiple communication links, especially in environments that include mobile or other roaming devices capable of communicating over multiple channels and with channel switching characteristics.

55. The '559 patent identifies the shortcomings of the prior art. Specifically, the specification describes that when multiple links, both physical elements and the bands or channels within each such element, are employed for communications in data networks, substantial coordination of communicated information, as well as security of the information, is exponentially complicated. In wireless communications, concurrent or sequential operations can occur over cellular or wireless LAN technologies. Each of these wireless communications methods experiences substantially greater complexity in timing, security, packet sequencing, data loss, and connectivity, over wired communications conditions.

56. The '559 patent teaches the use of a system that includes a link detector for determining the existence and usability of the communication links for communication of the

information, a pathfinder for selecting one or more of the communication links for communication of at least some of the information, a link handover for switching to the selected one or more communication links for communication of the information or portion thereof, and an auto reconnector for re-connecting to detected and selected one or more communication links for communication of the information or portions of it in the event that any communication is hindered, terminated, or upset.

57. The inventions disclosed in the ‘559 patent provide significant benefits and improvements to the function of the hardware in a computer network by ensuring secure and reliable communication over multiple communication links. This is particularly beneficial in environments that include mobile or other roaming devices capable of communicating over multiple channels and with channel switching characteristics. The system’s ability to detect usable communication links, select the most suitable ones, switch between them as needed, and reconnect in the event of communication disruption greatly enhances the reliability and efficiency of data transmission in a computer network.

58. The ‘559 patent family has been cited by 17 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies and research institutions have cited the ‘559 patent family as relevant prior art:

- International Business Machines Corporation
- Samsung Electronics Co., Ltd
- Alphabet Inc.
- Research In Motion Limited
- BT Group plc

U.S. Patent No. 8,429,169

59. U.S. Patent No. 8,429,169 (the “‘169 patent”) entitled, *Systems and Methods For Video Cache Indexing*, was filed on July 29, 2011. The ‘169 patent claims priority to U.S.

Provisional Patent Application No. 61/369,513, which was filed on July 30, 2010. A true and correct copy of the '169 patent is attached hereto as Exhibit 5.

60. The '169 patent has been in full force and effect since its issuance. OptiMorphix, Inc. owns by assignment the entire right, title, and interest in and to the '169 patent.

61. The '169 patent is directed to solving the problem of inefficient caching of content, particularly when dynamic URLs are used to refer to the content. Traditional caching methods that index content based on URLs can lead to multiple cache entries for the same content or entries with expired references, reducing the efficiency and capacity of the cache. The technologies taught in the '169 patent overcomes these inefficiencies by indexing the content cache based on a characterization of the content rather than the URL.

62. The '169 patent identifies the shortcomings of the prior art. Specifically, that conventional content caching methods, especially those employing dynamic URLs, lead to two main inefficiencies: (a) multiple cache entries corresponding to the same video content, thereby reducing the cache's capacity to serve unique content, and (b) content cache entries with expired references to content, reducing the useful capacity of the content cache. These inefficiencies hinder the performance of middleware services and website performance.

63. The '169 patent teaches the use of a novel approach to cache video content by indexing the content cache based on a characterization of the video content rather than the URL. This method involves identifying characterization data related to the content request and using a hash function to generate an index. This index is then used to identify the corresponding entry in the cache data structure. By avoiding the use of dynamic URLs in the indexing process, the patent's method allows for more efficient caching, eliminating redundancies and invalid entries, and improving the overall efficiency of content delivery.

64. The inventions disclosed in the '169 patent provide significant benefits and improvements to the function of the hardware in a computer network by enabling more efficient caching of video content. By indexing the content cache based on the characterization of the content rather than the URL, the patented method avoids the problems of redundant and invalid cache entries. This leads to better utilization of cache capacity, reduced burden on network infrastructure and web servers, and faster content delivery to users. The invention also allows for distinguishing between similar but non-identical videos, avoiding content aliasing, and ensuring that the correct content is delivered to the user.

65. The '169 patent family has been cited by 92 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies and research institutions have cited the '169 patent family as relevant prior art:

- Akamai Technologies, Inc.
- AMC Networks Inc.
- AT&T Inc.
- Atlassian Pty Ltd
- Canon Inc.
- Charter Communications, Inc.
- China Mobile Communications Corporation
- EchoStar Corporation
- Huawei Investment & Holding Co., Ltd.
- Interdigital, Inc.
- Juniper Networks, Inc.
- Koninklijke Philips Nv
- Microsoft Corporation
- Open Text Corporation
- SK Telecom Co., Ltd.
- Skyfire Labs, Inc., California
- ZTE Corporation

U.S. PATENT NO. 8,521,901

66. U.S. Patent No. 8,521,901 (the "'901 patent") entitled, *TCP Burst Avoidance*, was filed on December 22, 2008. The '901 patent claims priority to Provisional Patent Application

No. 61/017,275, filed on December 28, 2007. The ‘901 patent is subject to a 35 U.S.C. § 154(b) term extension of 525 days. A true and correct copy of the ‘901 patent is attached hereto as Exhibit 6.

67. The ‘901 patent has been in full force and effect since its issuance. OptiMorphix, Inc. owns by assignment the entire right, title, and interest in and to the ‘901 patent.

68. The ‘901 patent generally relates to methods and systems for minimizing packet bursts. The ‘901 patent teaches implementing a packet scheduler layer between the network layer and the transport layer of a device, which smooths the delivery of TCP packets by delaying their delivery, thus addressing the challenges posed by the rapid and bursty transmission of data packets in network communications.

69. The ‘901 patent is directed to solving the problem of TCP packet bursts in high-speed data networks, which can result from the buffering of TCP acknowledgment packets. These bursts can cause packet loss and inefficient use network bandwidth.

70. The ‘901 patent identifies the shortcomings of the prior art. Specifically, the specification describes that the prior art does not adequately address the issues of packet loss and inefficient bandwidth utilization resulting from the bursty nature of TCP packet transmission in data networks. The prior technologies do not effectively manage the sudden bursts of TCP acknowledgment packets, which can be caused by buffering, leading to suboptimal utilization of available bandwidth and undesirable packet loss.

71. The ‘901 patent teaches the use of a packet scheduler layer, which is positioned between the network and transport layers of a device. This layer receives, smoothens (by delaying), and sends TCP packets to ensure that the delivery of these packets is managed in a manner that mitigates the issues of packet bursts. The packet scheduler layer manages both

incoming and outgoing packets, ensuring that the transmission of these packets is smoothed out, thereby minimizing packet loss and ensuring more efficient use of available bandwidth. This approach provides benefits that differ from conventional methods by ensuring that TCP packet transmission is managed in a way that minimizes packet loss and ensures efficient bandwidth utilization, thereby addressing the specific challenges posed by TCP packet bursts in high-speed data networks.

72. The invention taught by the ’901 patent solves discrete, technological problems associated with computer systems; specifically, it addresses the issues of packet loss and inefficient bandwidth utilization in high-speed data networks by managing the transmission of TCP packets in a manner that smoothens their delivery, thereby ensuring that the available bandwidth is utilized efficiently, and that packet loss is minimized.

73. The ‘901 patent family has been cited by 21 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘901 patent family as relevant prior art:

- Lenovo Group Limited
- Telefonaktiebolaget Lm Ericsson
- Qualcomm, Inc.
- Nippon Telegraph & Telephone Corp.
- Hitachi, Ltd.
- Cisco Systems, Inc.
- Akamai Technologies, Inc.
- Huawei Technologies Co., Ltd.

U.S. PATENT NO. 9,936,040

74. U.S. Patent No. 9,936,040 (the “‘040 patent”) entitled, *Systems and Methods of Partial Video Caching*, was filed on December 19, 2014. The ‘040 patent is subject to a 35 U.S.C.

§ 154(b) term extension of 336 days. A true and correct copy of the '040 patent is attached hereto as Exhibit 7.

75. The '040 patent has been in full force and effect since its issuance. OptiMorphix, Inc. owns by assignment the entire right, title, and interest in and to the '040 patent.

76. The '040 patent relates to systems and methods for caching and keying segments for efficient data retrieval. The '040 patent outlines a technical framework that stores a set of instructions for acquiring, storing, and managing segments of data (e.g., video, image, and audio files) in response to requests generated by client devices. This framework is designed to optimize the delivery of content over networks by reducing the amount of data that needs to be transmitted from content servers to client devices, thereby decreasing network congestion and improving the efficiency of content delivery.

77. The '040 patent is directed to solving the problem of high network congestion and inefficient use of network resources caused by the delivery of large content files over the Internet. This issue places a substantial processing load on the network infrastructure and web servers, particularly affecting networks employing wireless technology, which generally offer lower throughput and suffer from greater packet loss and location-dependent throughput variations compared to wired networks.

78. The '040 patent identifies the shortcomings of the prior art by highlighting the inefficiencies in existing methods of content delivery. The specification describes that traditional methods do not adequately address the challenges of real-time streaming adjustments, such as bitrate and frame resolution changes, especially in formats like MPEG-4 Part 14 (MP4), which require advance transmission of index data. This limitation significantly constrains the ability to

adjust the bitrate in real-time, leading to inefficient use of network resources and a degraded user experience.

79. The ‘040 patent teaches the use of a cache server to store segments of data associated with user requests. This approach involves acquiring segments from a content server, storing these segments if they meet certain criteria (e.g., exceeding a threshold value), and generating keys for efficient retrieval. By caching only parts of the media data that are likely to be requested again, the system reduces the need for repeated data transmissions from the content server, thereby alleviating network congestion and improving content delivery efficiency.

80. The inventions disclosed in the ‘040 patent provide significant benefits and improvements to the function of the hardware in a computer network by optimizing the delivery of data. This is achieved through a reduction in the amount of data that needs to be transmitted across the network, which not only decreases network congestion but also minimizes the processing load on network infrastructure and web servers. As a result, the network and server capacity can be utilized more effectively, enabling a larger number of users to be served with electronic data without necessitating a proportional increase in network or server resources.

81. The inventions taught by the ’040 patent solve discrete, technological problems associated with computer systems and networks, particularly those related to the efficient delivery and caching of large amounts of data. These problems are inherently technical because they involve optimizing network resource usage, reducing bandwidth consumption, and improving the scalability of content delivery systems. The solutions provided by the ‘040 patent address these challenges by introducing innovative methods for partial caching and content delivery optimization, which are crucial for enhancing the performance and reliability of modern computer networks.

82. The ‘040 patent family has been cited by 26 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies and research institutions have cited the ‘040 patent family as relevant prior art:

- Cisco Systems, Inc.
- Comcast Corporation
- EchoStar Corporation
- Salesforce, Inc.
- Telefonaktiebolaget Lm Ericsson
- Tencent Holdings Ltd
- Hughes Network Systems, LLC
- Verizon Digital Media Services Inc.

U.S. PATENT NO. 10,264,093

83. U.S. Patent No. 10,264,093 (the "‘093 patent") entitled, *Systems and Methods for Partial Video Caching*, was filed on March 5, 2018. The ‘093 patent claims priority to U.S. Patent Application No. 14/577,078, which was filed on December 19, 2014. A true and correct copy of the ‘093 patent is attached hereto as Exhibit 8.

