1
2
3
4   UNITED STATES DISTRICT COURT

5   NORTHERN DISTRICT OF CALIFORNIA

6

7   FINJAN, INC.,   Case No. 14-cv-01197-WHO

8   Plaintiff,

9   v.   **ORDER RE POST-TRIAL MOTIONS**

10 SOPHOS, INC.,

11   Defendant.

12   **INTRODUCTION**

13   In this patent case, plaintiff Finjan, Inc. ("Finjan") accuses Sophos, Inc. ("Sophos") of

14 infringing five of Finjan's patents in the malware security software space. Following a two week

15 trial, a jury found that Sophos infringed all five of Finjan's asserted patents and awarded damages

16 of $15 million for the life of the patents. The parties have filed five post-trial motions: Finjan filed

17 a Motion for Attorneys' Fees and Costs, a Motion for a New Trial, or in the Alternative,

18 Remittitur, and a Motion to Amend the Judgment and for an Injunction; and, Sophos filed a

19 Renewed Motion for Judgment as a Matter of Law and a Motion for a Partial Judgment and

20 Finding of Fact. All five motions are DENIED, with the exception that Finjan's request for Pre-

21 and Post-Judgment Interest is GRANTED. Pre-and Post-Judgment interest will be awarded at the

22 treasury bill rate.

23   **MOTION FOR ATTORNEYS' FEES**

24   **BACKGROUND**

25   Finjan moves for Attorneys' Fees and Costs under 35 U.S.C. § 285 of the Patent Act,

26 which permits courts to award attorneys' fees in "exceptional cases." Finjan asserts that this is an

27 "exceptional case" because Sophos: (1) pursued objectively unreasonable invalidity defenses

28 premised on egregious litigation misconduct; (2) pursued meritless non-infringement defenses;

1   (3) engaged in pre-trial misconduct by refusing to streamline issues for trial; (4) engaged in

2   discovery misconduct related to its production of source code; and (5) improperly delayed

3   document production and produced irrelevant documents. After reviewing the parties' briefs and

4   the facts presented, I conclude that this is not an exceptional case warranting attorneys' fees and

5   costs.

6   **LEGAL STANDARD**

7   Section 285 permits a court to award attorneys' fees only in "exceptional cases" or ones

8   that are "uncommon, rare, or not ordinary." *Octane Fitness, LLC v. ICON Health & Fitness, Inc.*,

9   134 S.Ct. 1749, 1756 (2014). A case is exceptional when it "stands out from others with respect

10 to the substantive strength of a party's litigating position (considering both the governing law and

11 the facts of the case) or the unreasonable manner in which the case was litigated." *Id.* "District

12 courts may determine whether a case is 'exceptional' in the case-by-case exercise of their

13 discretion, considering the totality of the circumstances." *Id.* Relevant factors in assessing

14 whether a case is exceptional include "frivolousness, motivation, objective unreasonableness (both

15 in the factual and legal components of the case) and the need in particular circumstances to

16 advance considerations of compensation and deterrence." *Id.* at 1756, n.6. Most courts awarding

17 attorneys' fees post-*Octane* "have generally cited egregious behavior." *Aylus Networks, Inc. v.*

18 *Apple, Inc.*, No. 13-cv-4700-EMC, 2016 WL 1243454, at *7 (N.D. Cal. Mar. 30, 2016).

19   **DISCUSSION**

20 **I.   SOPHOS'S INVALIDITY DEFENSES**

21   Finjan first argues that Sophos engaged in egregious litigation misconduct by putting

22 forward meritless invalidity defenses. It asserts that Sophos relied on a trial demonstrative and

23 third-party components that were not prior art to satisfy claim elements of its Asserted Sweep-

24 InterCheck Art. Review of the record undermines Finjan's claims.

25   **A. The Demo2 Demonstrative**

26   Finjan asserts that Sophos improperly relied exclusively on "Demo2", a trial

27 demonstrative, to show certain elements of Claim 7 of the '844 Patent, Claim 18 of the '926

28 patent, and Claim 14 of the '494 Patent ("the Script Claim Elements") that were necessary to its

1   anticipation argument. Because Demo2 was created as a trial demonstrative, it is not prior art and

2   could not be used as direct evidence of anticipation. Indeed, in my May Order on Finjan's

3   summary judgment motion for validity, I noted that "Dr. Cohen obviously cannot rely on the

4   Demo2 programs as distinct prior art references." Dkt. No. 205 at 18. Finjan asserts that Sophos

5   violated this order because for the Script Claim Elements Dr. Cohen directed the jury only to his

6   slides on the Demo2 demonstrative and not to any actual source code. Finjan argues that this is

7   serious misconduct and makes this an exceptional case. *See, z4 Techs., Inc. v. Microsoft Corp.*,

8   No. 6-c-142, 2006 WL 2401099, at *23 (E.D. Tex. Aug. 18, 2006), *aff'd*, 507 F.3d 1340 (Fed. Cir.

9   2007) (awarding fees where defendant submitted false declaration to beat summary judgment).

10   Despite Finjan's assertions, the trial record shows that Sophos did not attempt to rely on

11   Demo2 as prior art. Dr. Cohen was clear that Demo2 was a "program that is compiled from a

12   source code program that [he] wrote that is intended to demonstrate the things that we're talking

13   about SWEEP-InterCheck doing." Trial Tr. at 1369:7-13. He added that Demos 2 was used to

14   "test that [his] analysis of the code was correct." Trial Tr. at 1461:18-19. When asked by Finjan's

15   counsel whether Demo2 satisfied a limitation of the asserted claims Dr. Cohen responded that

16   "SWEEP-InterCheck is the thing that meets the limitations." Trial Tr. at 1495:7-10.

17   As the record shows, Dr. Cohen used Demo2 as a demonstrative to help explain and

18   demonstrate his analysis of SWEEP-InterCheck. That Dr. Cohen pointed to his slides from the

19   Demo2 presentation when asked about the Script Claim Elements does not indicate that Dr. Cohen

20   attempted to use Demo2 itself as prior art. Given the full context of Dr. Cohen's testimony it

21   appears that Dr. Cohen was referring the jury generally to his testimony and analysis on SWEEP-

22   InterCheck and the portions of his Demo2 demonstration that helped illustrate the testimony most

23   relevant to the Script Claim Elements. Dr. Cohen's use of Demo2 as a demonstrative was

24   appropriate and not misconduct.

25   **B. Demo2's Programming and Reference to JavaScript**

26   Finjan next argues that Sophos engaged in misconduct because Dr. Cohen programmed

27   Demo2 to display words referencing "JavaScript" or "script." Finjan contends that this

28   misleadingly gave the impression that SWEEP-InterCheck can execute JavaScript, when it cannot,

3

1   and that Sophos relied on this misimpression to argue that SWEEP-InterCheck was able to receive

2   and inspect Downloadables, even when "the Downloadable includes JavaScript script." Ex. 3

3   Trial Tr. at 1407:24-1408:13; 1483:22-1484:1. It argues that because the Asserted Sweep Art

4   could not execute JavaScript, Sophos's attempt to show that it was able to receive and inspect

5   JavaScript Downloadables was frivolous and misleading.

6   Sophos's attempt to show that SWEEP-InterCheck satisfied this claim element was not

7   misleading. Sophos did not attempt to argue that SWEEP-InterCheck could execute JavaScript –

8   instead it argued that the claim did not require that the product "execute JavaScript" but merely

9   receive and inspect it. This is a reasonable, plain language interpretation of the claim and does not

10   demonstrate any kind of misconduct. Further, Dr. Cohen was clear to explain that SWEEP-

11   InterCheck does not execute JavaScript. Oppo. to Fees Mot. at 6. When asked whether he had

12   tried to show that SWEEP can execute a JavaScript program, Dr. Cohen testified, "No, that's not

13   what I said. What I said was pretty clear, that the executable program contained JavaScript, that it

14   printed it, that it wasn't interpreted or run in anyway. It just included it. That's what the patent

15   says." Trial Tr. at 1463:18-25. Dr. Cohen's inclusion of the "JavaScript" language in his Demo2

16   program was reasonable and was not part of a scheme to mislead the jury about SWEEP's ability

17   to execute a JavaScript program. Dr. Cohen's programming does not make this an exceptional

18   case.

19   **C. Ethernet Cards and Web Browsers**

20   Finally, Finjan argues that Sophos's invalidity arguments were frivolous because Dr.

21   Cohen testified that an Ethernet and Web Browser satisfied certain elements of the patents for the

22   purposes of anticipation, but these items were not part of the Asserted Sweep Art source code.

23   Mot. for Fees at 12. Sophos rebuts that it did not attempt to argue that the Ethernet and Web

24   Browser were prior art, but that SWEEP-InterCheck is prior art and necessarily requires these

25   outside elements to work. Oppo. to Fees at 7.

26   "A prior art reference may anticipate without disclosing a feature of the claimed invention

27   if that missing characteristic is necessarily present, or inherent, in the single anticipating

28   reference." *Schering Corp. v. Geneva Pharm.*, 339 F. 3d 1373, 1377 (Fed. Cir. 2003). Sophos

4

1   argues, "Just as a computer is necessary to run SWEEP-InterCheck, an Ethernet Card and

2   Microsoft operating system are necessary components of the computer system." Oppo. to Fees at

3   7. Notably, in the prior case between Finjan and Sophos, the Delaware court permitted Sophos to

4   rely on these outside elements in asserting its prior art. *Id.*; *Finjan, Inc. v Symantec Corp.*, 2013

5   WL 5302560, at *18 (D. Del. Sept. 19, 2013) (*JMOL Order*) ("[A]s SWEEP-InterCheck receives

6   incoming Downloadables, a functionality that the jury observed, it is clear that a network interface

7   would be necessary to receive that Downloadable.").

8   Sophos did not engage in misconduct by arguing that SWEEP-InterCheck included an

9   Ethernet Card and Web Browser. It has made a plausible showing that SWEEP included an

10 Ethernet Card and operating system even though these elements are not disclosed in the claimed

11 invention. Further, because Sophos successfully made this argument before the Delaware court, it

12 was not objectively frivolous or unreasonable for it to assert the same argument here. Sophos's

13 reliance on the Ethernet and Web Browser as part of its anticipation argument does not make this

14 an exceptional case.

15   **II. NON-INFRINGEMENT DEFENSE**

16   **A. Mr. Klausner's Construction of the term "database"**

17   Finjan argues that Sophos acted extraordinarily because its non-infringement expert, Mr.

18 Klausner, offered an unreasonable interpretation of the term "database." Mot. for Fees at 12. At

19 claim construction, I construed the term "database" to mean "[a] collection of interrelated data

20 organized according to a database scheme to serve *one or more* applications." Dkt. No. 73 at 3.

21 (emphasis added). At trial, and previously in his expert report, Klausner opined that the

22 requirement to "serve one or more applications" required a database to serve at least two

23 applications. Trial Tr. at 1241:18-19. Finjan asserts that this opinion is a frivolous perversion of

24 the English language and so entitles them to fees and costs.

25   Although Klausner's interpretation of "database" was not particularly convincing, this

26 single aspect of his opinion does not render this an extraordinary case. First, Klausner's non-

27 infringement opinion did not hinge on this interpretation. As he testified at trial, he did not base

28 his non-infringement opinion on whether a database "has to be more than one application."

5

1   Indeed the issue was only raised by Finjan on cross examination for impeachment purposes. Trial

2   Tr. 1241:4-6. The focus of Klausner's non-infringement opinion was instead that Sophos's

3   accused products do not have "databases" within the meaning of the patent because they do not

4   have a "database manager" and because they do not store information. For example, he explained

5   that Sophos's Blackboard system does not have a database manager and does not store

6   information because when it receives a downloadable security profile system "it just sits in

7   memory, just for the scan of that one particular file, and then goes away." Trial Tr. at 1222:3-14.

8   Mr. Klausner's interpretation that "database" must serve more than one application was irrelevant

9   to this testimony.

