PAUL J. ANDRE (State Bar No. 196585)
pandre@kramerlevin.com
LISA KOBIALKA (State Bar No. 191404)
lkobialka@kramerlevin.com
JAMES HANNAH (State Bar No. 237978)
jhannah@kramerlevin.com
KRISTOPHER KASTENS (State Bar No. 254797)
kkastens@kramerlevin.com
KRAMER LEVIN NAFTALIS & FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800

Attorneys for Plaintiff
FINJAN, INC.

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

FINJAN, INC., a Delaware Corporation,

Plaintiff,

v.

JUNIPER NETWORKS, INC., a Delaware Corporation,

Defendant.

Case No.: 3:17-cv-05659-WHA

PLAINTIFF FINJAN, INC.'S RESPONSE REGARDING PATENT ELIGIBILITY OF U.S. PATENT NO. 8,677,494

Claim 10 of U.S. Patent No. 8,677,494 (Trial Ex. 1, the "'494 Patent") is patent eligible under 35 U.S.C. § 101 because it teaches how to protect a user from malicious malware on the Internet using behavior-based analysis which was directly contrary to the conventional thinking at the time of filing the '494 Patent. Further, the Court should follow the Federal Circuit holding which confirmed that Finjan's behavior-based scanning technique (which is covered in the '494 Patent) is non-abstract and Judge Orrick's and Judge Freeman's reasoning finding that Claim 10 of the '494 Patent includes an inventive concept.

I. FACTUAL BACKGROUND

The '494 Patent solved a major problem in computer security. In 1996, when the invention of the '494 Patent was filed, viruses infected computer much like a cold and would spread when a file was shared on floppy disks attaching itself to other files on a user's computer. Trial Tr. at 226:1-19, 885:16-19. To combat these viruses, anti-virus companies would obtain the virus, dissect it, and write signatures which identified a series of unique bytes within the virus. Trial Tr. at 233:8-23, 234:16-24. If a file was scanned on a user's computer and it matched a signature of a virus, the file was deemed infected and remedial measures would be taken. Trial Tr. at 233:8-23, 234:16-24. This technique was known as "reactive" because the virus had to be known, obtained, and analyzed before any protection could be put in place to protect against the virus. Trial Tr. at 233:8-23; 235:1-7.

With the debut of the Internet, Finjan realized that signature-based technique would no longer work. Trial Tr. at 226:16-19. Instead of spreading viruses that attach to files, hackers would be able to create powerful malicious stand-alone software (termed "malware") that would infect computers as soon as the program was downloaded and run. Trial Tr. at 234:1-9. Finjan coined these threats as "Downloadables" and there was no solution that protected against them. U.S. Pat. No. 6,092,194 (the "'194 Patent") at 1:41-49 ("these security systems [at the time] are not configured to recognize computer viruses which have been attached to or configured as Downloadable application programs, commonly referred to as 'Downloadables'"); Trial Tr. at 869:3-870:8 (Downloadables were a "new kind of threats … and were not very well recognized and understood").

To protect against these new types of threats, Finjan invented proactive security that did not rely upon traditional signatures but rather analyzed the behavior of a program. Trial Ex. 107 at FINJAN-JN 437129 (recognizes Finjan is "the inventor of proactive content behavior inspection"). Contrary to traditional reactive techniques, Finjan's proactive approach created a behavior profile of the Downloadable and determined whether the behavior was malicious based on the generated profile. '494 Patent, Claim 10 (reciting "deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable"). In this way, Finjan was able to detect against brand-new malicious software programs that attempted to run on a user's computer regardless of whether anti-virus companies had analyzed the program before or tried to create a signature for it. *Finjan, Inc. v. Sophos, Inc.*, 244 F. Supp. 3d 1016, 1061 (N.D. Cal. 2017) (stating that the '494 Patent describes a technique capable of detecting unknown viruses); Trial Ex. 107 at FINJAN-JN 437130 (Finjan "provides day-zero defense against new, previously unknown attacks by leveraging its proprietary application-level behavior blocking technology").

The industry did not adopted Finjan's technology, in the beginning, for a number of reasons. First, the Internet was in its early stages and the threat of malicious Downloadables was simply not prevalent. Second, it was computationally expensive to generate a behavior profile for every Downloadable that was encountered. Third, it is difficult to break into an industry with cutting edge technology that had not been tested for many years before. '494 Patent at 1:65-2:21; *see also* Trial Tr. at 876:3-877:18 (explaining none of Juniper's alleged prior art provides the same level of functionalities as Claim 10 of the '494 Patent). In fact, industry reports published years after the invention of the '494 Patent showed that the computer security industry was slow to adopt behavior-based analysis, which confirms that the technique of Claim 10 was not well-understood, routine, or conventional in 1996. *See* Trial Ex. 126 at FINJAN-JN 009790-91 (where a 2003 industry report states that "[f]orward-looking organizations are beginning to realize they cannot rely upon reactive signature-based antivirus technology alone" and "IDC believes the integration of real-time behavior analysis technologies with traditional signature-based antivirus technologies will allow for a greater degree of accuracy in detecting both known and unknown threats"); Trial Ex. 125 at FINJAN-JN 429657 (which is a market analysis report bearing a copyright date of 2003, where the report states that "[s]everal proactive virus detection technologies, such as behavior-based analysis and heuristics, are becoming part of organizations' security architectures."); Trial Ex. 105 at FINJAN-JN 437020 (where a U.S. Government presentation shows that pre-2008, malware detection is largely signature-based).