84. The ‘093 patent has been in full force and effect since its issuance. OptiMorphix, Inc. owns by assignment the entire right, title, and interest in and to the ‘093 patent.

85. The ‘093 patent relates to advanced methods and systems for caching content in a network environment. It specifically addresses the optimization of content delivery by employing a cache server equipped with memory and processors. Each segment of data is associated with a unique key, facilitating efficient retrieval and management of cached content. This approach aims to reduce network congestion and enhance the delivery efficiency of content by intelligently caching and serving content segments.

86. The ‘093 patent is directed to solving the problem of inefficient content delivery over networks, particularly in scenarios where network congestion and bandwidth limitations impair the user experience. It addresses the challenges associated with delivering high-quality

content to a large number of users simultaneously, without incurring excessive bandwidth costs or causing significant delays.

87. The ‘093 patent identifies the shortcomings of the prior art by highlighting the inefficiencies in traditional content delivery methods. Specifically, the specification describes that prior systems failed to adequately address the dynamic nature of content consumption, where different users may request different segments of the same content at varying times. This resulted in redundant data transmissions and inefficient use of network resources, leading to increased latency and decreased quality of service.

88. The ‘093 patent teaches the use of a sophisticated caching mechanism that stores segments of content based on their popularity and request frequency. By generating unique keys for each segment and employing algorithms to predict which segments are likely to be requested, the system can preemptively cache and serve content more efficiently. This approach significantly reduces the need for repetitive data transmissions from the content server, thereby alleviating network congestion and enhancing user experience.

89. The inventions disclosed in the ‘093 patent provide significant benefits and improvements to the function of hardware in a computer network by optimizing data flow and reducing the load on network infrastructure. This is achieved through intelligent caching strategies that minimize redundant data transfers, thereby conserving bandwidth and improving the responsiveness of content delivery services. Additionally, the system's ability to adapt to changing content popularity patterns ensures that network resources are allocated efficiently, supporting a higher quality of service for a larger user base.

90. The inventions taught by the ’093 patent solve discrete, technological problems associated with computer systems; specifically, the inventions address the challenges of scaling

content delivery to meet the demands of a growing number of users. These challenges are inherently technical, involving complex considerations of data management, network bandwidth optimization, and user experience enhancement.

91. The technologies taught in the ‘093 patent constitute an improvement in computer network technology by introducing a more adaptive and efficient method for content caching and delivery. This approach leverages advanced algorithms to predict demand for specific content segments, enabling the system to cache and serve content more effectively. Such improvements not only enhance the scalability of content delivery systems but also contribute to the development of more sophisticated content distribution networks (CDNs) capable of supporting high-quality content delivery services.

92. The claim language of the ‘093 patent is directed to detailed and particular features that distinguish its approach from conventional methods. The ‘093 patent specifies the mechanisms for segment-based caching, unique key generation for each content segment, and the criteria for caching based on segment popularity. These features demonstrate how the invention operates to reduce network congestion and improve content delivery efficiency, offering clear benefits over well-known, conventional, and routine approaches. The specificity of the claims underscores the novelty of the patent, highlighting its contribution to advancing the state of content delivery technologies.

93. The ‘093 patent family has been cited by 26 United States and international patents and patent applications as relevant prior art. The following companies and research institutions have cited the ‘093 patent family as relevant prior art:

- Cisco Systems, Inc.
- Comcast Corporation
- EchoStar Corporation
- Salesforce, Inc.

- Telefonaktiebolaget Lm Ericsson
- Tencent Holdings Ltd
- Hughes Network Systems, LLC
- Verizon Digital Media Services Inc.

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 7,099,273

94. Plaintiff references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

95. F5 designs, makes, uses, sells, and/or offers for sale in the United States products comprising systems and methods for data transport acceleration and management within a network communication system.

96. F5 designs, makes, sells, offers to sell, imports, and/or uses the following products: BIG-IP Versions 14.1.x and later, F5 BIG-IP iSeries Platform Appliances running BIG-IP Versions 14.1.0 and later; F5 VELOS Chassis and Blades running BIG-IP Versions 14.1.x and later; F5 VIPRION Chassis and Blades running BIG-IP Versions 14.1.x and later; and BIG-IP Virtual Edition (VE) Versions 14.1.X and later (collectively, the "F5 '273 Product(s)").

97. One or more F5 subsidiaries and/or affiliates use the F5 '273 Products in regular business operations.

98. One or more of the F5 '273 Products include technology that performs the step of establishing a data connection between a sender and receiver using a handshake process.

99. The F5 '273 Products send a TCP packet with the SYN (Synchronize) flag set to the server. This packet contains an initial sequence number (ISN), which helps the server and client synchronize their sequence numbers. The ISN used by the F5 '273 Products are represented as "x." Upon receiving the SYN packet, the F5 '273 Products sends a TCP packet back with both the SYN and ACK flags set. This packet contains two pieces of information: the responsive ISN,

usually represented as 'y,' and an acknowledgment number, which is the ISN plus one (x+1). The acknowledgment number is used to confirm that the sender has received the SYN packet.

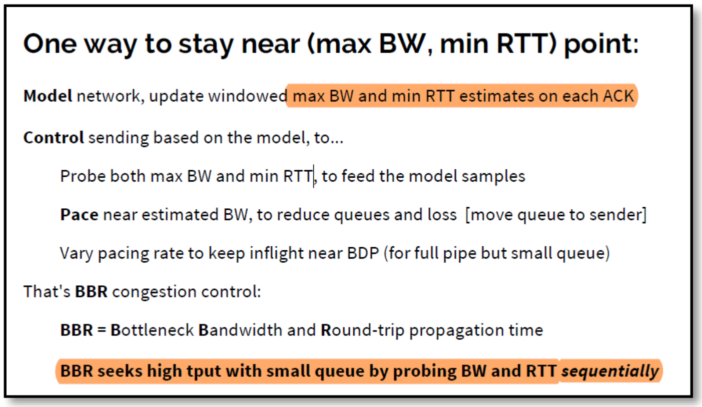
100. In establishing a connection between the sender and the receiver after receiving the SYN-ACK packet, the F5 '273 Products send another packet with the ACK flag set. This packet contains an acknowledgment number, which is the ISN plus one (y+1).

101. The F5 '273 Products measure round trip times (RTT) of packets sent between a client and server over a network. Specifically, the F5 '273 Products measure the round-trip propagation time (RTprop) using the minimum round-trip time (RTT) for the connection by keeping track of the lowest observed RTT in the recent past. This value represents the round-trip propagation time (RTprop) of the connection.

102. The F5 '273 Products perform timestamping. Specifically, when a F5 '273 Product transmits a data packet, it records the current time as a timestamp. The timestamp is stored in the transmission control block (TCB), which maintains the state of the TCP connection, including RTT measurements and other relevant information.

103. The F5 '273 Products perform acknowledgment processing. Specifically, the F5 '273 Products send an acknowledgment (ACK) for a specific packet, the sender processes the ACK and identifies the corresponding packet in the TCB. By matching the ACK with the original packet, the F5 '273 Products retrieve the original timestamp associated with that packet.

104. The F5 '273 Products perform a round-trip time (RTT) calculation. Specifically, the F5 '273 Products calculate the RTT for a specific packet by subtracting the original timestamp from the current time when the ACK is received. This gives an individual RTT sample for that packet as explained in the below excerpt.



One way to stay near (max BW, min RTT) point:

Model network, update windowed max BW and min RTT estimates on each ACK

Control sending based on the model, to...

Probe both max BW and min RTT, to feed the model samples

Pace near estimated BW, to reduce queues and loss [move queue to sender]

Vary pacing rate to keep inflight near BDP (for full pipe but small queue)

That's **BBR** congestion control:

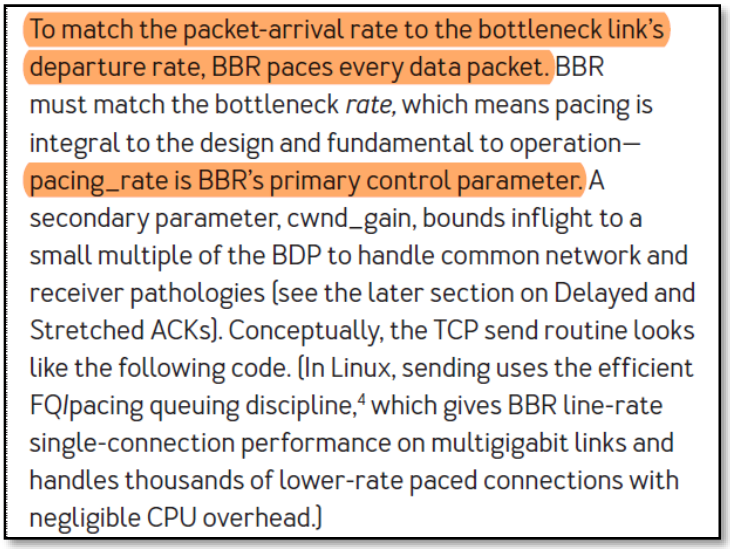
BBR = **B**ottleneck **B**andwidth and **R**ound-trip propagation time

BBR seeks high tput with small queue by probing BW and RTT *sequentially*

Neal Cardwell, Yunchung Cheng, et al, *BBR Congestion Control*, GOOGLE IETF 97: SEOUL PRESENTATION at 9 (November 2016) (emphasis added) (describing RTT_sample = ACK_receive_time - original_timestamp).

105. The F5 ‘273 Products perform the step of MinRTT estimation. Specifically, the F5 ‘273 Products maintain a running estimate of the minimum RTT observed (MinRTT) over a specified time window. The MinRTT is used by the F5 ‘273 Products to estimate the base round-trip propagation time without queuing delay. When a new RTT sample is calculated, the F5 ‘273 Products compare it with the current MinRTT value. If the new sample is lower than the existing MinRTT, the F5 ‘273 Products update MinRTT with a new value.

106. The F5 ‘273 Products perform round-trip time-based pacing. Specifically, the F5 products use the MinRTT estimate in performing pacing rate and congestion window calculations to ensure the sending rate is adapted based on the observed network conditions. BBR’s pacing rate and congestion window calculations factor in the MinRTT value to maintain a balance between efficient data transfer and minimal congestion.



To match the packet-arrival rate to the bottleneck link's departure rate, BBR paces every data packet. BBR must match the bottleneck *rate,* which means pacing is integral to the design and fundamental to operation—pacing_rate is BBR's primary control parameter. A secondary parameter, cwnd_gain, bounds inflight to a small multiple of the BDP to handle common network and receiver pathologies (see the later section on Delayed and Stretched ACKs). Conceptually, the TCP send routine looks like the following code. (In Linux, sending uses the efficient FQ/pacing queuing discipline,[4] which gives BBR line-rate single-connection performance on multigigabit links and handles thousands of lower-rate paced connections with negligible CPU overhead.)