10   While Klausner's interpretation that a "database" must serve more than one application

11   was not persuasive, his non-infringement opinion did not rely on this interpretation. This minor

12   aspect of his opinion had virtually no impact on the case. If anything, Klausner's interpretation of

13   "database" provided Finjan a strong line of attack on Klausner's credibility, an issue that Finjan

14   successfully emphasized on cross-examination and in closing arguments. Klausner's

15   interpretation of "database" does not make this an exceptional case.

16   **B. Klausner relied on the Delaware case**

17   Finjan asserts that Sophos acted unreasonably because its infringement expert Mr.

18   Klausner relied on and referenced the Delaware action in his expert report. Mot. for Fees at 8.

19   Finjan claims that this was improper because the Delaware action involved different patents and

20   different products and so was irrelevant to the claims here. *Id.* While I have previously expressed

21   skepticism that the Delaware action is relevant to the issues of infringement and invalidity in this

22   case, Klausner did not engage in gross misconduct by referencing it in his report. An expert is

23   entitled to rely on anything typically relied on by experts in their field. Fed. R. Evid. 703. The

24   '194 patent, asserted in the Delaware case, is directly related to four of the patents asserted in this

25   case, and the accused products and technology are similar in both cases. Klausner's attempt to

26   draw parallels to the Delaware case was not unreasonable and does not justify awarding attorneys'

27   fees.

28

                                           6

III. STREAMLINING ISSUES

Finjan argues that Sophos acted unreasonably because it refused to narrow its election of SWEEP-InterCheck products early in the litigation. Mot. for Fees at 15. Early in the case, Sophos asserted hundreds of versions of Sweep and InterCheck as prior art, despite requests from Finjan to elect particular versions and combinations. Sophos maintained that it was unnecessary for it to elect particular versions of SWEEP and InterCheck because there were no substantive differences between individual versions. When Sophos's expert Dr. Cohen used previously undisclosed versions of the products in his expert report, Finjan filed a motion to strike his opinions, which I granted. I subsequently ordered Sophos to elect a single combination of SWEEP-InterCheck to assert as prior art, which it then did. Finjan argues that Sophos's failure to elect a single version of prior art earlier in the litigation, or otherwise narrow its election to fewer versions, caused Finjan to waste considerable time and expense and was unreasonable.

Sophos's position that SWEEP-InterCheck is a single product and that it was therefore not necessary for it to elect particular versions was not wholly unreasonable. There is no evidence that Sophos engaged in misconduct by failing to narrow its election of particular SWEEP-InterCheck versions earlier in the litigation. Sophos's failure to comply with Finjan's request does not make this an exceptional case.

IV. SOURCE CODE

Finjan asserts that Sophos engaged in misconduct by attempting to obfuscate its source code productions. It contends that Sophos required Finjan to pay to have the source code transferred from Texas to California; that it produced source code that was organized in a confusing way with no discernible directory structure; that it pointed Finjan to a particular directory containing 29,000 files that it later admitted did not have relevant code; that Sophos's engineers testified that the source code production did not appear to be organized the way it was organized in the ordinary course; that Sophos presented a "blueprint" of the source code that failed to make the code discernible; that Sophos eventually gave Finjan access to its Perforce system where Finjan could see previously unviewable comments and references to Finjan that later disappeared; and that Sophos produced highly relevant source code near the end of discovery.

Mot. for Fees at 17-19.

Sophos rebuts that it did not do anything improper and that Finjan's trouble with understanding its source code does not amount to misconduct on the part of Sophos. It responds to Finjan's accusations by explaining that it produced its source code as it was kept in the ordinary course and only altered the code by dividing it into three top-level folders for the purposes of production; that Sophos provided Finjan with information on where the master build files were in its source code so that it could make sense of the code and offered to help Finjan's reviewer find the master build files; that it provided Finjan with access to its internal Perforce source code repository which includes both released code and code that is still in development - something that most technology companies would never provide access to; that it did not restrict Finjan's access to comments and references to Finjan in the Perforce system and demonstrated during the deposition of Robert Cook that it was still possible to access these files using Finjan's credentials; and that the code produced near the end of discovery was updated versions of the code Finjan already had that had previously not been available for production. Oppo. to Fees at 10-12.

Discovery of complex information, such as source code, is expensive and difficult and often requires substantial time and energy from all parties. Finjan highlights a number of problems in making sense of the Sophos source code and some hiccups in the production process, but these sorts of problems are to be expected during complex discovery. There is no evidence that Sophos intentionally obfuscated its code. All relevant code was produced by the discovery deadline. The conduct here does not rise to the level of misconduct: Sophos did not refuse to produce relevant information, did not violate any court orders, and did not display a "shifting litigation position." *Juniper Networks, Inc. v. Toshiba Am., Inc.*, No. 5-c-479, 2007 WL 2021776, at *3-5 (E.D. Tex. July 11, 2007); *Fleming v. Escort, Inc.*, No. 9-c-105, 2015 WL 713532, at *2 (D. Idaho Feb. 21, 2014); *Trs. of Bos. Univ. v. Everlight Elecs. Co.*, No. 12-c-11935, 2016 WL 3976603, at *3-4 (D. Mass. July 22, 2016). Sophos's conduct was reasonable and does not evidence misconduct.

V. DOCUMENT PRODUCTION

Finally, Finjan argues that Sophos acted unreasonably by producing over ten thousand

8

1   pages of irrelevant documents; by producing thousands of spam emails; and by producing a

2   substantial number of documents late in the discovery period, even though it had printed many of

3   those documents many months earlier. Mot. for Fees at 21.

4   Sophos acknowledges that it inadvertently produced some irrelevant documents, but notes

5   that these documents represented a fraction of the total documents produced and asserts that this

6   does not make this an exceptional case. *Vehicle IP, LLC v. Gen. Motors Corp.*, No. 07-c-345,

7   2008 WL 2273682, at *4 (W.D. Wis. June 2, 2008) (the production of irrelevant documents was

8   "not so unusual (unfortunately) as to make this an exceptional case"). It explains that it produced

9   the "spam" emails because these emails were responsive to specific search-term requests Finjan

10 had made and it was trying to comply with those requests. Oppo. to Fees at 14. Finally, it notes

11 that it produced all responsive documents before the close of fact discovery and asserts that a

12 minor discovery dispute, such as this, does not make this an exceptional case. *Indus., Inc. v. Kari-*

13 *Out Club, LLC*, No. 08-c-5349, 2013 WL 4730653, at *3 (D.N.J. Sept. 3, 2013) ("[P]edestrian

14 discovery disputes of the type concomitant with intellectual property litigation" do not make a

15 case exceptional). Sophos's conduct during document production appears to have been reasonable

16 and does not make this an exceptional case.

17 As Finjan's arguments reveal, this was a hard fought and zealously litigated case. Finjan

18 has pointed to various disputes between the parties that arose during the two years of this litigation

19 but has failed to identify any conduct by Sophos that would rise to the level of misconduct

20 necessary to find this an "exceptional case" and award attorneys' fees under Section 285. I

21 conclude that attorneys' fees are not appropriate. Finjan's motion for attorneys' fees and costs is

22 DENIED.

23 **MOTION FOR NEW TRIAL**

24 **BACKGROUND**

25 Sophos moves for a new trial, or in the alternative, remittitur. Mot. for New Trial (Dkt.

26 No. 423). It argues that it is entitled to a new trial on invalidity because (1) collateral estoppel

27 should apply to the issue of anticipation by SWEEP-InterCheck; (2) the jury's verdict was against

28 the clear weight of the evidence; (3) and Finjan intentionally presented evidence of post-grant

9

1   proceedings at trial in violation of an *in limine* order. *Id.* at 2. It also contends that it is entitled to

2   a new trial on infringement because the jury's verdict was against the clear weight of the evidence.

3   *Id.* In the alternative, Sophos asserts that it is entitled to a remittitur on damages because Finjan

4   improperly included fictional revenue in its royalty base. As discussed below, Sophos has failed

5   to show that collateral estoppel applies to this case or that the jury's verdict was against the clear

6   weight of the evidence. It has also failed to show that the jury's damage award included

7   SophosLabs revenues. Sophos's motion for a new trial or a remittitur is denied.

8   **LEGAL STANDARD**

9   Under Federal Rule of Civil Procedure 59(a), a court may grant a new trial to any party on

10   some or all issues after a jury trial. Fed. R. Civ. P. 59(a)(1). In patent cases, the local Circuit's

11   law on Rule 59 governs the standard for granting a new trial. *Finisar Corp. v. DirecTV Grp., Inc.*,

12   523 F.3d 1323, 1328 (Fed. Cir. 2008). In the Ninth Circuit, a "district court can grant a new trial

13   under Rule 59 on any ground necessary to prevent a miscarriage of justice." *Experience Hendrix*

14   *L.L.C. v. Hendrixlicensing.com Ltd.*, 762 F.3d 829, 842 (9th Cir. 2014).

15   **DISCUSSION**

16   **I.   NEW TRIAL ON INVALIDITY**

17   A.   **Collateral Estoppel**

18   Sophos asserts that it is entitled to a new trial on invalidity because collateral estoppel

19   should apply to the issue of anticipation by SWEEP-InterCheck. Mot. for New Trial at 3. It

20   contends that this exact issue was litigated in the prior Delaware action between the parties. *Id.*

21   Collateral estoppel applies where (1) the issue to be resolved is identical to an issue raised in the

22   prior litigation; (2) the issue was actually litigated in the prior litigation; and (3) the determination

23   of the issue in the prior litigation was a necessary part of the judgment in that action. *Littlejohn v.*

24   *United States*, 321 F.3d 915, 923 (9th Cir. 2003).

25   Sophos argues that collateral estoppel applies because "a jury in Delaware found all

26   asserted claims of Finjan's '194 patent anticipated by SWEEP-InterCheck." Mot. for New Trial at

27   4. The '194 patent was not asserted in this case but is related to four of the five asserted patents:

28   the '494, '844, '780, and '926 patents. *Id.* These four patents and the '194 patent all claim

                                                          10

1   priority to the same provisional patent application (No. 60/30,639) and the four patents asserted in

2   this case incorporate the '194 patent by reference. Because of the close relationship between the

3   '194 patent and the patents asserted here, Sophos contends that many of the anticipation

4   arguments for the asserted patents are collaterally estopped by the Delaware judgment.

5   Sophos previously raised this issue in its motion for partial summary judgment. It argued

6   that collateral estoppel should apply because it was asserting the same combination of SWEEP-

7   InterCheck in this case that it had asserted in the Delaware case – SWEEP-2.72 & InterCheck-

8   2.11. However, I ruled that Sophos could not assert the SWEEP-2.72 & InterCheck-2.11

9   combination because it did not timely elect and disclose that combination in this case. Dkt. No.