The Federal Circuit confirmed that Finjan was the pioneer of behavior-based malware detection, upholding the patentability of its parent application on those grounds. U.S. Patent No. 6,154,844 (the "'844 Patent") is a parent to the '494 Patent. The Federal Circuit confirmed that the '844 Patent was patent eligible because it covers behavior-based detection, just like the '494 Patent. *Finjan, Inc. v. Blue Coat Sys., Inc.*, 879 F.3d 1299, 1304 (Fed. Cir. 2018) ("[t]he question, then, is whether this behavior-based virus scan in the '844 patent constitutes an improvement in computer functionality. We think it does."); *see also Blue Coat Sys.*, 879 F.3d at 1304 ("[t]he 'behavior-based' approach to virus scanning was pioneered by Finjan" and "[i]n contrast to traditional 'code-matching' systems, which simply look for the presence of known viruses, 'behavior-based' scans can analyze a downloadable's code and determine whether it performs potentially dangerous or unwanted operations–such as renaming or deleting files."); *Ancora Techs., Inc. v. HTC Am., Inc.*, 908 F.3d 1343 (Fed. Cir. 2018) ("In *Finjan*, we held that claims to a 'behavior-based virus scan' were a specific improvement in computer functionality and hence not directed to an abstract idea.") (citing *Blue Coat Sys.*, 879 F.3d at 1304).

II. LEGAL FRAMEWORK

The '494 Patent should be viewed in the light most favorable to Finjan because patents are presumed valid under 35 U.S.C. § 101 unless proven otherwise by clear and convincing evidence. *CLS Bank Int'l v. Alice Corp. Pty. Ltd.*, 717 F.3d 1269, 1304-05 (Fed. Cir. 2013); *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1368 (Fed. Cir. 2018).

III. ARGUMENT

1. The Court Should Adopt the Reasoning Judges Freeman and Orrick, and Find Claim 10 Patent Eligible under Step Two of *Alice*

Two courts in this District have already found Claim 10 of the '494 Patent eligible under *Alice* step two because claim elements, when considered as a whole, recite an inventive concept. *Finjan, Inc. v. Blue Coat Sys. LLC*, No. 15-cv-03295-BLF, 2016 WL 7212322, at *11 (N.D. Cal. Dec. 13, 2016) (“at the time of invention, virus protection was localized and reactive” and that the ’494 Patent claims “both spatial and temporal alterations to this paradigm”) (the “*Blue Coat* Order”); *Sophos*, 244 F. Supp. 3d at 1061 (the “*Sophos* Order”) (“[l]ooking at the ’494 patent as a whole, the claims recite an inventive concept because they detail a system that involves scanning malware on an intermediate network, rather than an end-user computer, and because they detail a process for identifying unknown viruses by extracting specific suspicious operations from files.”).

In the *Sophos* Order, Judge Orrick agreed with Judge Freeman’s analysis in the *Blue Coat* Order, and found that “the claims recite an inventive concept when taken as an ordered combination and considered in context.” *Sophos*, 244 F. Supp. 3d at 1060. Judge Orrick found that “prior to its invention, malware protection programs were only able to detect and protect against known viruses and were installed on particular user computers.” *Id.*, *citing* ’494 Patent at 2:11-21. First, “the patent specifications make clear that the claim steps take place on a network” and “this arrangement represents a novel use of specific computer systems in a ‘non-conventional and non-generic arrangement’ to improve malware protection systems for computer networks.” *Id.* at 1960-61. Second, the ’494 Patent involves extracting operations of a file he found “innovative because it allows a malware detection program to detect new viruses, previously unknown files that contain suspicious operations, rather than identifying only known viruses.” *Id.*, *citing* ’494 Patent at 2:56-64.

The trial record supports the reasoning of Judge Orrick and Judge Freeman that the elements of Claim 10 recite an inventive concept that were not well-understood, routine, or conventional in 1996. Claim 10 addresses a problem from the advances of the computer networks technologies, which provided a new way of spreading viruses (*i.e.* via Downloadables) and allowed viruses to spread faster. Trial Tr. at 226:1-227:7 (“prior to the mid-’90s, the Internet has not yet taken off” and it was fairly slow “propagating viruses at the time; but then once the Internet came about, then it was much, much easier for viruses to simply be downloaded over the Internet”); ’194 Patent at 1:29-36 (the public Internet “has become a major source of many system damaging and system fatal application programs”); Trial Tr. at 869:3-870:8 (Downloadables were a “new kind of threats … and were not very well recognized and understood”). These types of inventions, *i.e.*, those that address the problem caused by Internet

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE

fastcase® Smarter legal research.