Neal Cardwell, Yuchung Cheng, C. Stephen Gunn, Soheil Hassas Yeganeh, Van Jacobson, *BBR: Congestion-Based Congestion Control*, ACM Queue, Sep/Oct 2016 and CACM, Feb 2017 (emphasis added).

107. The F5 '273 Products calculate a congestion window parameter, which defines the maximum quantity of unacknowledged data packets permitted to be transmitted to the recipient.

108. The F5 '273 Products calculate a pacing rate based on these estimates to determine how quickly it should transmit data.

109. The F5 '273 Products calculate a congestion window. Specifically, the F5 '273 Products calculate a cwnd value based on the estimated bottleneck bandwidth (BtlBw) and RTT to ensure the congestion window is large enough not to limit the sending rate derived from the BtlBw and RTT estimates. This is done by setting the cwnd to the product of the estimated BtlBw and RTT: cwnd = BtlBw * RTT. The calculation done by the F5 '273 Products ensures that the cwnd value is large enough to accommodate the in-flight data based on the BtlBw and RTT estimates, while also accounting for potential variations in network conditions.

110. The F5 '273 Products calculate a congestion window (cwnd) based on the bottleneck bandwidth (BtlBw) and round-trip time (RTT) estimates to ensure the sending rate is

not constrained by the window size. The cwnd effectively sets a limit on the number of unacknowledged data packets in transit, but it is not set by a specific parameter for the maximum number of unacknowledged packets.

111. The F5 '273 Products transmit additional data packets to the receiver in response to a transmit timer expiration. The period of the transmit timer is based on the round-trip time measurements and the congestion window parameter.

112. F5 has directly infringed and continues to directly infringe the '273 patent by, among other things, making, using, offering for sale, and/or selling technology for transferring data from a sender to a receiver in a communication network, including but not limited to the F5 '273 Products.

113. The F5 '273 Products are available to businesses and individuals throughout the United States.

114. The F5 '273 Products are provided to businesses and individuals located in the Eastern District of Texas.

115. By making, using, testing, offering for sale, and/or selling products and services for transferring data from a sender to a receiver in a communication network, including but not limited to the F5 '273 Products, F5 has injured Plaintiff and is liable to Plaintiff for directly infringing one or more claims of the '273 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

116. F5 also indirectly infringes the '273 patent by actively inducing infringement under 35 U.S.C. § 271(b).

117. F5 has had knowledge of the '273 patent since at least service of this Complaint or shortly thereafter, and F5 knew of the '273 patent and knew of its infringement, including by way of this lawsuit.

118. F5 intended to induce patent infringement by third-party customers and users of the F5 '273 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. F5 specifically intended and was aware that the normal and customary use of the accused products would infringe the '273 patent. F5 performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '273 patent and with the knowledge that the induced acts would constitute infringement. For example, F5 provides the F5 '273 Products that have the capability of operating in a manner that infringe one or more of the claims of the '273 patent, including at least claim 1, and F5 further provides documentation and training materials that cause customers and end users of the F5 '273 Products to utilize the products in a manner that directly infringe one or more claims of the '273 patent.[15] By providing instruction and training to customers and end-users on how to use the F5 '273 Products in a manner that directly infringes

[15] *See e.g.,* F5 CLOUD-NATIVE NETWORK FUNCTIONS V1.1.0 – INSTALLATION AND INTEGRATION GUIDE (2023); F5 CLOUD-NATIVE NETWORK FUNCTIONS V1.1.1 – INSTALLATION AND INTEGRATION GUIDE (2024); *BIG-IP System: Congest Control Algorithms for TCP Profiles*, F5 TECHDOCS (May 31, 2022), available at: https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-tcp-congestion-control-14-1-0/tcp-congestion-control-algorithms.html; *F5 Cloud Docs: TCP: Congestion*, F5 CLOUDDOCS API – IRULES (last visited February 2024), available at: https://clouddocs.f5.com/api/irules/TCP__congestion.html; *K29377715: Overview of the TCP profile (14.x),* MYF5 KNOWLEDGE BASE ARTICLE (September 1, 2023), available at: https://my.f5.com/manage/s/article/K29377715; *K50411377: Overview of the TCP profile (16.x and later),* MYF5 KNOWLEDGE BASE ARTICLE (September 1, 2023), available at: https://my.f5.com/manage/s/article/K50411377; *K74767112: Overview of the TCP profile (15.x),* MYF5 KNOWLEDGE BASE ARTICLE (September 1, 2023), available at: https://my.f5.com/manage/s/article/K74767112; *F5 BIG-IP AS3 3.49.0 Non-HTTP Services*, F5 CLOUDDOCS (last visited February 2024), available at: https://clouddocs.f5.com/products/extensions/f5-appsvcs-extension/latest/declarations/non-http-services.html; *F5 Release Notes : BIG-IP 14.1.0 New and Installation,* F5 TECHDOCS (April 28, 2022), available at: https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/releasenotes/product/relnote-bigip-14-1-0.html; and *F5Networks - f5-appsvcs-extension/example-bbr-congestion-control.json*, F5 NETWORKS GITHUB REPOSITORY (November 15, 2022), available at: https://github.com/F5Networks/f5-appsvcs-extension/blob/383763104b78e218505907f52f63b06ad74057.

one or more claims of the ‘273 patent, including at least claim 1, F5 specifically intended to induce infringement of the ‘273 patent. F5 engaged in such inducement to promote the sales of the F5 ‘273 Products, e.g., through F5 user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘273 patent. Accordingly, F5 has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘273 patent, knowing that such use constitutes infringement of the ‘273 patent.

119. The ‘273 patent is well-known within the industry as demonstrated by multiple citations to the ‘273 patent in published patents and patent applications assigned to technology companies and academic institutions. F5 is utilizing the technology claimed in the ‘273 patent without paying a reasonable royalty. F5 is infringing the ‘273 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

120. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘273 patent.

121. As a result of F5’s infringement of the ‘273 patent, Plaintiff has suffered monetary damages, and seeks recovery in an amount adequate to compensate for F5’s infringement, but in no event less than a reasonable royalty for the use made of the invention by F5 together with interest and costs as fixed by the Court.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 7,136,353

122. Plaintiff references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

123. F5 designs, makes, uses, sells, and/or offers for sale in the United States products comprising technology for managing multiple connections for sending data packets between a sender and a receiver in a computer network.

124. F5 designs, makes, sells, offers to sell, imports, and/or uses hardware, software, solutions, appliances, modules, services, technologies, platforms that include, incorporate, are designed to work with, can include, or are capable of integrating BIG-IP Local Traffic Manager (LTM) technology, specifically versions 13.0.x and later (collectively, the "F5 '353 Product(s)").

125. One or more F5 subsidiaries and/or affiliates use the F5 '353 Products in regular business operations.

126. The F5 '353 Products contain various load balancing algorithms (*e.g.*, Round Robin, Least Connections, Fastest Response, etc.) that can be configured to consider the current load or performance metrics of servers. Further, the F5 '353 Products contain rate limiting and bandwidth controllers that can dynamically adjust to the observed traffic rates,

127. The F5 '353 Products determine a host-level transmission rate between the sender and receiver by summing a current transmission rate associated with each of a plurality of connections.

128. The F5 '353 Products identify a present transmission rate for individual connections between a host and client device.

129. The F5 '353 Products perform Priority Group Activation and Rate Shaping that prioritizes traffic and manages bandwidth allocation. The F5 '353 Products allow for the preferential treatment of certain types of traffic.

130. The F5 ‘353 Products conduct automated bandwidth discovery in which a bandwidth test is performed by sending a short burst of bidirectional traffic and measuring the received rate at each end.

131. The F5 ‘353 Products compute a host-level transmission rate by totaling the current transmission rates over several connections.

132. The F5 ‘353 Products perform bandwidth aggregation across connections that utilizes all available links to deliver packets across different connections.

133. The F5 ‘353 Products allocate the host-level transmission rate across multiple connections based on a ratio of a weight related to each connection and the total of the weights for set of multiple connections.

134. The F5 ‘353 Products choose data packets for transmission in a way that each chosen data packet is linked with the connection exhibiting the greatest discrepancy between the allocated transmission rate and the actual transmission rate for the connection.

135. The F5 ‘353 Products perform packet scheduling including through the use of a guaranteed minimum aggregate bandwidth during congestion based on scheduler weight (or percentage of bandwidth.

136. The F5 ‘353 Products allocate the host-level transmission rate among the plurality of connections based on a ratio of a weight associated with each connection and a sum of the weights for the plurality of connections.

137. The F5 ‘353 Products transmit data packets from the host across the related connections based on data packets associated with connections having a highest difference between the allocated transmission rate and an actual transmission rate are transmitted first. Further, each data packet being transmitted from the sender is transmitted in response to each

expiration of a transmission timer having a period corresponding to the host-level transmission rate.

138. F5 has directly infringed and continues to directly infringe the ‘353 patent by, among other things, making, using, offering for sale, and/or selling technology for managing multiple connections for sending data packets between a sender and a receiver in a computer network, including but not limited to the F5 ‘353 Products.

139. The F5 ‘353 Products are available to businesses and individuals throughout the United States.

140. The F5 ‘353 Products are provided to businesses and individuals located in this District.

141. By making, using, testing, offering for sale, and/or selling products and services comprising technology for managing multiple connections for sending data packets between a sender and a receiver in a computer network, including but not limited to the F5 ‘353 Products, F5 has injured Plaintiff and is liable to Plaintiff for directly infringing one or more claims of the ‘353 patent, including at least claim 13 pursuant to 35 U.S.C. § 271(a).

142. F5 also indirectly infringes the ‘353 patent by actively inducing infringement under 35 U.S.C. § 271(b).

143. F5 has had knowledge of the ‘353 patent since at least service of this Complaint or shortly thereafter, and F5 knew of the ‘353 patent and knew of its infringement, including by way of this lawsuit.