10   205 at 34. Because Sophos's collateral estoppel argument hinged on the fact that it was asserting

11   combination SWEEP-2.72 & InterCheck-2.11, and I ruled it could not assert that combination, I

12   rejected its collateral estoppel argument. *Id.* In this case Sophos ultimately elected SWEEP-2.72

13   & InterCheck-2.01. Sophos argues that, despite my prior ruling, collateral estoppel should apply

14   because (1) there is no legal requirement that a party assert an identical version of prior art to

15   sustain a finding of invalidity; (2) there is no functional difference between the combinations of

16   SWEEP-2.72 & InterCheck-2.11 and SWEEP-2.71 & InterCheck-2.01; and (3) it actually asserted

17   SWEEP-2.72 & InterCheck-2.01 in the Delaware case.

18   First, Sophos contends that it is irrelevant that it asserted a different combination of

19   SWEEP-InterCheck in the Delaware case than the combination asserted here because "all that is

20   required is that the prior art product be the same in both cases, not the particular version of the

21   product." Mot. for New Trial at 3. Sophos cites to *Leader Techs. v. Facebook, Inc.*, 678 F.3d

22   1300, 1307 (Fed. Cir. 2012), in which the Federal Circuit upheld an invalidity verdict based on

23   evidence presented of a post-critical date version of the asserted prior art software reasoning that

24   the patentee failed "to point to any contemporaneous evidence in the record that indicates that [a

25   prior version] was substantively different from the post-critical date software." Sophos seems to

26   argue that *Leader Technologies* establishes a legal rule that all versions of software are

27   interchangeable for the purposes of prior art. But this argument is unsupported by the case: the

28   *Leader Technologies* court did not conclude that all versions of software are inherently

11

1   interchangeable as a matter of law, but that the relevant versions of software in that case were not

2   substantively different. *Id.* Indeed, the court acknowledged that "as a general matter a computer

3   scientist can easily modify and change software code and that two versions of the same software

4   product may function differently." *Id.* Whether two versions of software are identical or

5   interchangeable for the purposes of prior art is a factual issue, not a legal one. As the party

6   asserting collateral estoppel it is Sophos's burden to show that the combination of SWEEP-

7   InterCheck asserted in the Delaware case is interchangeable with the combination asserted here.

8   Sophos next addresses this exact issue, arguing that the version of SWEEP-InterCheck

9   asserted in the Delaware case is materially identical to the combination asserted here. Sophos

10   made this same argument in its motion for partial summary judgment, asserting that it was

11   "undisputed" that the combination of SWEEP-2.72 & InterCheck-2.11 is materially identical to all

12   other combinations of SWEEP-InterCheck. In my May 24 Order I responded to this argument as

13   follows:

> [C]ontrary to Sophos's repeated assertions, it is not undisputed that the various
> SWEEP-InterCheck combinations at issue in this case are materially identical. The
> only evidence identified by Sophos on this point – Dr. Cohen's report – says
> nothing about whether the different *combinations* of SWEEP-InterCheck are
> materially identical. Meanwhile, Finjan has presented evidence indicating that at
> least some of the SWEEP-InterCheck combinations are considerably different, in
> that certain of them – *including SWEEP-2.72 & InterCheck-2.11* – are in fact
> "incompatible . . .and would result in faulty operation." Jaeger Rpt. ¶ 185 (Kastens
> Decl. Ex. 38, Dkt. No. 143-40)

20   Sophos does not cite to any additional evidence demonstrating the similarity between the

21   combination of SWEEP-InterCheck asserted in the Delaware case and the one asserted here and

22   again relies exclusively on evidence that InterCheck 2.01 and 2.11 are substantively similar to

23   each other. As I concluded in my prior order, this evidence does not address the similarity

24   between the asserted *combinations.* Finjan has presented evidence that different combinations of

25   SWEEP-InterCheck, including the SWEEP-2.72 & InterCheck-2.11 combination may be

26   materially different from other asserted combinations. Jaeger Rpt. ¶ 185 (Kastens Decl. Ex. 38,

27   Dkt. No. 143-40). Sophos has not demonstrated that the combination of SWEEP-2.72 &

28

12

1   InterCheck-2.11 is materially identical to SWEEP-2.72 & InterCheck-2.01.

2   Finally, Sophos argues that SWEEP-2.72 & InterCheck-2.01, the combination asserted in

3   this case, was also asserted in the Delaware case. It points to a reference from the Delaware

4   court's JMOL order in which the court noted that "Mr. Klausner testified specifically as to which

5   release he used in his invalidity analysis, stating that he relied on SWEEP version 2.72 and

6   InterCheck version 2.11, as well as on InterCheck versions 2.01 and 2.10, which were earlier

7   versions of the program incorporated into version 2.11." *JMOL Order*, 2013 WL 5302560 at *17.

8   While this reference does suggest that Mr. Klausner considered the SWEEP-2.72 & InterCheck-

9   2.01 combination, the Delaware court's discussion indicates that Sophos did not rely on this

10   combination and instead relied exclusively on the SWEEP-2.72 & InterCheck-2.11 combination in

11   pursuing its invalidity defense. The court noted that "the specific prior art reference on which

12   Sophos and Websense rel[ied] [was] version 2.72 of Sweep and version 2.11 of Intercheck." *Id.* at

13   *14. It also explained that "Sophos notes that its citations to source code were to a single version

14   of SWEEP (version 2.72) and a single version of InterCheck (version 2.11), which were sold

15   together as a single software product." *Id.* at *17. Despite Sophos's argument that it relied on the

16   SWEEP-2.72 & InterCheck-2.01 combination in the Delaware case, the Delaware court's JMOL

17   Order indicates that, in fact, it relied exclusively on the SWEEP-2.72 & InterCheck-2.11

18   combination.

19   Sophos has failed to show that collateral estoppel should apply in this case. It did not rely

20   on the same combination of SWEEP-InterCheck in the Delaware case and has failed to present

21   evidence that the combination of SWEEP-2.72 & InterCheck-2.01 (asserted here) and the

22   combination of SWEEP-2.72 & InterCheck-2.11 (asserted in the Delaware case) are substantively

23   identical. As a result, Sophos has failed to demonstrate that this case involves identical factual

24   issues to the ones actually litigated in the Delaware action and collateral estoppel does not apply.

25   B.   **Clear and Convincing Evidence**

26   Sophos next argues that it is entitled to a new trial on invalidity because it proved, by clear

27   and convincing evidence, that its asserted SWEEP-InterCheck Art (1) was a single anticipatory

28   reference; (2) was publicly available in the United States before 1995; and (3) satisfied every

13

1   claim element of the asserted patents. As addressed below, Finjan presented evidence on all three

2   of these issues that would have given the jury a reasonable basis for declining to find invalidity.

1. Single Anticipatory Reference

4   Sophos argues that it proved by clear and convincing evidence that SWEEP-InterCheck is

5   a single prior art reference for anticipation purposes because Sophos witnesses testified that (1)

6   after InterCheck was released, it was provided with SWEEP at no extra charge; (2) although

7   SWEEP could work on its own, InterCheck was developed to work with SWEEP and could not

8   function as a separate product; and (3) SWEEP-InterCheck was a single product. Mot. for New

9   Trial at 15.

10   In response, Finjan asserts that there were substantial doubts that SWEEP-InterCheck was

11   a single product because it presented evidence that (1) the programs were developed and released

12   at different times; (2) had different source code repositories; (3) were distributed to customers on

13   separate disks; (4) and that SWEEP could work separately from InterCheck. Oppo. to New Trial

14   at 16 (Dkt. No. 16).

15   Although Sophos presented evidence in support of its claim that SWEEP-InterCheck was a

16   single product, Finjan provided sufficient evidence to raise doubts and give the jury a reasonable

17   basis to conclude that SWEEP-InterCheck was not a single product.

2. Available in the United States

19   Sophos next argues that it presented clear and convincing evidence that SWEEP-

20   InterCheck was available in the United States prior to November 8, 1995 because (1) Sophos's

21   witness Dr. Lammer testified that it was "impossible to imagine" that SWEEP-2.72 & InterCheck-

22   2.01 were not sent to the United States before that time; (2) it presented a 1993 press release that

23   announced a worldwide license between Sophos and the U.S.-based company Digital Equipment

24   Corporation; (3) it showed that the backups for the SWEEP-2.75 & InterCheck-2.01 programs

25   predate November 8, 1995; (4) it demonstrated that the server code for a 1994 version of SWEEP-

26   InterCheck includes a comment indicating that Dr. Lammer made an adjustment "for a U.S.

27   customer" indicating that SWEEP-InterCheck was being sent to the United States prior to 1995;

28   (5) it presented Sophos's Data Security Reference Guide from March of 1995, which indicated

14

1 that SWEEP-InterCheck was available for sale and listed Sophos's U.S. distributer for Sophos

2 products; (6) it presented evidence that Sophos took steps to promote its products in the United

3 States starting in March of 1995; and (7) it presented a contract showing that Sophos sold

4 SWEEP-InterCheck to the World Bank in Washington, D.C. in August, 1995 following

5 negotiations that likely began prior to June 1995. Mot. for New Trial at 15-18.

6   In response, Finjan argues that Sophos failed to present clear and convincing evidence on

7 this point because (1) not a single Sophos witness had actual knowledge of whether InterCheck

8 2.01 was actually sent to any U.S. customers; (2) Sophos did not have any sales or shipping record

9 evidencing sales of InterCheck 2.01 or shipments of InterCheck 2.01 to U.S.-based customers; and

10 (3) Dr. Lammer testified that the August 1995 contract with the World Bank only applied to later

11 versions of SWEEP-InterCheck and not to the asserted SWEEP-2.71 & InterCheck-2.01

12 combination. Oppo. to New Trial at 16-17.

13   Although Sophos presented a considerable amount of circumstantial evidence that

14 InterCheck 2.01 may have been used by customers in the United States prior to November 8,

15 1995, it did not present any direct testimony or direct evidence confirming this point. The jury

16 could have found the lack of sales and shipping records or Dr. Lammer's inability to remember

17 whether InterCheck 2.01 was actually mailed to any U.S. customers compelling. Further,

18 although Sophos presented a range of evidence showing that SWEEP-InterCheck was generally

19 available in the U.S. prior to November 8, 1995, it presented very little evidence on the availability

20 of version 2.01 of InterCheck specifically. Without specific corroborating evidence about this

21 particular version of InterCheck, the jury was asked to rely heavily on Dr. Lammer's somewhat

22 speculative testimony that it was "impossible to imagine" that InterCheck 2.01 was not mailed to

23 any U.S. customers. As the Federal Circuit has held, "uncorroborated oral testimony, particularly

24 that of interested persons recalling long-past events," is not clear and convincing evidence.

25 *Woodland Trust v. Flowertree Nursery, Inc.*, 148 F.3d 1368, 1369, 1371-73 (Fed. Cir. 1998).

26 Given the uncertainty of Dr. Lammer's testimony and the lack of direct evidence that InterCheck

27 2.01 was sent to any U.S. customers, the jury had a reasonable basis to conclude that Sophos's

28 asserted combination of SWEEP-InterCheck was not publically available in the United States

15

1   prior to November 8, 1995.

2   **3. Anticipation**

3   Finally, Sophos argues that it presented clear and convincing evidence that SWEEP-

4   InterCheck meets every claim element of the asserted patents and directs the court to various

5   excerpts of trial testimony from its invalidity expert, Dr. Cohen who opined that SWEEP-

6   InterCheck anticipated each of the prior patents. Mot. for New Trial at 18.

7   In response, Finjan explains, at length, that there were numerous ways that Sophos failed

8   to show that SWEEP-InterCheck meets the various claim elements. Finjan notes that it presented

9   evidence that: (1) SWEEP-InterCheck did not meet the '844 patent's "generating" element

10   because the technology was limited to byte-matching to identify known viruses and could not

11   broadly identify suspicious code and did not meet the '844 patent's "linking" requirement because

12   the "linking" does not occur before a web server makes the Downloadable available to web

13   clients; (2) SWEEP-InterCheck did not satisfy various elements of the '494 patent including the

14   "downloadable scanner" limitation (because the source code Dr. Cohen introduced did not include

15   a list of suspicious operations) and the "database manager" limitation (because Dr. Cohen did not

16   show that the hash table he presented included a schema); (3) SWEEP-InterCheck did not satisfy

17   the '926 patent's "receiving an incoming Downloadable" limitation (because SWEEP searches for

18   known viruses) and the '926 patent's "transmit an incoming Downloadable" limitation (because

19   InterCheck forwards unknown files to the SWEEP server, which never sends them back to

20   InterCheck); (4) SWEEP-InterCheck did not meet the '780 patent's "communications engine that

21   obtains Downloadables" limitation (because SWEEP-InterCheck only scans local file systems, not

22   Downloadables from the Internet, and did not have the ability to fetch software components); and,

23   finally, (5) SWEEP-InterCheck did not satisfy the '154 patent's "dynamically-generated malicious

24   content" element (because SWEEP-InterCheck only checks for known viruses).