144. F5 intended to induce patent infringement by third-party customers and users of the F5 ‘353 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. F5 specifically

intended and was aware that the normal and customary use of the accused products would infringe the '353 patent. F5 performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '353 patent and with the knowledge that the induced acts would constitute infringement. For example, F5 provides the F5 '353 Products that have the capability of operating in a manner that infringe one or more of the claims of the '353 patent, including at least claim 13, and F5 further provides documentation and training materials that cause customers and end users of the F5 '353 Products to utilize the products in a manner that directly infringe one or more claims of the '353 patent.[16] By providing instruction and training to customers and end-users on how to use the F5 '353 Products in a manner that directly infringes one or more claims of the '353 patent, including at least claim 13, F5 specifically intended to induce infringement of the '353 patent. F5 engaged in such inducement to promote the sales of the F5 '353 Products, e.g., through F5 user manuals, product support, marketing materials, and

[16] *See e.g.,* F5 BIG-IP LOCAL TRAFFIC MANAGEMENT: BASICS VERSION 13.0 (January 18, 2019); F5 BIG-IP LOCAL TRAFFIC MANAGER: CONCEPTS VERSION 11.5.1 (February 13, 2017); F5 BIG-IP LOCAL TRAFFIC MANAGER: IMPLEMENTATIONS VERSION 13.0 (March 4, 2019); *Using Selective Compression,* F5 DEVCENTRAL YOUTUBE CHANNEL (June 7. 2016), available at: https://www.youtube.com/watch?v=d85swKvXS1w; *Setup, Configuration and Backup of F5OS - rSeries: F5's Next Generation Appliance,* F5 DEVCENTRAL YOUTUBE CHANNEL (June 4, 2023), available at: https://www.youtube.com/watch?v=CiXkvkBWt6M; *Basic iRule Anatomy,* F5 DEVCENTRAL YOUTUBE CHANNEL (December 16, 2015), available at: https://www.youtube.com/watch?v=OhXS-Yt_gWc; *BIG-IP Basic Nomenclature,* F5 DEVCENTRAL YOUTUBE CHANNEL (April 12, 2017), available at: https://www.youtube.com/watch?v=2YRKTyMgV4M; *Introduction to rSeries: F5's Next Generation Appliance,* F5 DEVCENTRAL YOUTUBE CHANNEL (January 4, 2023), available at: https://www.youtube.com/watch?v=rCc5D6MEMcI; F5 BIG-IP LOCAL TRAFFIC MANAGER: DATA SHEET (2022); F5 STUDY GUIDE: 301B – BIG-IP LTM TECHNOLOGY SPECIALIST: MAINTAIN AND TROUBLESHOOT (2015); F5 BIG-IP LOCAL TRAFFIC MANAGER: DATA SHEET (2023); *F5 BIG-IP Local Traffic Policies*, F5 DEVCENTRAL YOUTUBE CHANNEL (August 12, 2025), available at: https://www.youtube.com/watch?v=-iLzxfKbl5A; *What is BIG-IP,* F5 DEVCENTRAL YOUTUBE CHANNEL (May 10, 2017), available at: https://www.youtube.com/watch?v=D6J_j7HdkV8; *BIG-IP Life of a Packet*, F5 DEVCENTRAL YOUTUBE CHANNEL (February 1, 2017), available at: https://www.youtube.com/watch?v=qCLEw5xIZ7s; *BIG-IP in the Public Cloud,* F5 DEVCENTRAL YOUTUBE CHANNEL (June 14, 2017), available at: https://www.youtube.com/watch?v=DMXpY9lx804; *LTM Load Balancing Algorithms: Round Robin, Ratio, & Dynamic Ratio*, F5 DEVCENTRAL YOUTUBE CHANNEL (June 8, 2019); https://www.youtube.com/watch?v=Gg-6yS12-7Q; and *BIG-IP LTM & DNS Load Balancer Integration*, F5 DEVCENTRAL YOUTUBE CHANNEL (Jone 4, 2020).

training materials to actively induce the users of the accused products to infringe the ‘353 patent. Accordingly, F5 has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘353 patent, knowing that such use constitutes infringement of the ‘353 patent.

145. The ‘353 patent is well-known within the industry as demonstrated by multiple citations to the ‘353 patent in published patents and patent applications assigned to technology companies and academic institutions. F5 is utilizing the technology claimed in the ‘353 patent without paying a reasonable royalty. F5 is infringing the ‘353 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

146. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘353 patent.

147. As a result of F5’s infringement of the ‘353 patent, Plaintiff has suffered monetary damages, and seek recovery in an amount adequate to compensate for F5’s infringement, but in no event less than a reasonable royalty for the use made of the invention by F5 together with interest and costs as fixed by the Court.

COUNT III
INFRINGEMENT OF U.S. PATENT NO. 7,586,871

148. Plaintiff references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

149. F5 designs, makes, uses, sells, and/or offers for sale in the United States products that process data communications passing through a node between a first data network and a second data network.

150. F5 designs, makes, sells, offers to sell, imports, and/or uses the hardware, software, solutions, appliances, modules, services, technologies, platforms that include, incorporate, are designed to work with, can include, or are capable of integrating F5's BIG-IP Advanced Web Application Firewall (Advanced WAF) technology (collectively, the "F5 '871 Product(s)").

151. One or more F5 subsidiaries and/or affiliates use the F5 '871 Products in regular business operations.

152. The F5 '871 Products detect an event associated with a data communication arriving at the node from a first data network.

153. The F5 '871 Products perform various detection mechanisms, including signature-based detection, anomaly detection, and behavioral analysis, to identify threats such as SQL injection, cross-site scripting (XSS), and other web application attacks.

154. The F5 '871 Products monitor incoming data packets at the node from a first data network.

155. The F5 '871 Products determine whether the data communication is to be suspended for service at the node based on the detected event. Specifically, once an event associated with the data communication is detected by the F5 '871 Products, the system evaluates the nature and severity of the event. The decision to suspend or allow the communication is based on rules and policies configured by the F5 '871 Products.

156. The F5 '871 Products upon detecting suspicious or anomalous activity perform the step of applying predefined security policies and profiles. This includes the ability to block, challenge, or rate-limit traffic deemed malicious or anomalous.

157. The F5 '871 Products determine (based on a detected event) whether the data communication should be suspended at the node.

158. The F5 ‘871 Products process one or more suspended data communications using information in the suspended data communication. Specifically, the F5 ‘871 Products isolate the suspended data communication for (at least in part) the purpose of processing the suspended data communication. Based on the analysis and processing, the F5 ‘871 Products determine how to handle the suspended data communication.

159. The F5 ‘871 Products detect a return data communication arriving at the node from the second data network in response to the processed data communication from the first data network. Further, the F5 ‘871 Products allow the detected return data communication to pass through the node without processing.

160. The F5 ‘871 Products monitor the incoming data communication from the second data network. If the detected return data communication is associated with prior processed data communication from the first network the F5 ‘871 Products determine that the return data communication does not need further processing at the node.

161. The F5 ‘871 Products process a suspended data communication based on information in the data communication.

162. F5 has directly infringed and continues to directly infringe the ‘871 patent by, among other things, making, using, offering for sale, and/or selling technology that process data communications passing through a node between a first data network and a second data network, including but not limited to the F5 ‘871 Products.

163. The F5 ‘871 Products are available to businesses and individuals throughout the United States.

164. The F5 ‘871 Products are provided to businesses and individuals located in this District.

165. By making, using, testing, offering for sale, and/or selling products and services that process data communications passing through a node between a first data network and a second data network, including but not limited to the F5 '871 Products, F5 has injured Plaintiff and is liable to Plaintiff for directly infringing one or more claims of the '871 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

166. F5 also indirectly infringes the '871 patent by actively inducing infringement under 35 U.S.C. § 271(b).

167. F5 has had knowledge of the '871 patent since at least service of this Complaint or shortly thereafter, and F5 knew of the '871 patent and knew of its infringement, including by way of this lawsuit.

168. F5 intended to induce patent infringement by third-party customers and users of the F5 '871 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. F5 specifically intended and was aware that the normal and customary use of the accused products would infringe the '871 patent. F5 performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '871 patent and with the knowledge that the induced acts would constitute infringement. For example, F5 provides the F5 '871 Products that have the capability of operating in a manner that infringe one or more of the claims of the '871 patent, including at least claim 1, and F5 further provides documentation and training materials that cause customers and end users of the F5 '871 Products to utilize the products in a manner that directly infringe one or more claims of the '871 patent.[17] By providing instruction and training to

[17] *See e.g., WAF 101 - BIG-IP Security: Mitigating App Vulnerabilities with AWAF,* F5 WEB APPLICATION FIREWALL SOLUTIONS DOCUMENTATION (last visited February 2024), available at: https://clouddocs.f5.com/training/community/waf/html/waf2023/waf2023.html; *Lab 1.1:*

customers and end-users on how to use the F5 ‘871 Products in a manner that directly infringes one or more claims of the ‘871 patent, including at least claim 1, F5 specifically intended to induce infringement of the ‘871 patent. F5 engaged in such inducement to promote the sales of the F5 ‘871 Products, e.g., through F5 user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘871 patent. Accordingly, F5 has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘871 patent, knowing that such use constitutes infringement of the ‘871 patent.

169. The ‘871 patent is well-known within the industry as demonstrated by multiple citations to the ‘871 patent in published patents and patent applications assigned to technology companies and academic institutions. F5 is utilizing the technology claimed in the ‘871 patent without paying a reasonable royalty. F5 is infringing the ‘871 patent in a manner best described

Creation of an AWAF Base Policy, F5 WEB APPLICATION FIREWALL SOLUTIONS DOCUMENTATION (last visited February 2024), available at: https://clouddocs.f5.com/training/community/waf/html/waf301/module1/lab1.html; *Configuring Advanced WAF Polices,* F5 BIG-IP NEXT v20.0.2 DOCUMENTATION (last visited February 2024), available at: https://clouddocs.f5.com/bigip-next/20-0-2/waf_management/orphans/awaf_how_to_create_policy_OLD.html; F5 ADVANCED WAF OVERVIEW DC0318 | OV-SEC 253143946 (2018); *Protection for Every App Anywhere - DC0822 | OV-815153139*, F5 SOLUTIONS OVERVIEW (2022); WHITE PAPER - ADVANCED APPLICATION THREATS REQUIRE AN ADVANCED WAF - DC0418 | WP-SEC-222132511 (2018); F5 ADVANCED WAF DATASHEET - DS-BIGIP-268260962 (2018); F5 DISTRIBUTED CLOUD WEB APPLICATION FIREWALL (WAF) - DC0123 | OV-XPILLAR-1030894587 (2023); F5 ADC SYSTEM DATASHEET - DC 09.2023 | DS-GTM-1173795077 (2023); CHOOSING THE WAF THAT’S RIGHT FOR YOU - A HOW-TO GUIDE - EBOOK-SEC-798087620 (2022); *Creating a BIG-IP Advanced WAF Policy*, F5 DEVCENTRAL YOUTUBE CHANNEL (September 21, 2022), available at: https://www.youtube.com/watch?v=8iXwrtXWiRQ; *Coding Live: F5 BIG-IP Packet Captures,* F5 DEVCENTRAL YOUTUBE CHANNEL (February 9, 2023), available at: https://www.youtube.com/watch?v=eexz9hnzNU0; and *Introducing The F5 Advanced WAF*, F5 DEVCENTRAL YOUTUBE CHANNEL (April 30, 2018), available at: https://www.youtube.com/watch?v=HBbDKBV4QW0.

as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

170. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘871 patent.

171. As a result of F5’s infringement of the ‘871 patent, Plaintiff has suffered monetary damages, and seeks recovery in an amount adequate to compensate for F5’s infringement, but in no event less than a reasonable royalty for the use made of the invention by F5 together with interest and costs as fixed by the Court.

COUNT IV
INFRINGEMENT OF U.S. PATENT NO. 7,616,559

172. Plaintiff references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

173. F5 designs, makes, uses, sells, and/or offers for sale in the United States products that communicate information over multiple communications links.

174. F5 designs, makes, sells, offers to sell, imports, and/or uses hardware, software, solutions, appliances, modules, services, technologies, platforms that include, incorporate, are designed to work with, can include, or are capable of integrating BIG-IP Local Traffic Manager (LTM) technology, specifically versions 13.0.x and later (collectively, the “’559 F5 Product(s)”).

175. One or more F5 subsidiaries and/or affiliates use the F5 ‘559 Products in regular business operations.

176. The F5 ‘559 Products identify an initial communication path with a specific security protocol for the transmission of data between a client system and a server system.

177. The F5 ‘559 Products perform managing multiple traffic routes or connections with varying security postures such as SSL/TLS profiles or a secure VLAN setup.

178. The F5 ‘559 Products detect a first communications link having a first security feature for communicating data between a client device and a server device. The F5 ‘559 Products utilize algorithms to ensure the first security level’s parameters, such as encryption and authentication protocols are met. By identifying the presence of this first communications link, the F5 ‘559 Products can prioritize a communications link for use based on predefined security requirements or other criteria.

179. The F5 ‘559 Products contain functionality for identifying an alternate communication pathway that possesses a different level of security for exchanging data between a client and a server.

180. The F5 ‘559 Products perform the step of detecting an alternative traffic route or connection that has a different level of security, such as a different SSL/TLS profile or another secure network configuration.

181. The F5 ‘559 Products detect a second communications link having a second security feature. The second communications link enables data to be sent between a client and server. Further, the F5 ‘559 Products monitor network channels and enable security protocols to evaluate the parameters of the second communications link. The security features used by the F5 ‘559 Products include encryption standards and/or authentication technology. The second communications link serves to ensure continuous data transfer by the F5 ‘559 Products if the first communications link is unavailable.

182. The F5 ‘559 Products perform intelligent traffic management, where the F5 ‘559 Products can preferentially route traffic over a preferred (first) communications link based on its availability and security settings.

183. The F5 ‘559 Products determine if the initial communication path is inaccessible, opting for the alternate communication pathway with its distinct security level, to facilitate data transmission between a client and server.

184. The F5 ‘559 Products select the first communications link, having first security, for communicating between a client device and a server. After the detection of both the first and second communications links, the F5 ‘559 Products prioritize the link with the higher security features (e.g., first link) for data transmission. This prioritization by the F5 ‘559 Products is based on pre-established security criteria and network conditions. If the first link meets the requirements, it is selected by the F5 ‘559 Products to provide enhanced security and reliability.

185. The F5 ‘559 Products contain redundancy features that ensure continuous availability by automatically rerouting traffic to an alternative (second) communications link if the primary (first) link is unavailable.

186. The F5 ‘559 Products maintain a connection with one of either the initial or alternate communication pathways, to ensure uninterrupted data exchange between the client system and the server system.

187. The F5 ‘559 Products perform dynamic load balancing and traffic management, which routes traffic through the available and optimal path to maintain continuous connectivity between the client and server devices.

188. The F5 ‘559 Products conduct health monitoring, where the F5 ‘559 Products can detect issues with the currently active (second) communications link and automatically revert to the primary (first) link once it becomes available and is deemed optimal for traffic.

189. If the first communications link is not available, the F5 ‘559 Products select the second communications link having second security, for communicating between the client device

and the server device. This action is prompted when the preferred first link, typically with higher security, is unavailable or fails to meet a criterion. The F5 '559 Products switch to the second link, ensuring continuous communication. While generally considered less secure, the second link serves as a contingency, allowing uninterrupted information flow between a client and server.

190. If the data transmission is interrupted over the alternate communication pathway, the F5 '559 Products contain functionality for restoring the connection to the initial communication link to continue exchanging information between the client and the server.

191. The F5 '559 Products enable linking to one of either the first communications link and the second communications link, to maintain communicative connectivity during communications between the client and server. The F5 '559 Products establish a dynamic link management process, maintaining an active connection by continuously evaluating both communication links.

192. The F5 '559 Products contain functionality where if communication disruption occurs over the primary communication link, the alternate communication link is reestablished to facilitate the exchange of information between the client and server.

193. The F5 '559 Products enable reconnecting to the first communications link for communicating information between the client and server if communications are hindered over the second communications link. This step is a part of a resilient communication strategy that actively monitors both links and switches back to the first link when issues are detected with the second communications link.

194. The F5 '559 Products enable reconnecting to the second communications link for communicating information between the client device and the server device, if communications are hindered over the first communications link. If issues are detected on the primary link, the F5

‘559 Products automatically switch to the secondary link, maintaining the communication while also adhering to the security protocols.

195. F5 has directly infringed and continues to directly infringe the ‘559 patent by, among other things, making, using, offering for sale, and/or selling technology comprising a method of communicating information over multiple communications links, including but not limited to the F5 ‘559 Products.

196. The F5 ‘559 Products are available to businesses and individuals throughout the United States.

197. The F5 ‘559 Products are provided to businesses and individuals located in this District.

198. By making, using, testing, offering for sale, and/or selling products and services comprising a method of communicating information over multiple communications links, including but not limited to the F5 ‘559 Products, F5 has injured Plaintiff and is liable to Plaintiff for directly infringing one or more claims of the ‘559 patent, including at least claim 5 pursuant to 35 U.S.C. § 271(a).

199. F5 also indirectly infringes the ‘559 patent by actively inducing infringement under 35 U.S.C. § 271(b).

200. F5 has had knowledge of the ‘559 patent since at least service of this Complaint or shortly thereafter, and F5 knew of the ‘559 patent and knew of its infringement, including by way of this lawsuit.

201. F5 intended to induce patent infringement by third-party customers and users of the F5 ‘559 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. F5 specifically

intended and was aware that the normal and customary use of the accused products would infringe the ‘559 patent. F5 performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘559 patent and with the knowledge that the induced acts would constitute infringement. For example, F5 provides the F5 ‘559 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘559 patent, including at least claim 5, and F5 further provides documentation and training materials that cause customers and end users of the F5 ‘559 Products to utilize the products in a manner that directly infringe one or more claims of the ‘559 patent.[18] By providing instruction and training to customers and end-users on how to use the F5 ‘559 Products in a manner that directly infringes one or more claims of the ‘559 patent, including at least claim 5, F5 specifically intended to induce

[18] *See e.g.,* F5 BIG-IP LOCAL TRAFFIC MANAGEMENT: BASICS VERSION 13.0 (January 18, 2019); F5 BIG-IP LOCAL TRAFFIC MANAGER: CONCEPTS VERSION 11.5.1 (February 13, 2017); F5 BIG-IP LOCAL TRAFFIC MANAGER: IMPLEMENTATIONS VERSION 13.0 (March 4, 2019); *Using Selective Compression,* F5 DEVCENTRAL YOUTUBE CHANNEL (June 7. 2016), available at: https://www.youtube.com/watch?v=d85swKvXS1w; *Setup, Configuration and Backup of F5OS - rSeries: F5's Next Generation Appliance,* F5 DEVCENTRAL YOUTUBE CHANNEL (June 4, 2023), available at: https://www.youtube.com/watch?v=CiXkvkBWt6M; *Basic iRule Anatomy,* F5 DEVCENTRAL YOUTUBE CHANNEL (December 16, 2015), available at: https://www.youtube.com/watch?v=OhXS-Yt_gWc; *BIG-IP Basic Nomenclature,* F5 DEVCENTRAL YOUTUBE CHANNEL (April 12, 2017), available at: https://www.youtube.com/watch?v=2YRKTyMgV4M; *Introduction to rSeries: F5's Next Generation Appliance,* F5 DEVCENTRAL YOUTUBE CHANNEL (January 4, 2023), available at: https://www.youtube.com/watch?v=rCc5D6MEMcI; F5 BIG-IP LOCAL TRAFFIC MANAGER: DATA SHEET (2022); F5 STUDY GUIDE: 301B – BIG-IP LTM TECHNOLOGY SPECIALIST: MAINTAIN AND TROUBLESHOOT (2015); F5 BIG-IP LOCAL TRAFFIC MANAGER: DATA SHEET (2023); *F5 BIG-IP Local Traffic Policies*, F5 DEVCENTRAL YOUTUBE CHANNEL (August 12, 2025), available at: https://www.youtube.com/watch?v=-iLzxfKbl5A; *What is BIG-IP,* F5 DEVCENTRAL YOUTUBE CHANNEL (May 10, 2017), available at: https://www.youtube.com/watch?v=D6J_j7HdkV8; *BIG-IP Life of a Packet*, F5 DEVCENTRAL YOUTUBE CHANNEL (February 1, 2017), available at: https://www.youtube.com/watch?v=qCLEw5xIZ7s; *BIG-IP in the Public Cloud,* F5 DEVCENTRAL YOUTUBE CHANNEL (June 14, 2017), available at: https://www.youtube.com/watch?v=DMXpY9lx804; *LTM Load Balancing Algorithms: Round Robin, Ratio, & Dynamic Ratio*, F5 DEVCENTRAL YOUTUBE CHANNEL (June 8, 2019); https://www.youtube.com/watch?v=Gg-6yS12-7Q; and *BIG-IP LTM & DNS Load Balancer Integration*, F5 DEVCENTRAL YOUTUBE CHANNEL (Jone 4, 2020).

infringement of the ‘559 patent. F5 engaged in such inducement to promote the sales of the F5 ‘559 Products, e.g., through F5 user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘559 patent. Accordingly, F5 has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘559 patent, knowing that such use constitutes infringement of the ‘559 patent.

202. The ‘559 patent is well-known within the industry as demonstrated by multiple citations to the ‘559 patent in published patents and patent applications assigned to technology companies and academic institutions. F5 is utilizing the technology claimed in the ‘559 patent without paying a reasonable royalty. F5 is infringing the ‘559 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

203. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘559 patent.

204. As a result of F5’s infringement of the ‘559 patent, Plaintiff has suffered monetary damages, and seeks recovery in an amount adequate to compensate for F5’s infringement, but in no event less than a reasonable royalty for the use made of the invention by F5 together with interest and costs as fixed by the Court.

COUNT V
INFRINGEMENT OF U.S. PATENT NO. 8,429,169

205. Plaintiff references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

206. F5 designs, makes, uses, sells, and/or offers for sale in the United States products comprising technology for video cache indexing.

207. F5 designs, makes, sells, offers to sell, imports, and/or uses hardware, software, solutions, appliances, modules, services, technologies, platforms that include, incorporate, are designed to work with, can include, or are capable of integrating F5 NGINX Plus Release 11 and later (collectively, the "F5 '169 Product(s)").

208. One or more F5 subsidiaries and/or affiliates use the F5 '169 Products in regular business operations.

209. The F5 '169 Products receive a content request from a user's device. The F5 '169 Products are configured to listen on specific network ports (usually port 80 for HTTP and port 443 for HTTPS) for incoming connections. This capability is configured in the server block of the NGINX configuration file (nginx.conf).

210. The F5 '169 Products parse the HTTP headers and payload. The F5 '169 Products examine the request URI, method (GET, POST, etc.), and headers to determine how the request should be routed or processed according to the configuration rules defined in nginx.conf.