25   In its reply, Sophos engages these issues more deeply. It attempts to rebut each of Finjan's

26   arguments by explaining that SWEEP-InterCheck either does meet each element that Finjan

27   describes, and/or that the claim elements do not require the specific details that Finjan claims

28   Sophos failed to show. Reply for New Trial at 9-12.

16

1   This case involved complex patents and technologies. Substantial evidence regarding the

2   issue of invalidity was presented by both sides. The parties dispute both what the patent claims

3   required and what SWEEP-InterCheck actually does. While Sophos presented expert testimony

4   and evidence asserting that SWEEP-InterCheck anticipated all five of the asserted patents, Finjan

5   presented conflicting expert testimony asserting that SWEEP-InterCheck failed to meet a number

6   of necessary elements of each patent. Sophos, unsurprisingly, asserts that Finjan's evidence was

7   meritless and that Sophos's evidence should have been credited instead. But there is no

8   reasonable dispute that Finjan presented sufficient evidence on the issues of invalidity to provide

9   the jury with a reasonable basis to conclude that SWEEP-InterCheck did not anticipate the '844,

10   '494, '926, '780, and '154 patents.

11   There was a reasonable basis for the jury to conclude (1) that SWEEP and InterCheck were

12   not a single product; (2) that the elected combination of SWEEP-2.72 & InterCheck-2.01 was not

13   publicly available in the United States prior to November 8, 1995; and (3) that SWEEP-

14   InterCheck did not meet each and every element of the asserted patents. Each of these issues

15   provided the jury an independent basis to conclude that SWEEP-2.72 & InterCheck-2.01 did not

16   anticipate the asserted patents. Because the jury's verdict on invalidity was supported by

17   substantial evidence, its verdict was not against the clear weight of the evidence. Sophos is not

18   entitled to a new trial on invalidity on this basis.

19   **C. Use of Post-Grant proceedings**

20   Sophos argues that it is entitled to a new trial on invalidity because Finjan violated an *in*

21   *limine* ruling excluding evidence on post-grant proceedings before the patent office. Mot. for New

22   Trial at 19. Prior to trial Sophos moved to preclude Finjan from presenting "evidence or argument

23   about post-grant proceedings before the United States Patent & Trademark Office." Dkt. 217 at

24   19. I granted the motion and ruled that the parties could not produce any evidence related to post-

25   grant proceedings explaining "it would take a significant amount of time and effort to adequately

26   explain the relevance and limitations of the PTO proceedings to the jury and because I believe

27   there is a substantial risk that the jury will improperly substitute its own judgment for the PTO

28   decisions." Dkt. No. 291 at 25.

1   At trial, in attempting to show that SWEEP-InterCheck was considered by the patent

2 office, Finjan briefly displayed two slides that were excerpts from the prosecution history of the

3 '844 patent reexamination filed by a different company, Proofpoint, and asked Dr. Cohen four to

4 five questions related to whether the patent office considered the SWEEP-InterCheck product.

5 Trial Tr. at 1471:15-1473:2. Sophos contends that this was an intentional violation of the *in*

6 *limine* order. Finjan responds that Sophos had "opened the door" to evidence related to the post-

7 grant proceedings by stating in its opening statement that "The Patent Office did not know about

8 the software code that you're going to see and the demonstrations that you're going to see of how

9 our product operated before their system, before their patents were filed." Trial Tr. at 137:24-

10 138:5.

11   As I stated during trial outside the presence of the jury, Finjan's line of questioning on this

12 issue and display of the reexamination slides, without giving prior notice to Sophos or the court,

13 was improper. Finjan "stepped over [the] line" established by the *in limine* ruling on this issue.

14 *Id.* at 1532:16-20. Although Sophos requested that I instruct the jury that "there's been no

15 evidence that the Patent Office considered the SWEEP-InterCheck Product," I instead issued the

16 following instruction: "The parties dispute the extent to which SWEEP and InterCheck was

17 considered by the Patent and Trademark Office before some of the patents were issued, if at all.

18 And you should not consider the questions asked on this subject yesterday of Dr. Cohen, his

19 responses, or any documents that were shown during his testimony related to that." *Id.* at 1579:4-

20 9. Then, when the issue came up regarding what statements could be made during closing

21 arguments, I stated that "we would say nothing - - well, nothing would be said with respect to the

22 PTO, and [Sophos] couldn't make an argument that no evidence has been shown." *Id.* at 1643:3-

23 5. Similarly, I said that "Finjan may not use [the lack of evidence on the PTO] as a shortcoming

24 in [Sophos's] opening or the evidence." *Id.* at 1644:17-18. Sophos argues that "[t]he net effect of

25 Finjan's intentional violation of the Court's *in limine* order was to discredit a key theme of

26 Sophos's defense—that the jury was the first to consider the SWEEP-InterCheck source code and

27 demonstrations in determining the validity of Finjan's patents." Mot. for New Trial at 21.

28   Sophos's inability to rely on the lack of evidence presented with regards to the PTO

1   proceedings was a consequence of its successful motion *in limine*. Sophos wanted an instruction

2   from the court, or alternatively to make the argument itself, that there had been no evidence that

3   SWEEP-InterCheck was considered by the patent office. But as Finjan attempted to show with its

4   slides from the '844 patent reexamination, SWEEP-InterCheck was submitted to the patent office

5   as prior art. The parties therefore disputed whether the patent office "considered" this evidence,

6   but all of Finjan's potential evidence on the issue was excluded by the *in limine* ruling. Allowing

7   Sophos to argue that there was no evidence that the patent office considered SWEEP-InterCheck

8   would have been unfair and prejudicial to Finjan, since this was only true because Sophos

9   successfully moved to exclude that evidence.

10   Sophos explained to the court that it sought its *in limine* ruling and made its opening

11 argument because it *knew* that "Under the reexam, under the initial thing, the SWEEP-InterCheck

12 product was not considered [by the PTO]." Trial Tr. at 1539: 12-14. If Sophos was confident in

13 its evidence on this issue, and intended to rely on this fact for a major theme of its case, it should

14 have attempted to resolve the issue on summary judgment or in some other format – not through a

15 motion *in limine*. *Id.* at 1644:4-6. Instead of attempting to definitively resolve this fact issue in its

16 favor in advance of trial, Sophos successfully moved to exclude all of Finjan's potential evidence

17 on the issue. Then, because none of Finjan's evidence disputing Sophos's position would be

18 admissible, it planned to make the argument at trial that no evidence was presented that the patent

19 office considered SWEEP-InterCheck. While Sophos was not able to follow through with its

20 theme that the jury was the first to consider the SWEEP-InterCheck source code and

21 demonstration, this result was largely a self-created issue resulting from Sophos's strategic

22 maneuvering.

23   Although Finjan overstepped by displaying evidence related to the '844 patent

24 reexamination proceedings, this error was addressed with an instruction that the jury was not to

25 consider any evidence or testimony related to whether the PTO office considered SWEEP-

26 InterCheck. My ruling prevented Sophos from emphasizing in its closing that the jury was the

27 first to consider the SWEEP-InterCheck source code and demonstration; it did not prevent the jury

28 from actually considering the SWEEP-InterCheck source code and demonstration and assessing

19

1   the evidence on the merits. Because the only prejudice Sophos identifies is that it was not able to

2   carry-through on one of its themes, and because this issue arose predominantly as the result of

3   Sophos's own choices and trial strategy, Finjan's use of the post-grant proceedings evidence did

4   not result in a miscarriage of justice and does not justify a new trial on the issue of invalidity.

5   **II. NEW TRIAL ON INFRINGEMENT**

6   Sophos argues that it is entitled to a new trial on the issue of infringement because the

7   jury's verdict was against the great weight of the evidence. It incorporates by reference its Motion

8   for Judgment as a Matter of Law ("JMOL"). Mot. for New Trial at 21. For the reasons set forth

9   in my discussion of Sophos's JMOL motion, there was a reasonable basis for the jury's verdict on

10   infringement and Sophos is not entitled to a new trial on this basis.

11   **III. REMITTITUR**

12   Sophos asserts that it is entitled to a remittitur because Finjan improperly included revenue

13   related to SophosLabs in its royalty base, a service that Sophos asserts earns no revenue and

14   operates entirely outside the United States. Mot. for New Trial at 21. It is undisputed that

15   SophosLabs is not a separate product and does not generate separate revenue for Sophos. Trial Tr.

16   at 1076:2-7; 1077:4-20. Sophos contends that any indirect value for SophosLabs is captured by

17   the revenue for Sophos's UTM and Endpoint products and so the inclusion of additional proxy

18   revenue for SophosLabs was improper. Mot. for New Trial at 22.

19   At trial, Finjan's damages expert, Dr. Layne-Farrar testified that, although SophosLabs

20   does not generate revenue, it still provides value to Sophos by enhancing all of Sophos's products

21   and so its value should be captured in some way in a reasonable royalty analysis. Oppo. to New

22   Trial at 21. Layne-Farrar used a proxy to capture SophosLabs's value: she multiplied the number

23   of Endpoint Users that had enabled Sophos Live Protection, the infringing technology of

24   SophosLabs, by the price Sophos charged for the Live Protection technology. *Id.* at 21. Sophos

25   asserts that this value is already included in the Endpoint revenues and so the additional value

26   attributable to SophosLabs is duplicative and unsupported by evidence.

27   There is a strong argument that the value that SophosLabs adds to Endpoint and the UTM

28   was already captured by the Endpoint and UTM revenues. However, Layne-Farrar testified that

1   her understanding, based on the expert opinions of Finjan's technical experts, was that

2   SophosLabs adds value to all Sophos products. Trial Tr. at 833:1-7. There is no reason that the

3   Endpoint and UTM revenues would account for the value that SophosLabs adds to Sophos's other

4   products. Nevertheless, even if Sophos is correct, and the value of SophosLabs is fully captured

5   by the Endpoint and UTM revenues, I cannot conclude that the jury's verdict improperly

6   incorporated SophosLabs revenues.

7   It is unclear how the jury calculated its award and whether it factored SophosLabs

8   revenues into its damages calculation. The jury was not required to outline its method of

9   calculating the award on the verdict form and simply indicated that it was awarding damages of

10   $15 million for the life of the asserted patents. Sophos argues that the jury must have attributed

11   revenue to SophosLabs because the jury's verdict was greater than Layne-Farrar's damage

12   calculation without SophosLabs. Mot. for New Trial at 22. Layne-Farrar opined that Finjan was

13   entitled to a total reasonable royalty of $8.7 to $16.1 million composed of (1) $1.7-$2.2 million for

14   the UTM products; (2) $5.1-$10.2 million for the Endpoint products; and (3) $1.9-$3.7 million for

15   the SophosLabs product. Trial Tr. 842:14-843:24. Sophos argues that Layne-Farrar's maximum

16   royalty without SophosLabs would only be $12.4 million so the jury's award of $15 million must

17   have included SophosLabs revenues.

18   There are two primary problems with Sophos's argument. First, Sophos mischaracterizes

19   Layne-Farrar's $16.1 million figure ($12.4 without the SophosLabs revenues) as her maximum

20   royalty. At trial, Layne-Farrar repeatedly emphasized that her reasonable royalty opinion was a

21   conservative estimate and testified that she was "defining what the floor is for damages. My

22   reasonable royalty number should be the bottom line." *Id.* at 833:22-24. Layne-Farrar explained

23   various ways that her calculations were conservative, including that her royalty calculation was

24   significantly less than amounts Finjan had received in particular licensing deals or from other jury

25   awards. *Id.* at 844:10-22. Layne-Farrar's testimony and opinion, and the underlying evidence on

26   which she relied, provided the jury with evidence to support a damage award above her

27   "maximum" royalty amounts and so could support a $15 million figure even excluding

28   SophosLabs revenues.

21

1   Second, it is not clear that the jury adopted Layne-Farrar's opinion. While the jury's $15

2 million award was within the range Layne-Farrar presented, it does not line up with any of her

3 precise figures. It is possible that the jury adopted a modified version of Layne-Farrar's analysis,

4 but it is also possible that they jury based its damage award on the fact evidence presented or the

5 expert testimony of Sophos's expert, Brian Napper. For example, the parties presented a

6 substantial amount of factual evidence on damages including evidence of Finjan's prior jury

7 verdicts and licenses involving the Asserted Patents. 213:13-20; 818:20-821:20; 844;18-19; TX-

8 152; TX-2491; TX-3051; TX-13; TX-3052. The jury could have used this licensing information

9 to determine what a hypothetical license between Sophos and Finjan would have looked like. Its

10 $15 million award is well within the range of Finjan's prior licensing agreements and jury awards,

11 which, on the high end, range from $39-$85 million.

12   *LaserDynmaics, Inc. v. Quanta Computer, Inc.*, which Sophos cites, does not support

13 remittitur or a new trial. 694 F.3d 51 (Fed. Cir. 2012). In *LaserDynamics*, the Federal Circuit

14 ordered a new trial on damages following a jury award of $8.5 million dollars. *Id.* at 78. The

15 evidence supporting the jury's verdict was the opinion of LaserDynamics' expert, who calculated

16 a $10.5 million royalty using a 6 percent royalty rate. *Id.* at 65. Because the Federal Circuit

17 concluded that the 6 percent royalty rate was "untethered from the patented technology at issue"

18 and because comparable licensing agreements were all for lump sums of no more than $1 million,

19 the court concluded that "[a] new trial is required because the jury's verdict was based on an

20 expert opinion that finds no support in the facts in the record."

21   In *LaserDynamics,* it was clear that the jury relied on LaserDynamics' expert's opinion to

22 support its verdict as no other evidence was presented that would have justified an $8.5 million

23 award, and the award far exceeded all of LaserDynamics' prior licensing agreements. Here it is

24 less clear how the jury calculated its award; whether it relied on part or all of Layne-Farrar's

25 opinion, or Napper's, or whether it calculated its royalty rate using only the fact evidence

26 presented. Since the jury could have calculated its award using Finjan's prior licensing

27 agreements as a reference, and because its $15 million award is well within the range of Finjan's

28 prior licensing agreements, I cannot conclude that the jury's verdict is not supported by substantial

1 | evidence. Sophos's request for a remittitur is DENIED.

2 | **MOTION TO AMEND JUDGMENT**

3 | **BACKGROUND**

4 | Finjan moves to amend the judgment, issue an injunction, and for pre- and post-judgment

5 | interest. Mot. to Amend (Dkt. No. 424). After a 10-day trial, a jury found Sophos liable for

6 | infringing five of Finjan's patents and awarded Finjan damages of $15 million for the life of the

7 | patents. Dkt. No. 398 at 4. Judgment was entered for "damages payable as a lump sum for the

8 | life of the asserted patents." Dkt. No. 407. Finjan argues that because the only Sophos revenue

9 | information, expert opinion, and argument presented to the jury went through December 22, 2017,

10 | the judgment should be amended to "correct the time period covered by the damages award from

11 | 'the life of the asserted patents' to ending on December 22, 2017." Mot. to Amend at 2. It asserts

12 | that if the judgment is amended, as it requests, the court should enjoin Sophos from infringing the

13 | '154 patent from December 22, 2017 through its expiration on December 12, 2025 to prevent

14 | irreparable harm to Finjan's core business activities, reputation, and goodwill. *Id.* at 2-3. Finally,

15 | it contends that it is entitled to pre-judgment interest at the prime rate and to post-judgment

16 | interest. *Id.* at 2.

17 | **LEGAL STANDARD**

18 | Federal Rule of Civil Procedure 59(e) permits amendment to a judgment. Fed. R. Civ. P.

19 | 59(e). "Since specific grounds for a motion to amend or alter are not listed in the rule, the district

20 | court enjoys considerable discretion in granting or denying the motion." *McDowell v. Calderon*,

21 | 197 F. 3d 1253, 1255 n.1 (9th Cir. 1999). However, amending a judgment is considered an

22 | "extraordinary remedy which should be used sparingly." *Allstate Ins. Co. v. Herron*, 634 F. 3d

23 | 1101, 1111 (9th Cir. 2011). "In general, there are four basic grounds upon which a Rule 59(e)

24 | motion may be granted: (1) if such motion is necessary to correct manifest errors of law or fact

25 | upon which the judgment rests; (2) if such motion is necessary to present newly discovered or

26 | previously unavailable evidence; (3) if such motion is necessary to prevent manifest injustice; or

27 | (4) if the amendment is justified by an intervening change in controlling law." *Id.* A district court

28 | may nevertheless amend a judgment in other circumstances if appropriate. *Id.*

23

DISCUSSION

I. MOTION TO AMEND JUDGMENT

Finjan contends that it is entitled to an amended judgment because it has not been fully compensated for Sophos's infringement of its patents. Mot to Amend at 9. It argues that this is clear because the jury's verdict, awarding $15 million for the life of the patents, is inconsistent with the evidence and expert opinions presented at trial. *Id.*

Prior to trial I issued an Order preventing Finjan's damage expert, Dr. Layne-Farrar, from presenting an opinion that projected Sophos's future revenues on infringing sales through December 12, 2025, the date of expiration for the '154 patent. *Id.* at 4. The evidence was excluded as overly speculative and unreliable because Layne-Farrar simply presumed steady sales without any reference or reliance on evidence regarding the future of the malware software market, Sophos's business position in the market, or other information that would support a conclusion of constant sales over a nearly ten-year period. Dkt. No. 250 at 7-8. The functional result of this ruling was that Finjan did not present an expert damage theory that accounted for sales beyond December 22, 2017. Mot. to Amend at 4.

Sophos's damages expert, Brian Napper, also did not present a damage theory that accounted for the full life of the patents. Napper presented two different reasonable royalty opinions, but both were limited to the two year period from the start of the litigation through trial. His first opinion was based on the "use" of the accused technology. He concluded that Sophos's accused SAV Engine blocked .6 percent of malware and so he applied a .6 percent royalty rate to Sophos's revenues for the two year period to calculate a royalty of $1.1 million. Trial Tr. at 1314:2-1315:4. For his second opinion, he used Finjan's prior licensing agreements to estimate what a Finjan-Sophos license would look like. *Id.* at 1279:15-24. He compared Sophos's relevant market share to that of Finjan's existing licensees and then adjusted Finjan's licensing agreements to reflect Sophos's relative size. *Id.* Finally, because Finjan's licenses are generally one-time lump sum agreements that run for 10-15 year periods, Napper adjusted his royalty calculation to limit it to the approximately two year period of the litigation and opined that approximately $2 million was appropriate for this shortened time period. *Id.* at 1302:4-1303:3.

24

1   Following the close of evidence the parties submitted their proposed verdict forms. At the

2 charging conference Finjan took issue with Sophos's inclusion of a "one-time payment for the life

3 of the patents" on the damages sheet, arguing that because "Napper was very clear that he actually

4 did not give an opinion for the life of the patents, that he only gave it up through either the March

5 or the September date . . . that particular question actually doesn't work as written because it's not

6 for the life of the patents." *Id.* at 1651:20-1652:2. In defending the inclusion of the "one-time

7 payment" option, Sophos contended that "there is also testimony in the record about Finjan's

8 licenses, the other licenses they have, that are for a lump sum, and so the jury could certainly

9 decide something else based on that testimony and evidence." *Id.* at 1652:13-17. After the parties

10 briefly conferred on this issue Finjan conceded that there might be facts that "[Sophos] can stitch

11 together, right. So I guess I wouldn't - - I wouldn't oppose it, if that's what they are going to be

12 doing." *Id.* at 1653:3-5.

13   During closing arguments, Finjan attempted to present a "summation" of the evidence that

14 offered a new theory for calculating damages for the life of the asserted patents: Finjan noted that

15 there are 3.9 million Sophos end users, that for a 24 month period these users are charged $21.60

16 per user, and that Finjan's technical expert, Dr. Medvidovic, had testified that a 50 percent

17 apportionment, based on the value-added of the accused technology, was appropriate for Sophos's

18 products. Finjan then proposed that the jury could multiply 3.9 million by .5($21.60) to get

19 $42.12 million. *Id.* at 1732:18-1733:21. Sophos objected because Finjan was presenting a new

20 theory not in the evidence. After a discussion at sidebar, I sustained the objection and Finjan was

21 not permitted to continue its argument on this issue. *Id.* at 171733:22-1738:7. Finjan's closing

22 argument was limited to discussing the damage theory its expert, Layne-Farrar presented, which

23 only went through December 22, 2017.

24   Finjan submits that because it was not permitted to present evidence, expert opinion, or

25 argument about a reasonable royalty through the life of the patents, the jury verdict and judgment,

26 which purport to award damages through the life of the Asserted Patents, are inconsistent with the

27 evidence and that Finjan has not been awarded a reasonable royalty as required by 35 U.S.C. §

28 284.

25

1   Although Finjan asserts that no evidence was presented on which the jury could have

2 based an award through the life of the patents, there was substantial evidence in the record to

3 support the jury's finding. Both parties presented evidence demonstrating that in a hypothetical

4 negotiation, Finjan and Sophos likely would have agreed to a one-time lump sum payment. For

5 example, Napper testified that "I think they would strike a one-time lump-sum payment" and

6 Layne-Farrar testified that "[Finjan's license agreements] were all lump sums." Trial Tr. at

7 1292:11-13; 874:4-875:9.

8   Both parties also presented evidence of Finjan's prior licensing agreements. Napper

9 discussed and analyzed these agreements in detail as part of one of his damage theories. *Id.* at

10 1279:15-24 (calculating an estimated royalty by adjusting Finjan's prior licensing agreements to

11 account for Sophos's size relative to Finjan's other licensees). He explained that he used the prior

12 licensing agreements to calculate what a hypothetical Finjan-Sophos licensing agreement would

13 look like, but, because actual Finjan licensing agreements are lump sum agreements that cover 10-

14 15 year periods, at the very end of his analysis he adjusted his final royalty calculation to represent

15 a payment for a two-year period only (as Sophos had only asked him to calculate a royalty for the

16 two year duration of the litigation). *Id.* at 1302:4-1303:3.

17   Based on this testimony, and the underlying evidence, the jury easily could have calculated

18 an appropriate one-time lump sum payment by working backwards from Napper's two-year

19 royalty amount to calculate an appropriate royalty for a 15-year, lump sum licensing agreement.

20 Because Napper testified that a $2 million royalty was reasonable for a two-year span, under

21 Napper's analysis, $15 million would be a reasonable royalty for a 15 year span. The jury's lump

22 sum award of $15 million is entirely consistent with Napper's opinion and is well supported by the

23 evidence in the record.

24   Finjan cites three cases to support its claim that it has not been compensated for future

25 damages. None of these cases support Finjan's position. First, it cites to *Finjan, Inc. v. Secure*

26 *Computing Corp.*, 626 F.3d 1197, 1213 (Fed. Cir. 2010), in which the Federal Circuit stated that a

27 "patentee is not fully compensated if the damages award did not include future lost sales." The

28 *Secure Computing* court concluded that Finjan was entitled to additional damages based on future

26

1   sales that the jury did not consider. *Id.* However, *Secure Computing* is easily distinguishable

2   because in that case the verdict form required the jury to list a royalty rate, royalty base, and total

3   royalty amount, so it was clear from the verdict form both how the jury calculated its award and

4   that the jury did not include future sales in its calculation. *Id.* at 1209. In contrast, in this case the

5   verdict form did not require the jury to select a particular royalty base or royalty rate, did not

6   require the jury to calculate its award by multiplying a royalty rate by a royalty base, and did not

7   require the jury to show how it calculated its award. As a result, it is rank speculation to conclude

8   that the jury did not include future sales in its analysis. The jury could have projected future sales

9   and included those in a royalty base, or it could have calculated its award without using a royalty

10   base at all, for example, by calculating a single lump sum payment based on Finjan's past

11   licensing agreements. *Secure Computing* does not support amending the judgment.