211. The F5 '169 Products perform SSL/TLS termination, decrypting incoming requests to process them internally. This functionality is enabled in the F5 '169 Products through Application-Layer Protocol Negotiation (ALPN).

212. The F5 '169 Products request a portion of content from a web server based on a user's content request. After receiving a client request, the F5 '169 Products resolve where to send the request based on the configuration F5 '169 Products. This involves parsing the request URI, headers, and method to match server blocks and location directives defined in nginx.conf. The F5 '169 Products then forward the request to the appropriate backend server(s) based on this configuration.

213. The F5 ‘169 Products enable “Vary” headers for Cached Content. Specifically, "characterization data" includes any request header or combination of headers that the Vary header specifies. For instance, if the backend server's response includes Vary: Accept-Encoding, User-Agent, the characterization data the F5 ‘169 Products identifies would be the values of the Accept-Encoding and User-Agent headers in the incoming request.

214. The F5 ‘169 Products use the identified characterization data (e.g., `Accept-Encoding` and `User-Agent` header values) as part of the cache key. The F5 ‘169 Products input this characterization data into a hash function to generate a unique index (cache key) for storing and retrieving the cached content.

215. The F5 ‘169 Products contain a Health Check Module the enables the F5 ‘169 Products to communicate with backend servers. This module supports balancing across multiple backend servers, selecting a server based on its health.

216. The F5 ‘169 Products query a web server for a specific segment of content related to the user’s content request. Once the F5 ‘169 Products have received and parsed the request, the F5 ‘169 Products determine how to handle the request based on its configuration rules. If the requested content is not available in the F5 ‘169 Products’ caches, the F5 ‘169 Products may act as a reverse proxy and forward the request to the appropriate origin server. The web server processes this request and returns the requested content back to the F5 ‘169 Products.

217. The F5 ‘169 Products identify one or more descriptors for the content corresponding to the user’s request, where these descriptors include the particular content segment associated with the initial request.

218. The F5 ‘169 Products compute an index related to the requested content by applying the identified descriptors to a hashing function, wherein this computed index aids in locating a corresponding entry in a cache data structure by matching against indices tied to existing entries.

219. When storing a response in the cache, the F5 ‘169 Products generate a key using a hash function. The key can be modified using the proxy_cache_key directive. This key is used to store and retrieve the cached content efficiently.

220. Once the F5 ‘169 Products have determined that it needs to retrieve content from a web server, the F5 ‘169 Products send a request to the server using the HTTP protocol. The request includes the request line, headers, and any data from the client’s request that needs to be passed to the server. The F5 ‘169 Products can be configured to use different algorithms to choose the web server that will receive the request.

221. The F5 ‘169 Products process the content to identify characterization data that can be used to cache the content. The characterization data is a compact representation of the content that allows the F5 ‘169 Products to quickly determine whether it has a cached copy of the content that is identical to the requested content. The F5 ‘169 Products can use various algorithms to generate characterization data, such as a checksum, a hash function, or a compression algorithm. For example, a checksum can be used for small pieces of data, while a hash function can be used for larger pieces of data. The characterization data is then stored in the F5 ‘169 Products cache, along with the content, so that it can be quickly retrieved when a subsequent request for the same content is received.

222. The F5 ‘169 Products generate an index corresponding to content associated with the received content request by inputting the at least one identified characterization data into a hash function, wherein the generated index is used for identifying, in the cache data structure, an

entry associated with the content by comparing the generated index to one or more index fields associated with one or more entries within the cache data structure.

223. F5 has directly infringed and continues to directly infringe the ‘169 patent by, among other things, making, using, offering for sale, and/or selling technology comprising video cache indexing, including but not limited to the F5 ‘169 Products.

224. The F5 ‘169 Products are available to businesses and individuals throughout the United States.

225. The F5 ‘169 Products are provided to businesses and individuals located in this District.

226. By making, using, testing, offering for sale, and/or selling products and services comprising technology for video cache indexing, including but not limited to the F5 ‘169 Products, F5 has injured Plaintiff and is liable to Plaintiff for directly infringing one or more claims of the ‘169 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

227. F5 also indirectly infringes the ‘169 patent by actively inducing infringement under 35 U.S.C. § 271(b).

228. F5 has had knowledge of the ‘169 patent since at least service of this Complaint or shortly thereafter, and F5 knew of the ‘169 patent and knew of its infringement, including by way of this lawsuit.

229. F5 intended to induce patent infringement by third-party customers and users of the F5 ‘169 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. F5 specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘169 patent. F5 performed the acts that constitute induced infringement, and would induce

actual infringement, with knowledge of the '169 patent and with the knowledge that the induced acts would constitute infringement. For example, F5 provides the F5 '169 Products that have the capability of operating in a manner that infringe one or more of the claims of the '169 patent, including at least claim 1, and F5 further provides documentation and training materials that cause customers and end users of the F5 '169 Products to utilize the products in a manner that directly infringe one or more claims of the '169 patent.19 By providing instruction and training to customers and end-users on how to use the F5 '169 Products in a manner that directly infringes one or more claims of the '169 patent, including at least claim 1, F5 specifically intended to induce infringement of the '169 patent. F5 engaged in such inducement to promote the sales of the F5 '169 Products, e.g., through F5 user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '169 patent. Accordingly, F5 has induced and continues to induce users of the accused products to use the

[19] *See e.g., Best Practices for Caching,* NGINX CONFERENCE PRESENTATION (2018); *NGINX Plus Reference Guide - Release 6,* F5 NGINX DOCUMENTATION (April 8, 2015); *NGINX Content Caching*, NGINX PLUS DOCUMENTATION (last visited February 2024), available at: https://docs.nginx.com/nginx/admin-guide/content-cache/content-caching/; *Using NGINX Plus for Advanced Video Streaming*, NGINX YOUTUBE CHANNEL (April 13, 2020), available at: https://www.youtube.com/watch?v=xbFBjvUT-k0; *Learn How to Stop Worrying and Build Your Own CDN,* NGINX BLOG (February 24, 2017), available at: https://www.nginx.com/blog/learn-to-stop-worrying-build-cdn/; *NGINX Plus Reference Guide - Release 16,* F5 NGINX DOCUMENTATION (April 28, 2018); *High-Performance Caching with NGINX and NGINX Plus*, NGINX Blog (August 24, 2016), available at: https://www.nginx.com/blog/nginx-high-performance-caching/; *Best Practices for Caching,* NGINX YOUTUBE CHANNEL (October 30, 2018), available at: https://www.youtube.com/watch?v=iNH6APQzIog; *NGINX Reverse Proxy,* NGINX PLUS DOCUMENTATION (last visited February 2024), available at: https://docs.nginx.com/nginx/admin-guide/web-server/reverse-proxy/; *Building a Powerful, Efficient and Highly Available Caching Layer with NGINX*, NGINX YOUTUBE CHANNEL (September 20, 2017), available at: https://www.youtube.com/watch?v=xZrOjmAkFC8; and *Smart and Efficient Byte-Range Caching with NGINX & NGINX Plus*, NGINX BLOG (January 21, 2016), available at: https://www.nginx.com/blog/smart-efficient-byte-range-caching-nginx/.

accused products in their ordinary and customary way to infringe the ‘169 patent, knowing that such use constitutes infringement of the ‘169 patent.

230. The ‘169 patent is well-known within the industry as demonstrated by multiple citations to the ‘169 patent in published patents and patent applications assigned to technology companies and academic institutions. F5 is utilizing the technology claimed in the ‘169 patent without paying a reasonable royalty. F5 is infringing the ‘169 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

231. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘169 patent.

232. As a result of F5’s infringement of the ‘169 patent, Plaintiff has suffered monetary damages, and seek recovery in an amount adequate to compensate for F5’s infringement, but in no event less than a reasonable royalty for the use made of the invention by F5 together with interest and costs as fixed by the Court.

COUNT VI
INFRINGEMENT OF U.S. PATENT NO. 8,521,901

233. Plaintiff references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

234. F5 designs, makes, uses, sells, and/or offers for sale in the United States products comprising technology for a data packet scheduler that reduces packet bursts.

235. F5 designs, makes, sells, offers to sell, imports, and/or uses hardware, software, solutions, appliances, modules, services, technologies, platforms that include, incorporate, are designed to work with, can include, or are capable of integrating BIG-IP Local Traffic Manager (LTM) technology, specifically versions 13.0.x and later (collectively, the “F5 ’901 Product(s)”).

236. One or more F5 subsidiaries and/or affiliates use the F5 ‘901 Products in regular business operations.

237. The F5 ‘901 Products receive a transmission control protocol (TCP) packet from a sending layer on the first device. The sending layer is one of the network interface layer or the transport layer and the TCP packet is sent over a connection between the first device and a second device.

238. The F5 ‘901 Products perform the functions of a full proxy for TCP traffic, sitting between the client (first device) and the server (second device). The F5 ‘901 Products terminate client-side connections and establish new server-side connections.

239. F5 ‘901 Products contain functionality for receiving and sending TCP packets and comprise functionality for optimizing the flow of data between devices over various network paths.

240. F5 ‘901 Products store information about the connection between a first device and the second device. The information stored by the F5 ‘901 products include a last packet delivery time for a specific connection/link. Specifically, the F5 ‘901 products store information about the network connection, such as metrics regarding packet delivery, latency, and jitter, to optimize the path selection and improve performance.

241. The F5 ‘901 Products maintain connection tables that track the state and characteristics of each TCP connection, including timestamps of last packet delivery. This stored information is used by the F5 ‘901 Products to apply various optimizations and ensure efficient handling of ongoing connections.

242. F5 ‘901 Products determine if a TCP packet is part of a bursty transmission on the connection by looking at whether a burst count for the connection is greater than a burst-count threshold.

243. The F5 ‘901 Products manage bursty traffic using rate shaping and priority queuing. By monitoring the flow and characteristics of traffic, including burst counts, the F5 ‘901 Products can determine if the incoming traffic exceeds thresholds indicative of bursty behavior.

244. F5 ‘901 Products calculate a delay time for a connection using the last packet delivery time after determining that the TCP packet is part of a bursty transmission. Specifically, the F5 ‘901 Products measure latency and jitter for each connection/link. This measurement is then used to determine the burstiness of a TCP packet transmission.

245. The F5 ‘901 Products can use bandwidth control and traffic policing to calculate an appropriate delay for the traffic, to smooth out bursts and prevent network congestion. The F5 ‘901 Products use the stored connection information and last packet delivery time, to dynamically adjust the handling of packets.

246. The F5 ‘901 Products contain functionality for delivering the TCP packet to a receiving layer based on the calculated delay time, wherein the receiving layer is either the network interface layer or the transport layer that is not the sending layer. Specifically, the F5 ‘901 Products manage packet transmission times and delays as part of the F5 ‘901 Product’s traffic optimization and prioritization functionality.

247. The F5 ‘901 Products can temporarily hold back the delivery of TCP packets. By delaying the delivery of packets, the F5 ;901 Products can reduce the burstiness of a transmission.