12   *Whiteserve, LLC v. Computer Packages, Incorporated*, 694 F.3d 10 (Fed. Cir. 2012) and

13   *Telcordia Technologies Incorporated v. Cisco Systems Incorporated* , 612 F.3d 1365 (Fed. Cir.

14   2010) are similarly not analogous. In *Whiteserve*, the Federal Circuit concluded that the jury had

15   not awarded a fully paid-up license where the jury did not indicate on its verdict form that its

16   award was meant to cover future damages and the trial court interpreted the jury's award as not

17   covering future damages. *Whiteserve*, 694 F.3d at 35. Likewise, in *Telcordia*, it was "unclear

18   whether the jury compensated Telcordia only for Cisco's past infringement or for both past and

19   ongoing infringement" as the verdict form only asked the jury to "identify the amount of monetary

20   damages that will compensate Telcordia for Cisco's infringement" and the jury did not indicate

21   anything other than an amount of $6,500,000. *Telcordia*, 612 F.3d at 1377-78. As a result, the

22   Federal Circuit concluded that the district court did not abuse its discretion by concluding that the

23   award was only for past infringement. *Id.* at 1378.

24   In contrast, here the jury was instructed that it could award damages through September,

25   2016, through December, 2017, or for the life of the patents. Faced with these choices the jury

26   deliberately chose to award damages for the life of the patents and indicated so on the verdict

27   form. While the intent of the juries in *Whiteserve* and *Telcordia* was ambiguous, here there is no

28   reasonable dispute that the jury intended to award a lump sum payment for the life of the patents.

27

1   Because the jury's intention to award Finjan a lump sum fee for the entire life of the

2   patents is clear from the face of the verdict form, and because the jury's award is supported by

3   substantial evidence in the record, the "extraordinary remedy" of an amended judgment is not

4   appropriate. *Allstate*, 634 F. 3d at 111. Finjan's motion to amend the judgment is DENIED.

5   **II. INJUNCTION**

6   Finjan asks, contingent on its requested amendment to the judgment, that the court enjoin

7   Sophos from infringing the '154 patent from December 22, 2017 through its expiration on

8   December 12, 2025. Mot. to Amend at 13. Because an injunction would only be possible if the

9   judgment were amended, and because, as discussed above, amendment is not appropriate in this

10 case, Finjan's request for an injunction is DENIED.

11 **III. PRE- & POST-JUDGMENT INTEREST**

12   A.   **Pre-Judgment Interest**

13   Under 35 U.S.C. § 284, "[u]pon finding for the claimant the court shall award the claimant

14 damages adequate to compensate for the infringement . . . together with interest and costs as fixed

15 by the court." Awarding prejudgment interest to a prevailing patentee is "the rule, not the

16 exception." *Crystal Semiconductor Corp. v. TriTech Microelectronics Int'l, Inc.*, 246 F.3d 1336,

17 1361 (Fed. Cir. 2001). "[P]rejudgment interest should be awarded under [35 U.S.C.] § 284 absent

18 some justification for withholding such an award." *Gen. Motors Corp. v. Devex Corp.*, 461 U.S.

19 648, 657 (1983).

20   District courts have discretion to determine the rate of prejudgment interest. *Uniroyal, Inc.*

21 *v. Rudkin-Wiley Corp.*, 939 F.2d 1540, 1545 (Fed. Cir. 1991). Courts often award interest at the

22 prime rate "where there is evidence that the plaintiff would have been spared from borrowing

23 money at the prime rate during the infringement period had the infringer been paying royalties,

24 and thus, prejudgment interest is necessary to compensate for 'the forgone use of the money.' "

25 *Finjan, Inc. v. Blue Coat Sys., Inc.*, No. 13-cv-03999-BLF, 2016 WL 3880774, at *18 (Aug. 22,

26 2016). Courts have declined to use the prime rate where the plaintiff does "not present any

27 evidence that it needed to borrow money *because* it was deprived of the damages award." *Apple,*

28 *Inc. v. Samsung Elecs. Co., Ltd.*, 67 F. Supp. 3d 1100, 1122 (N.D. Cal. 2014) (emphasis in

original); *Laitram Corp. v. NEC Corp.*, 115 F.3d 947, 955 (Fed. Cir. 1997) (finding the prime rate may not be appropriate if there is no "causal connection between any borrowing and the loss of the use of money awarded as a result of [] infringement").

Sophos argues that Finjan is not entitled to any prejudgment interest because it unduly delayed in bringing its suit. *Gen. Motors Corp. v. Devex Corp.*, 461 U.S. 648, 655 (1983) (prejudgment interest may not be appropriate where the plaintiff unduly delayed in prosecuting the case). Sophos suggests that because Finjan previously brought suit against Sophos in 2010 for similar patents and products, "Finjan necessarily was aware of a possible claim for infringement as to four of the asserted patents by 2010." Oppo. to Mot. to Amend at 20 (Dkt. No. 441). Finjan responds that this claim of delay is not based on any evidence or facts and asserts that it did not know of Sophos's infringement until October or November of 2013. It filed suit against Sophos only a few months later. Caire Decl. Ex. 4 (Dkt. No. 445-5). Since Sophos's argument that Finjan delayed in bringing suit is based on speculation and Finjan has presented evidence that it brought suit with due diligence, I cannot conclude that Finjan unduly delayed in bringing suit. Finjan is entitled to prejudgment interest.

Next I must decide how prejudgment interest will be calculated. Finjan argues that it is entitled to prejudgment interest at the prime rate because it entered into financing deals during the period of Sophos's infringement at rates above the prime rate. Mot. to Amend at 22. Finjan notes that, in particular, on May 6, 2016, it secured $10.2 million in a round of Series A investment financing at a rate higher than the prime rate. *See* Harstein Decl. ¶ 8, Ex. 3 (Dkt. No. 422-4); Mot. to Amend at 23. In his declaration, Harstein claims that Finjan was required to obtain this financing at unfavorable terms as a result of Sophos's failure to pay a royalty and as a result of expenses incurred in bringing the action against Sophos to enforce Finjan's patent rights. Harstein Decl. ¶ 7-8.

Sophos contends that Finjan has failed to show that it needed to obtain unfavorable financing as a result of Sophos's infringement, Oppo. to Mot. to Amend at 21. It notes that Finjan does not indicate whether more favorable financing options were available to it, such as lines of credit, bank loans, or rejected settlement offers. It also challenges the assertion that Finjan's need

29

1 for financing is the result of litigation costs incurred in its suit against Sophos. Sophos notes that

2 Finjan has chosen to simultaneously sue a number of entities, has fought to lift stays in other cases

3 thereby incurring immediate litigation costs that could have been postponed, and brought a second

4 suit against Blue Coat before recovering its substantial judgment against that entity. *Id.* at 21-22.

5 Sophos notes that Finjan has secured tens of millions of dollars in verdicts and licensing

6 agreements during the two years of this litigation and argues that it is unlikely that Finjan's case

7 against Sophos specifically put it into a position that required it to borrow money. *Id.* at 22.

8 Accordingly, Sophos submits that the treasury rate should apply to any interest.

9 Finjan has failed to demonstrate that Sophos's infringement required it to borrow money at

10 the prime rate. The treasury rate is appropriate. Finjan's request for prejudgment interest is

11 GRANTED. Prejudgment interest will be calculated at the treasury rate compounded annually.

12 B. **Post-Judgment Interest**

13 Finjan asserts that it is entitled to post-judgment interest, calculated using the "weekly

14 average 1-year constant maturity Treasury yield . . . compounded annually" pursuant to 28 U.S.C.

15 § 1961. Sophos does not dispute that Finjan is entitled to post-judgment interest. Finjan's request

16 for post-judgment interest is GRANTED and will be awarded at the treasury rate compounded

17 annually.

18 **RENEWED MOTION FOR JUDGMENT AS A MATTER OF LAW**

19 **BACKGROUND**

20 At the close of Finjan's infringement case, Sophos moved for judgment as a matter of law

21 under Federal Rule of Civil Procedure 50(b). Sophos now renews its motion, arguing that the

22 jury's verdict, finding that Sophos infringed all five of Finjan's asserted patents, is not supported

23 by substantial evidence. For the reasons outlined below, Sophos's motion is DENIED.

24 **LEGAL STANDARD**

25 A court should grant a motion for judgment as a matter of law following a jury trial where

26 "the evidence, construed in the light most favorable to the nonmoving party, permits only one

27 reasonable conclusion, and that conclusion is contrary to that of the jury." *InTouch Techs., Inc. v.*

28 *VGO Commc'ns, Inc.*, 751 F.3d 1327, 1338 (Fed. Cir. 2014). "[T]o set aside the verdict, there

1 must be an absence of substantial evidence—meaning relevant evidence that a reasonable mind

2 would accept as adequate to support a conclusion—to support the jury's verdict." *Emblaze Ltd. v.*

3 *Apple Inc.*, No. 11-c-01079-PSG, 2015 WL 396010, at *3 (N.D. Cal. Jan. 29, 2015).

4 **DISCUSSION**

5 I. **THERE WAS SUBSTANTIAL EVIDENCE THAT SOPHOS PRACTICED METHOD CLAIMS IN THE UNITED STATES**

6

7 Sophos claims that judgment as a matter of law is warranted for Finjan's method claims

8 because Finjan did not present any evidence that Sophos practiced each step of the asserted

method claims in the United States.

9

10 A. **Finjan was required to show Sophos performed every step of the method claims**

11 First, the parties dispute whether the law requires Finjan to show that Sophos itself

12 practiced every step of Finjan's method claims, or whether Finjan may rely on evidence that

13 Sophos's customers practiced the elements of the method claims. Sophos contends that "to

14 infringe a method claim, a person must have practiced all steps of the claimed method." *Secure*

15 *Computing*, 626 F.3d at 1206; *see also Ericsson, Inc. v. D-Link Sys., Inc.*, 773 F.3d 1201, 1221

16 (Fed. Cir. 2014) ("the direct infringer must *actually* perform the steps in the method claim")

17 (emphasis in original); *France Telecom S.A. v. Marvell Semiconductor Inc.* 82 F. Supp. 3d 987,

18 993 (N.D. Cal. 2015) ("A defendant can only directly infringe a method claim . . . by 'using' the

19 method within the United States, which requires that the defendant practice every step of the

20 method within the United States").

21 Finjan responds that, under the Federal Circuit's recent decision in *Akami Techs., Inc. v.*

22 *Limelight Networks, Inc.*, 797 F.3d 1020 (Fed. Cir. 2015), it can sustain its method claims against

23 Sophos by showing vicarious use of the method steps by Sophos's customers. Oppo. to JMOL at

24 4 (Dkt. No. 440). In *Akami IV*, the Federal Circuit held that a party that does not personally

25 perform all elements of a method claim may still be held liable for direct infringement of those

26 claims if the "alleged infringer conditions participation in an activity or receipt of a benefit upon

27 performance of a step or steps of a patented method and establishes the manner or timing of that

28 performance." 797 F.3d at 1023. Finjan argues that because Sophos's products perform all of the

31

1   steps of the method claims, "Sophos conditioned the ability of its customers to receive the benefit

2   of the UTM and Endpoint Products upon their use of these products in the infringing manner."

3   Oppo. to JMOL at 2.

4   Finjan misapplies the *Akami IV* court's divided infringement ruling to this case. As the

5   *Akami IV* court explained, its divided infringement analysis applies "[w]here more than one actor

6   is involved in practicing the steps" of the asserted method claim. *Akami IV*, 797 F.3d at 1022.