248. The F5 ‘901 Products enable sending the TCP packet to the receiving layer.

249. F5 has directly infringed and continues to directly infringe the ‘901 patent by, among other things, making, using, offering for sale, and/or selling technology for a data packet scheduler that reduces packet bursts, including but not limited to the F5 ‘901 Products.

250. The F5 ‘901 Products are available to businesses and individuals throughout the United States.

251. The F5 ‘901 Products are provided to businesses and individuals located in this District.

252. By making, using, testing, offering for sale, and/or selling products and services comprising technology for a data packet scheduler that reduces packet bursts, including but not limited to the F5 ‘901 Products, F5 has injured Plaintiff and is liable to Plaintiff for directly infringing one or more claims of the ‘901 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

253. F5 also indirectly infringes the ‘901 patent by actively inducing infringement under 35 U.S.C. § 271(b).

254. F5 has had knowledge of the ‘901 patent since at least service of this Complaint or shortly thereafter, and F5 knew of the ‘901 patent and knew of its infringement, including by way of this lawsuit.

255. F5 intended to induce patent infringement by third-party customers and users of the F5 ‘901 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. F5 specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘901 patent. F5 performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘901 patent and with the knowledge that the induced acts would constitute infringement. For example, F5 provides the F5 ‘901 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘901 patent, including at least claim 1, and F5 further provides documentation and training materials that cause

customers and end users of the F5 '901 Products to utilize the products in a manner that directly infringe one or more claims of the '901 patent.[20] By providing instruction and training to customers and end-users on how to use the F5 '901 Products in a manner that directly infringes one or more claims of the '901 patent, including at least claim 1, F5 specifically intended to induce infringement of the '901 patent. F5 engaged in such inducement to promote the sales of the F5 '901 Products, e.g., through F5 user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '901 patent. Accordingly, F5 has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '901 patent, knowing that such use constitutes infringement of the '901 patent.

[20] *See e.g.,* F5 BIG-IP LOCAL TRAFFIC MANAGEMENT: BASICS VERSION 13.0 (January 18, 2019); F5 BIG-IP LOCAL TRAFFIC MANAGER: CONCEPTS VERSION 11.5.1 (February 13, 2017); F5 BIG-IP LOCAL TRAFFIC MANAGER: IMPLEMENTATIONS VERSION 13.0 (March 4, 2019); *Using Selective Compression,* F5 DEVCENTRAL YOUTUBE CHANNEL (June 7. 2016), available at: https://www.youtube.com/watch?v=d85swKvXS1w; *Setup, Configuration and Backup of F5OS - rSeries: F5's Next Generation Appliance,* F5 DEVCENTRAL YOUTUBE CHANNEL (June 4, 2023), available at: https://www.youtube.com/watch?v=CiXkvkBWt6M; *Basic iRule Anatomy,* F5 DEVCENTRAL YOUTUBE CHANNEL (December 16, 2015), available at: https://www.youtube.com/watch?v=OhXS-Yt_gWc; *BIG-IP Basic Nomenclature,* F5 DEVCENTRAL YOUTUBE CHANNEL (April 12, 2017), available at: https://www.youtube.com/watch?v=2YRKTyMgV4M; *Introduction to rSeries: F5's Next Generation Appliance,* F5 DEVCENTRAL YOUTUBE CHANNEL (January 4, 2023), available at: https://www.youtube.com/watch?v=rCc5D6MEMcI; F5 BIG-IP LOCAL TRAFFIC MANAGER: DATA SHEET (2022); F5 STUDY GUIDE: 301B – BIG-IP LTM TECHNOLOGY SPECIALIST: MAINTAIN AND TROUBLESHOOT (2015); F5 BIG-IP LOCAL TRAFFIC MANAGER: DATA SHEET (2023); *F5 BIG-IP Local Traffic Policies*, F5 DEVCENTRAL YOUTUBE CHANNEL (August 12, 2025), available at: https://www.youtube.com/watch?v=-iLzxfKbl5A; *What is BIG-IP,* F5 DEVCENTRAL YOUTUBE CHANNEL (May 10, 2017), available at: https://www.youtube.com/watch?v=D6J_j7HdkV8; *BIG-IP Life of a Packet*, F5 DEVCENTRAL YOUTUBE CHANNEL (February 1, 2017), available at: https://www.youtube.com/watch?v=qCLEw5xIZ7s; *BIG-IP in the Public Cloud,* F5 DEVCENTRAL YOUTUBE CHANNEL (June 14, 2017), available at: https://www.youtube.com/watch?v=DMXpY9lx804; *LTM Load Balancing Algorithms: Round Robin, Ratio, & Dynamic Ratio*, F5 DEVCENTRAL YOUTUBE CHANNEL (June 8, 2019); https://www.youtube.com/watch?v=Gg-6yS12-7Q; and *BIG-IP LTM & DNS Load Balancer Integration*, F5 DEVCENTRAL YOUTUBE CHANNEL (Jone 4, 2020).

256. The ‘901 patent is well-known within the industry as demonstrated by multiple citations to the ‘901 patent in published patents and patent applications assigned to technology companies and academic institutions. F5 is utilizing the technology claimed in the ‘901 patent without paying a reasonable royalty. F5 is infringing the ‘901 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

257. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘901 patent.

258. As a result of F5’s infringement of the ‘901 patent, Plaintiff has suffered monetary damages, and seek recovery in an amount adequate to compensate for F5’s infringement, but in no event less than a reasonable royalty for the use made of the invention by F5 together with interest and costs as fixed by the Court.

COUNT VII
INFRINGEMENT OF U.S. PATENT NO. 9,936,040

259. Plaintiff references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

260. F5 designs, makes, uses, sells, and/or offers for sale in the United States products for caching and keying segments for efficient data retrieval.

261. F5 designs, makes, sells, offers to sell, imports, and/or uses the hardware, software, solutions, appliances, modules, services, technologies, platforms that include, incorporate, are designed to work with, can include, or are capable of integrating F5 NGINX Plus Release 12 and later (collectively, the “F5 ‘040 Product(s)”).

262. One or more F5 subsidiaries and/or affiliates use the F5 ‘040 Products in regular business operations.

263. The F5 ‘040 Products use ngx_http_slice_module to efficiently manage the acquisition of large files by breaking them down into smaller segments. When a client device requests a large file, the F5 ‘040 Products request only a portion of the file from the backend server, corresponding to the size of the slice. This slicing mechanism allows the F5 ‘040 Products to handle large content.

264. The F5 ‘040 Products utilize the Cache Slice module to store "slices" of a large file in its cache. Each slice is cached independently, allowing the F5 ‘040 Products to serve a part of the file directly from cache if a subsequent request matches a previously cached slice.

265. The F5 ‘040 Products generate a cache key based on aspects of the request that uniquely identify the requested content, such as the request URI, headers, or query parameters. The F5 ‘040 Products allows for the customization of cache keys through its configuration directives, enabling precise control over how content is cached and retrieved.

266. The F5 ‘040 Products generate a unique cache key for each slice of the content. This allows the F5 ‘040 Products to differentiate between the slices of a large file in the cache.

267. The F5 ‘040 Products append information about the slice range to the cache key, ensuring that each slice is uniquely identifiable.

268. The F5 ‘040 Products generate a first set entry that includes a first set key for the one or more segments associated with the first request. The F5 ‘040 Products create a structured entry in the cache that groups together related segments of content under a unified key, known as a set key. This set key acts as an identifier for the entire set of related content segments, facilitating efficient retrieval of all related segments when needed.

269. The F5 '040 Products perform the step of acquiring one or more segments related to an initial request, which originates from one or multiple client devices.

270. The F5 ‘040 Products perform the step of acquiring one or more segments associated with a first request through HTTP requests. When a client device initiates a request for content, the F5 ‘040 Products, acting as a reverse proxy or direct web server, receive this request. The F5 ‘040 Products then processes the request according to the configured rules and directives. If the content is not locally available or is designated to be fetched from a backend server, the F5 ‘040 Products establish a connection to the appropriate backend server(s) to retrieve the requested segments of data.

271. The F5 '040 Products store the acquired segments related to the initial request on a cache server.

272. The F5 '040 Products create a unique identifier for each segment among the one or more segments linked to the initial request.

273. The F5 '040 Products produce an initial set entry that encompasses a primary set key for the one or more segments tied to the initial request.

274. F5 has directly infringed and continues to directly infringe the ‘040 patent by, among other things, making, using, offering for sale, and/or selling technology for caching and keying segments for efficient data retrieval, including but not limited to the F5 ‘040 Products.

275. The F5 ‘040 Products are available to businesses and individuals throughout the United States.

276. The F5 ‘040 Products are provided to businesses and individuals located in this District.

277. By making, using, testing, offering for sale, and/or selling products and services for caching and keying segments for efficient data retrieval, including but not limited to the F5 ‘040

Products, F5 has injured Plaintiff and is liable to Plaintiff for directly infringing one or more claims of the '040 patent, including at least claim 14 pursuant to 35 U.S.C. § 271(a).

278. F5 also indirectly infringes the '040 patent by actively inducing infringement under 35 U.S.C. § 271(b).

279. F5 has had knowledge of the '040 patent since at least service of this Complaint or shortly thereafter, and F5 knew of the '040 patent and knew of its infringement, including by way of this lawsuit.

280. F5 intended to induce patent infringement by third-party customers and users of the F5 '040 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. F5 specifically intended and was aware that the normal and customary use of the accused products would infringe the '040 patent. F5 performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '040 patent and with the knowledge that the induced acts would constitute infringement. For example, F5 provides the F5 '040 Products that have the capability of operating in a manner that infringe one or more of the claims of the '040 patent, including at least claim 14, and F5 further provides documentation and training materials that cause customers and end users of the F5 '040 Products to utilize the products in a manner that directly infringe one or more claims of the '040 patent.[21] By providing instruction and training to

[21] *See e.g., Best Practices for Caching,* NGINX CONFERENCE PRESENTATION (2018); *NGINX Plus Reference Guide - Release 6,* F5 NGINX DOCUMENTATION (April 8, 2015); *NGINX Content Caching*, NGINX PLUS DOCUMENTATION (last visited February 2024), available at: https://docs.nginx.com/nginx/admin-guide/content-cache/content-caching/; *Using NGINX Plus for Advanced Video Streaming*, NGINX YOUTUBE CHANNEL (April 13, 2020), available at: https://www.youtube.com/watch?v=xbFBjvUT-k0; *Learn How to Stop Worrying and Build Your Own CDN,* NGINX BLOG (February 24, 2017), available at: https://www.nginx.com/blog/learn-to-stop-worrying-build-cdn/; *NGINX Plus Reference Guide - Release 16,* F5 NGINX DOCUMENTATION (April 28, 2018); *High-Performance Caching with NGINX and NGINX Plus*,

customers and end-users on how to use the F5 '040 Products in a manner that directly infringes one or more claims of the '040 patent, including at least claim 14, F5 specifically intended to induce infringement of the '040 patent. F5 engaged in such inducement to promote the sales of the F5 '040 Products, e.g., through F5 user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '040 patent. Accordingly, F5 has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '040 patent, knowing that such use constitutes infringement of the '040 patent.