7   This is not a divided infringement case. Finjan asserts that a single actor satisfies all of the steps

8   of the method claims by operating Sophos's UTM and Endpoint products. Finjan is attempting to

9   show direct infringement by demonstrating that Sophos's customers perform *all* of the steps of the

10   method claims: this is an indirect infringement claim, not a divided direct infringement claim, and

11   *Akami IV* does not apply to these facts. Because *Akami IV* does not apply, and because Finjan

12   voluntarily dismissed its indirect infringement claims, Finjan was required to show that Sophos

13   itself performed all of the steps of the method claims.

14   B.   **There was Substantial Evidence that Sophos Personally Performed the Steps
                of the Method Claims**

15   Finjan presented substantial evidence that Sophos performed every step of Finjan's method

16   claims in the United States. First, Finjan presented overwhelming evidence demonstrating that

17   operating the UTM and Endpoint products satisfies each and every method of the method claims.

18   Trial Tr. 330:11-334:12; 386:12-21; TX-2173 at 1197SOPHOS_00407505. Sophos does not

19   dispute that use of its products meets every method of the method claims or that Finjan established

20   this fact at trial. Finjan also presented substantial evidence that Sophos is a Massachusetts

21   corporation with its principal place of business in the United States, that it sells its UTM and

22   Endpoint Products in the United States, and that these products have millions of users in the

23   United States. Trial Tr. at 116:13-15; Trial Tr. at 834:4-7, 834:11-835:19. These facts are

24   similarly, not disputed.

25   To establish that Sophos itself practices the method claims in the United States, Finjan

26   presented internal Sophos documents demonstrating that Sophos developed and performed

27   troubleshooting on its infringing products, in the United States. Finjan presented Trial Exhibit

28

                                                    32

1   120, a Sophos internal document of PowerPoint slides dated February 2010, which appears to

2   indicate that Sophos's SXL technology, which had previously been used on Sophos's OEM and

3   mail gateway products, will be implemented on Sophos's Endpoint products. TX-120 at

4   1197SOPHOS_01737110. To illustrate how this will impact the user interface in Endpoint, the

5   exhibit includes images of a Sophos employee changing the configuration in a "Sophos Endpoint

6   Security and Control" screen so that the Endpoint product will "automatically send field data, such

7   as checksums." TX-120 at 1197SOPHOS_01737097 (internal Sophos document showing screen

8   grabs of a user navigating a Sophos Endpoint Security and Control system).   The exhibit then

9   provides details on how to troubleshoot the implementation of the SXL on the Endpoint products.

10   TX-120 at 1197SOPHOS_01737115 ("Verify that SXL DNS lookups are working correctly within

11   the customer's environment"). It also shows examples of performing these troubleshooting steps

12   which show running SXL lookups on the "01" SXL server located in Miami. TX-120 at

13   1197SOPHOS_01737116. This document offers strong evidence that Sophos used its own

14   Endpoint products in the United States around February 2010 as it appears it must have used the

15   products to develop troubleshooting instructions and to prepare the document slides and images

16   seen in Exhibit 120.

17   Trial Exhibit 120 also provides evidence that Sophos used and tested its UTM product in

18   the United States. Trial Exhibit 120 shows Sophos employees running a program called

19   "Wireshark" on Sophos's "02" server located in Phoenix, Arizona. TX-120 at

20   1197SOPHOS_01737119. At trial, Finjan's expert Dr. Cole testified that Wireshark is a tool that

21   security professionals use to capture the information moving in and out of a computer system

22   during testing and that he personally used Wireshark to test the Sophos UTM product. Trial Tr.

23   380:16-381:20. He explained that he set up and used a Sophos UTM box at a facility in the

24   United States and that by using the Wireshark program in conjunction with the UTM he could see

25   how the UTM was working and that it was communicating with SXL servers in the United States.

26   *Id.*

27   Dr. Cole's testimony and Trial Exhibit 120 demonstrate that Sophos had the means and

28   tools to test its UTM products within the United States using the Wireshark program and that this

1   type of testing would have involved Sophos using the UTM product. Further, Trial Exhibit 120

2   establishes that Sophos employees tested how its SXL technology functioned on its Endpoint

3   product. Since the UTM also uses SXL technology, Trial Exhibit 120, offers substantial evidence

4   that Sophos would have run similar tests on the UTM products. Trial Exhibit 120 demonstrates

5   that Sophos tested and used its Endpoint and UTM products within the United States.

6   Sophos challenges the value of Trial Exhibit 120, noting that it is dated years before the

7   infringement period. To rebut the idea that Sophos may have stopped testing its products after

8   2010, Finjan presented Trial Exhibit 125, dated October 7, 2015, which shows that Sophos

9   continued to perform testing and troubleshooting on its products in 2015. TX-125. Similarly,

10   Finjan's evidence that Sophos is a Massachusetts company with millions of customers in the

11   United States supports the inference that Sophos would have continued to test and use its products

12   during this period as such testing would have been necessary to develop new features and

13   improvements, market and sell its products, and troubleshoot for existing customers.

14   Sophos also challenges the evidentiary weight of Exhibits 120 and 125 because they relate

15   primarily to testing of the SXL technology, which Sophos asserts is irrelevant to the Endpoint and

16   UTM products. But Finjan demonstrated that both Endpoint and the UTM use SXL technology

17   and communicate with the SXL servers as part of the Live Cloud or Sophos Cloud function of the

18   products. Trial Tr. 378:19-379:21 ("[B]oth the UTM and the Endpoint product do utilize the

19   Sophos Cloud in a similar manner. The UTM would receive a downloadable from the Internet.

20   And if it needed additional information, it would take a hash of that downloadable, and it would

21   go to the SXL server and do a lookup to say, is there any additional information from the cloud?").

22   Testing of the SXL technology would involve testing whether Sophos's products that use the Live

23   Cloud feature are properly communicating with the SXL servers and running SXL lookups.

24   Therefore SXL testing in the United States, especially in the context of Exhibit 120, offers

25   substantial evidence that Sophos would have tested and used its Endpoint and UTM products in

26   the United States.

27   Because Finjan presented overwhelming evidence that using Sophos's UTM and Endpoint

28   products infringes the method claims and substantial evidence that Sophos tested and used the

34

1   UTM and Endpoint products in the United States, there was substantial evidence to support the

2   jury's finding that Sophos directly infringed Finjan's method claims.

3   II.   **THERE WAS SUBSTANTIAL EVIDENCE THAT SOPHOS LIVE CLOUD INFRINGED THE ASSERTED SYSTEM CLAIMS**

4

5   Sophos asserts that Finjan has failed to show that Sophos's "Sophos Live Cloud" service

6   infringes the asserted patents because (1) it presented no evidence that Sophos Live Cloud actually

      exists and Sophos presented evidence that Sophos Live Cloud was not a real product; (2) and it
7
      failed to show that Sophos Live Cloud was used in or imported into the United States. Mot. for
8
      JMOL at 5-6 (Dkt. No. 421).
9
            A.   **Substantial Evidence Demonstrates that Sophos Live Cloud is Real**
10
           Finjan presented substantial evidence that the cloud service that it called "Sophos Live
11
      Cloud" at trial is a real service that runs on servers in the United States. Drs. Cole and
12
      Mitzenmacher testified that Sophos's "cloud" servers analyze, detect, and block against malicious
13
      code and are located in various locations around the United States. Trial Tr. at 329:19-21
14
      ("Sophos Live Cloud are servers out on the Cloud . . . it's just servers at an outsource facility that
15
      are accessible form the Internet); 548:17-20 ("Sophos Live Cloud consists of multiple
16
      components, multiple servers."). They explained that Sophos Live Cloud consists of the Sophos
17
      SXL Servers, Sample Servers, and the automation systems of LabRules and Warzone in
18
      SophosLabs, which all communicate and interact with each other. *Id.* at 329:6-331:14; 389:2-
19
      390:8; 548:15-549:4; 585:24-587:3; TX-2065; TX-2150; TX-2252.
20
           Although Sophos showed that the term "Sophos Live Cloud" is not one that Sophos uses
21
      internally and was adopted by Finjan's experts for the purposes of this litigation, it did not rebut
22
      Finjan's evidence that the servers and processes that Finjan has tried to encompass with the term
23
      "Sophos Live Cloud" are real. Indeed, two of Sophos's witnesses testified about the component
24
      servers that Finjan references when it uses the term "Sophos Live Cloud" and confirmed that they
25
      are real servers. Trial Tr. at 1079:5-1080:16; 1153:18-1154:15; 1161:8-1166:11. Finjan presented
26
      substantial evidence that the "Sophos Live Cloud" technology its experts described is not a fiction.
27

28

                                                   35

B.   **Substantial Evidence Demonstrates that Sophos Live Cloud was Used in the United States**

Finjan claims that it demonstrated that Sophos Live Cloud was "used" in the United States. Oppo. to JMOL at 10. At first look it is not entirely clear where Sophos Live Cloud is "used" as there are elements of the system located in the United States – where various Sophos servers are located and where U.S. customers operate UTM and Endpoint products – and in the United Kingdom – where "SophosLabs" is located. Finjan asserts that under *NTP, Inc. v. Research In Motion, Ltd.*, 418 F.3d 1282, 1317 (Fed. Cir. 2005), a patentee may prove direct infringement of a system claim for a multinational system – one with elements located in multiple countries – by showing that "the place at which the system as a whole is put into service, *i.e.* the place where control of the system is exercised and beneficial use of the system obtained" is within the United States.

Sophos argues that Finjan's reliance on *NTP* is improper because *NTP* only applies to indirect infringement claims. *NTP* was an indirect infringement case and the jury found that the defendant's customers, and not the defendant itself, directly infringed. *Id.* at 1317 n.13. But Sophos offers no explanation why the logic of *NTP* and the benefit-and-control factors would not apply equally to a direct infringement claim on a multinational system. The *NTP* holding directly undermines Sophos's position. To affirm the indirect infringement claims in *NTP,* the Federal Circuit necessarily found that one may directly infringe a system claim even when certain parts of the system are located outside the United States, so long as the system is controlled or benefits those in the United States. *Id.* (affirming the jury's finding that defendants' customers directly infringed the system claims). The only difference in a direct infringement claim is that a patentee must show that the defendant itself, rather than its customers, infringed the claim. There is no reason that the benefit-and-control factors of *NTP* do not apply to a direct infringement claim and Sophos offers no explanation. I conclude that *NTP* applies to direct infringement multinational system claims.

Sophos argues that, even if *NTP* applies, Finjan did not show that Sophos Live Cloud is controlled from the United States. Reply to JMOL at 7 (Dkt. No. 448). There is competing evidence on this point. Finjan's experts testified that the material components of Sophos Live

1   Cloud are located in the U.S., including the SXL Servers and Sample Servers. Trial Tr. at 382:1-

2   385:6; 548:17-549:4. Cole testified that Sophos Live Cloud is controlled by the UTM and

3   Endpoint products (many of which are located in the United States) because these products

4   generate requests that are sent to the Cloud servers and because the Sophos Live Cloud service

5   cannot do anything unless a UTM box or Endpoint product tells it what to do. Trial Tr. 389:2-

6   390:8. He also testified that the benefit of Sophos Live Cloud runs to the United States because

7   "the company or person sitting behind [a] UTM in the U.S. receives the direct benefit of that

8   service" because "it allow[s] [a] system to be protected and [the] system not to get infected by

9   malware." *Id.* at 390:23-391:4. In opposition, Sophos presented evidence that Sophos Live Cloud

10 is controlled from the United Kingdom because file submissions via Sophos Live Cloud cannot

11 happen unless SophosLabs creates a "wanted poster" for malware samples, thereby requesting

12 submissions from users' UTM or Endpoint products. Trial Tr. at 1161:8-1166:11.