281. The '040 patent is well-known within the industry as demonstrated by multiple citations to the '040 patent in published patents and patent applications assigned to technology companies and academic institutions. F5 is utilizing the technology claimed in the '040 patent without paying a reasonable royalty. F5 is infringing the '040 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

282. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '040 patent.

283. As a result of F5's infringement of the '040 patent, Plaintiff has suffered monetary damages, and seeks recovery in an amount adequate to compensate for F5's infringement, but in

NGINX Blog (August 24, 2016), available at: https://www.nginx.com/blog/nginx-high-performance-caching/; *Best Practices for Caching,* NGINX YOUTUBE CHANNEL (October 30, 2018), available at: https://www.youtube.com/watch?v=iNH6APQzIog; *NGINX Reverse Proxy,* NGINX PLUS DOCUMENTATION (last visited February 2024), available at: https://docs.nginx.com/nginx/admin-guide/web-server/reverse-proxy/; *Building a Powerful, Efficient and Highly Available Caching Layer with NGINX*, NGINX YOUTUBE CHANNEL (September 20, 2017), available at: https://www.youtube.com/watch?v=xZrOjmAkFC8; and *Smart and Efficient Byte-Range Caching with NGINX & NGINX Plus*, NGINX BLOG (January 21, 2016), available at: https://www.nginx.com/blog/smart-efficient-byte-range-caching-nginx/.

no event less than a reasonable royalty for the use made of the invention by F5 together with interest and costs as fixed by the Court.

COUNT VIII
INFRINGEMENT OF U.S. PATENT NO. 10,264,093

284. Plaintiff references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

285. F5 designs, makes, uses, sells, and/or offers for sale in the United States products for segment-based media data caching with unique key generation.

286. F5 designs, makes, sells, offers to sell, imports, and/or uses hardware, software, solutions, appliances, modules, services, technologies, platforms that include, incorporate, are designed to work with, can include, or are capable of integrating F5 NGINX Plus Release 12 and later (collectively, the "F5 '093 Product(s)").

287. One or more F5 subsidiaries and/or affiliates use the F5 '093 Products in regular business operations.

288. The F5 '093 Products perform the step of obtaining multiple segments of media data tied to an initial request, as well as multiple segments for a subsequent request, both initiated by one or more client devices.

289. The F5 '093 Products acquire multiple segments of media data for both initial and subsequent requests through HTTP requests. When the F5 '093 Products receive requests from client devices, the F5 '093 Products can serve as a reverse proxy to fetch segments from backend servers or from its cache if the data is already stored.

290. The F5 '093 Products utilize a Cache Slice module that allows NGINX Plus to request and cache only parts (slices) of a larger file.

291. The F5 '093 Products undertake the creation of multiple keys for the media data segments pertaining to the initial request and additional keys for the segments related to the subsequent request, assigning each segment a distinct identifier.

292. The F5 '093 Products generate a unique cache key that is associated with each segment of media data. The cache key is generated by the F5 '093 Products based on the request parameters and the segment's identifier.

293. The Cache Slice module in the F5 '093 Products enables the generating of unique keys for each slice of the content.

294. The F5 '093 Products create a first set entry, including a first set key for the segments associated with the first request, by utilizing the F5 '093 Products advanced cache key functionality. Specifically, the F5 '093 Products generate a composite key that represents a set of related segments, facilitating grouped caching and retrieval.

295. The F5 '093 Products execute the process of forming a primary set entry that encompasses a key representing the collective segments linked to the initial request.

296. The F5 '093 Products perform the step of creating associations between segments of subsequent requests and those of initial requests through conditional logic and variable comparisons using the JavaScript module (njs). In addition, the F5 '093 Products have functionality comparing request parameters and cache keys.

297. The F5 '093 Products engage in evaluating whether the media data segments from the subsequent request are connected to those from the initial request.

298. The F5 '093 Products carry out the formulation of an additional set entry containing a unique key for the segments tied to the subsequent request, provided these segments differ from those associated with the initial request.

299. The F5 ‘093 Products generate a second set entry for segments associated with the second request, distinct from those of the first request. Specifically, the F5 ‘093 Products create unique cache keys and use the njs module to recognize when segments do not match those of a prior request.

300. The Cache Slice module in the F5 ‘093 Products enables the slicing and caching of content segments with unique identifiers.

301. The F5 ‘093 Products group segments of media data associated with a particular request into a set for more efficient cache management. By generating a first set entry, which includes a unique key (the first set key) for the collection of segments associated with the first request, the F5 ‘093 Products can group segments. Specifically, the first set key is used by the F5 ‘093 Products as an identifier for all the segments of a particular media request, allowing the F5 ‘093 Products to perform batch operations on the cache.

302. The F5 ‘093 Products compare the segments requested in the second request with those in the first request to determine any overlap or association. Specifically, the F5 ‘093 Products analyze the keys of the segments. If the segments of the second request share keys with those of the first request, it indicates an association between them. If the segments are associated, the F5 ‘093 Products use the already cached segments instead of fetching them again from the origin server.

303. The F5 ‘093 Products generate a second set entry that includes a second set key. Specifically, when the segments of the second request are determined to be unrelated to those of the first request, the F5 ‘093 Products generate a new set entry for these segments, assigning a unique second set key.

304. F5 has directly infringed and continues to directly infringe the ‘093 patent by, among other things, making, using, offering for sale, and/or selling technology for segment-based media data caching with unique key generation.

305. The F5 ‘093 Products are available to businesses and individuals throughout the United States.

306. The F5 ‘093 Products are provided to businesses and individuals located in this District.

307. By making, using, testing, offering for sale, and/or selling products and services comprising a system for segment-based media data caching with unique key generation, including but not limited to the F5 ‘093 Products, F5 has injured Plaintiff and is liable to Plaintiff for directly infringing one or more claims of the ‘093 patent, including at least claim 7 pursuant to 35 U.S.C. § 271(a).

308. F5 also indirectly infringes the ‘093 patent by actively inducing infringement under 35 U.S.C. § 271(b).

309. F5 has had knowledge of the ‘093 patent since at least service of this Complaint or shortly thereafter, and F5 knew of the ‘093 patent and knew of its infringement, including by way of this lawsuit.

310. F5 intended to induce patent infringement by third-party customers and users of the F5 ‘093 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. F5 specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘093 patent. F5 performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘093 patent and with the knowledge that the induced

acts would constitute infringement. For example, F5 provides the F5 '093 Products that have the capability of operating in a manner that infringe one or more of the claims of the '093 patent, including at least claim 7, and F5 further provides documentation and training materials that cause customers and end users of the F5 '093 Products to utilize the products in a manner that directly infringe one or more claims of the '093 patent.[22] By providing instruction and training to customers and end-users on how to use the F5 '093 Products in a manner that directly infringes one or more claims of the '093 patent, including at least claim 7, F5 specifically intended to induce infringement of the '093 patent. F5 engaged in such inducement to promote the sales of the F5 '093 Products, e.g., through F5 user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '093 patent. Accordingly, F5 has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '093 patent, knowing that such use constitutes infringement of the '093 patent.

[22] *See e.g., Best Practices for Caching,* NGINX CONFERENCE PRESENTATION (2018); *NGINX Plus Reference Guide - Release 6,* F5 NGINX DOCUMENTATION (April 8, 2015); *NGINX Content Caching*, NGINX PLUS DOCUMENTATION (last visited February 2024), available at: https://docs.nginx.com/nginx/admin-guide/content-cache/content-caching/; *Using NGINX Plus for Advanced Video Streaming*, NGINX YOUTUBE CHANNEL (April 13, 2020), available at: https://www.youtube.com/watch?v=xbFBjvUT-k0; *Learn How to Stop Worrying and Build Your Own CDN,* NGINX BLOG (February 24, 2017), available at: https://www.nginx.com/blog/learn-to-stop-worrying-build-cdn/; *NGINX Plus Reference Guide - Release 16,* F5 NGINX DOCUMENTATION (April 28, 2018); *High-Performance Caching with NGINX and NGINX Plus*, NGINX Blog (August 24, 2016), available at: https://www.nginx.com/blog/nginx-high-performance-caching/; *Best Practices for Caching,* NGINX YOUTUBE CHANNEL (October 30, 2018), available at: https://www.youtube.com/watch?v=iNH6APQzIog; *NGINX Reverse Proxy,* NGINX PLUS DOCUMENTATION (last visited February 2024), available at: https://docs.nginx.com/nginx/admin-guide/web-server/reverse-proxy/; *Building a Powerful, Efficient and Highly Available Caching Layer with NGINX*, NGINX YOUTUBE CHANNEL (September 20, 2017), available at: https://www.youtube.com/watch?v=xZrOjmAkFC8; and *Smart and Efficient Byte-Range Caching with NGINX & NGINX Plus*, NGINX BLOG (January 21, 2016), available at: https://www.nginx.com/blog/smart-efficient-byte-range-caching-nginx/.

311. The ‘093 patent is well-known within the industry as demonstrated by multiple citations to the ‘093 patent in published patents and patent applications assigned to technology companies and academic institutions. F5 is utilizing the technology claimed in the ‘093 patent without paying a reasonable royalty. F5 is infringing the ‘093 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

312. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘093 patent.

313. As a result of F5’s infringement of the ‘093 patent, Plaintiff has suffered monetary damages, and seeks recovery in an amount adequate to compensate for F5’s infringement, but in no event less than a reasonable royalty for the use made of the invention by F5 together with interest and costs as fixed by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff OptiMorphix, Inc. respectfully requests that this Court enter:

A. A judgment in favor of Plaintiff that F5 has infringed, either literally and/or under the doctrine of equivalents, the ‘273, ‘353, ‘871, ‘559, ‘169, ‘901, ‘040, and ‘093 patents;

B. An award of damages resulting from F5’s acts of infringement in accordance with 35 U.S.C. § 284;

C. A judgment and order finding that F5’s infringement was willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate within the meaning of 35 U.S.C. § 284 and awarding to Plaintiff enhanced damages.

D. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff reasonable attorneys' fees against F5.

E. Any and all other relief to which Plaintiff may show themselves to be entitled.

JURY TRIAL DEMANDED

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

Dated: February 22, 2024

Respectfully submitted,

/s/ Daniel P. Hipskind

Dorian S. Berger (CA SB No. 264424)
Daniel P. Hipskind (CA SB No. 266763)
Erin E. McCracken (CA SB No. 244523)
BERGER & HIPSKIND LLP
9538 Brighton Way, Ste. 320
Beverly Hills, CA 90210
Telephone: 323-886-3430
Facsimile: 323-978-5508
E-mail: dsb@bergerhipskind.com
E-mail: dph@bergerhipskind.com
E-mail: eem@bergerhipskind.com

Elizabeth L. DeRieux
State Bar No. 05770585
Capshaw DeRieux, LLP
114 E. Commerce Ave.
Gladewater, TX 75647
Telephone: 903-845-5770
E-mail: ederieux@capshawlaw.com

Attorneys for OptiMorphix, Inc.