13   In short, the parties both presented plausible evidence as to where Sophos Live Cloud is

14 controlled: Finjan presented evidence that the system cannot work if it does not receive requests

15 from UTM and Endpoint products, which may be located in the United States, and Sophos

16 produced evidence showing that the UTM and Endpoint products do not send any files to the

17 Sophos Live Cloud unless SophosLabs, in the UK, has requested specific types of files. This was

18 a close factual issue but there was substantial evidence to support the jury's conclusion that

19 Sophos Live Cloud is controlled from and benefits those in the United States.

20   Finally, Sophos argues that even if the benefits and control standard applies, Finjan has

21 failed to prove direct infringement because it only presented evidence that customers used and

22 directed the processes of Sophos Live Cloud from the United States but did not present any

23 evidence that Sophos itself benefitted from or directed the use of Sophos Live Cloud. Reply to

24 JMOL at 7. For the reasons outlined above in Section I.B, Finjan has presented substantial

25 evidence that Sophos used and tested its own products in the United States. As Finjan presented

26 evidence that use of the UTM and Endpoint products controls Sophos Live Cloud, and leads to the

27 benefit of Sophos Live Cloud being felt in the United States, there is substantial evidence on

28 which the jury could have concluded that Sophos benefitted from and controlled Sophos Live

37

Cloud from the United States.

III. **FINJAN PRESENTED SUBSTANTIAL EVIDENCE THAT SOPHOS'S PRODUCTS SATISFY EVERY LIMITATION OF EACH ASSERTED CLAIM**

A. **The '844 Patent**

Sophos asserts that Finjan failed to demonstrate that its accused products perform the "linking" element of the '844 patent, which requires "linking by the inspector the first Downloadable security profile to the Downloadable before a Web server makes the Downloadable available to Web clients." Mot. for JMOL at 7. Sophos does not dispute that its products perform a linking function, but claims that this does not happen "before a Web server makes the Downloadable available to Web clients" because the accused products are themselves web clients and so can only perform the necessary linking after the Downloadable has been made available to them. *Id.* It also argues that web servers like CNN.com make Downloadables available to web clients as soon as they place the Downloadables on their servers and, since Sophos's products can only inspect Downloadables that have been made available to the general public, they do not perform the linking function until after the Downloadables have been made available to web clients in the general public.

Finjan asserts that Sophos is relying on an overly broad interpretation of the term "web client." It submits that a "web client" within the meaning of the patent is an end user that is actually using a Sophos product or other inspector device. The term is not meant to include all computers, such as an inspector computer or computers in the general public not employing a malware security system. It contends that the relevant question is whether Sophos's products perform the linking element before making the Downloadable available to end users actually using Sophos's products, not whether any user anywhere is able to access the Downloadable before Sophos's product performs the linking function.

Both of Sophos's arguments rest on a broad interpretation of "web client" that the jury reasonably could have rejected in favor of Finjan's position that Sophos's products act as the "inspector," not a web client, and that "web client" refers only to computers using Sophos's products or similar inspector devices. As there is no dispute that Sophos's products perform this

38

1   linking function, the jury's finding that Sophos's accused products meet the linking element of the

2   '844 Patent is supported by substantial evidence.

3   B.   **The '926 Patent**

4   Sophos contends that Finjan failed to show that its accused products meet the '926 patent's

5   element of "transmitting the incoming Downloadable and a representation of the retrieved

6   Downloadable security profile data to a destination computer" because Finjan did not show that

7   this information is transmitted to the end-user computers. Mot. for JMOL at 9. It asserts that a

8   "destination computer" must be the end-user computer because this is consistent with the patent's

9   specification. *Id.*; TX-6, '926 patent at 7:63-65 ("[a] suitable information-destination or 'user

10   device' can further include one or more devices or processes (such as email, browser or other

11   clients))." It adds that if the "destination computer" can be any kind of computer then the word

12   "destination" would be redundant because the element already requires a transmission.

13   Finjan asserts that "destination computer" does not refer exclusively to an end-user

14   computer. Oppo. to JMOL at 15. It argues that Sophos's reading would exclude certain

15   embodiments of the '926 patent that do not require the "destination computer" to be an end-user

16   device. *Id.*; TX-6 Col. 7, 11. 2-6 ("other configuration of interconnected elements might also be

17   utilized (e.g. peer-peer, routers, proxy servers, networks, converters, gateways, services, network

18   reconfiguration elements, etc.) in accordance with a particular application"). It adds that it

19   presented substantial evidence that Sophos's products transmit the Downloadable security profiles

20   to various destination computers. *See, e.g.*, Trial Tr. at 633:7-636:16, TX-95 (Mitzenmacher

21   testifying that the UTM product submits downloadable security profiles to a sample submission

22   server, which stores the content and the threat identity on the SXL server).

23   Sophos's argument that Finjan's interpretation of "destination computer" would read

24   "destination" out of the claim is plausible but not conclusive. Even under Finjan's reading the

25   word "destination" adds something – it emphasizes that the computer to which the downloadable

26   is being transmitted is not *any* computer, but rather a particular computer. Further, Finjan has

27   presented evidence that "destination computer" may have many meanings under the '926 patent.

28   Finjan has presented substantial evidence that Sophos's products transmit downloadable security

39

1 profiles to particular designated servers that act as the "destination computer" for the purposes of

2 this claim element. The jury's conclusion that Sophos's products infringe the '926 patent is

3 supported by substantial evidence.

4   C.   **The '780 Patent**

5   Sophos argues that Finjan failed to show that Sophos's products meet two limitations of

6 the '780 patent: "obtaining a Downloadable that includes one or more references to software

7 components required to be executed by the Downloadable" and "fetching at least one software

8 component identified by the one or more references." Mot. for JMOL at 10-11.

9   Sophos asserts that the term "fetching" requires the infringing product to go out and

10 acquire code that was not originally included in the Downloadable. Mot. for JMOL at 10. It

11 asserts that Finjan's evidence shows that the Sophos products only "fetch" code that was already

12 included in the Downloadable and so do not meet this limitation. *Id.* Sophos also contends that

13 these "fetched" components are not "required to be executed" because Finjan did not show that

14 they "needed to run or complete the corresponding page." *Id.*

15   Finjan presented substantial evidence that Sophos's products meet both of these

16 limitations. Oppo. to JMOL at 16. Mitzenmacher testified that the SAV engine in the UTM and

17 Sophos Live Cloud products fetches multiple components while processing the content, computes

18 hashes for this content, and then divides the components up into individual streams. Trial Tr. at

19 568:23-569:8; 571:15-21, TX-2228 at 1197SOPHOS_00388944. He also testified that Sophos's

20 products fetch "dropped" files, which are "outside code that would be downloaded also and is

21 needed to run or complete the corresponding page." Trial Tr. at 563:6-14.

22   The parties have different interpretations of what the "fetching" and "required to be

23 executed" terms require, but Finjan's interpretations are plausible and the jury reasonably could

24 have adopted them. Finjan presented substantial evidence to demonstrate that Sophos's products

25 meet the '780 patent limitations.

26   D.   **The '154 Patent**

27   Sophos argues that Finjan failed to meet three different elements of the '154 patent.

28

40

1   1.   **Whether the second function is invoked using the same input as the first function**

2   The '154 patent requires that the content processor receive content that includes a "call to a

3   first function and the call including an input," and invoke "a second function with the input." TX-

4   4. The parties agree that the claim requires that the input included in the first function be the same

5   input invoked in the second function. Mot. for JMOL at 12; Oppo. to JMOL at 17. Sophos

6   contends that this element is not met because, as Mitzenmacher testified, for Sophos's accused

7   products, the input to the accused first function is a "highly obfuscated URL" but the input to the

8   accused second function is the "de-obfuscated URL." Trial Tr. at 658:8-659:18; 664:3-15;

9   666:13-23.

10   Finjan rebuts by emphasizing that the URLs in the first and second function are the same

11   except that the first one is "obfuscated" and the second one has been de-obfuscated so that it may

12   be read. Oppo. to JMOL at 17. Whether these two inputs are sufficiently similar to qualify as the

13   same input is a close fact question and the jury reasonably could have adopted either

14   interpretation. The jury's apparent conclusion that these were the same input is substantially

15   supported by the undisputed evidence.

16   2.   **Whether the accused products invoke the second function "only if" a security computer indicates it is safe**

17   The '154 patent requires that the "second function" be invoked "only if a security

18   computer indicates that such invocation is safe." Sophos contends that its products do not meet

19   this limitation because the second function must be run to trigger a check of the security computer

20   and so is always invoked. Mot. for JMOL at 13; Trial Tr. at 665:4-66:5; 739:4-10.

21   Finjan asserts that this was a disputed fact question at trial and that it presented substantial

22   evidence in support of its claim that the second function is only invoked when it is safe. Oppo. to

23   JMOL at 18. It notes that Mitzenmacher testified that the invocation only occurs if the SXL

24   server, or the "security computer," indicates that the invocation is safe. Trial Tr. at 663:24-664:17.

25   He also testified that the SAV engine processes the content and prevents the execution of

26   malicious code if the SXL server determines that the content is not safe. *Id.*; 671:13-674:25; TX-

27   2808. Finjan presented substantial evidence to demonstrate that Sophos's products meet this

28

41

claim limitation.

3. **Whether Sophos's products receive content with a call to a substitute function**

Sophos asserts that the '154 patent requires that the claimed first function be a "substitute function" and that the claimed second function be the "original function." It points to language from the patent explaining that "the present invention operates by replacing original function calls with substitute function calls within the content, at a gateway computer, prior to the content being received at the client computer." TX-4, '154 patent at 4:57-60; *Verizon Servs. Corp. v. Vonage Holdings Corp.*, 503 F.3d 1295, 1308 (Fed. Cir. 2007) ("When a patent thus describes the features of the 'present invention' as a whole, this description limits the scope of the invention.")

Finjan rebuts that this is a new construction of the term and does not comport with a plain and ordinary reading of the claims as nothing suggests s "first function" must be a "substitute function" in the claim itself. Oppo. to JMOL at 19. It notes that Mitzenmacher's opinion was based on testimony from Sophos's engineers and documents, and that he concluded that Sophos's products infringed this element under its plain and ordinary meaning. Trial Tr. at 657:25-666:12, TX-2150 at 2; TX-2831 at 223.

Finjan presented substantial evidence that Sophos's products infringed the '154 patent under a plain and ordinary reading of Claim 1. This is sufficient to support the jury's verdict.

E. **The '494 Patent**

Sophos contends that Finjan failed to meet two elements of the '494 patent.

1. **Whether the accused products run Downloadables on destination computers**

Sophos argues that Finjan failed to show that Sophos's products run a "Downloadable" on a destination computer. The court construed "Downloadable" to mean "an executable application program, which is downloaded from a source computer and run on the destination computer." Dkt. No. 73. Cole testified that for this patent, the destination computer is the end-user computer that makes the initial request. He testified that Sophos's UTM "block[s] [the downloadable] from ever making it to the user." Trial Tr. 359:13-19. He also testified that if SophosLabs determines that a Downloadable is malicious "it will be blocked" and will not be executed on the destination

1   computer. *Id.* at 332:19-333:3. Sophos contends that because these applications are blocked

2   before they run on the destination computer, they do not meet the claim construction definition of

3   "Downloadable." To meet the definition, it argues, the applications must actually be run on the

4   destination computer.

5   Finjan asserts that Sophos's argument is based on a "twisted interpretation" of the term

6   Downloadable. Oppo. to JMOL at 21. It submits that the term Downloadable refers to a category

7   of content, including JavaScript, JavaApplets, and ActiveX components and that content of this

8   kind remains a "Downloadable" even when it is not actually run on a destination computer. *Id.* at

9   20. It also notes that even Sophos's experts testified that a product that prevents a Downloadable

10 from running on the destination computer may satisfy this claim. Trial Tr. 1404:24-1405:12;

11 1405:11-12 .

12 The question of whether a Downloadable must be run on a destination computer to be a

13 Downloadable, or whether it needs only to be able to run, was a question raised by the jury. Dkt.

14 No. 394. After discussing the issue with counsel, and concluding that there was no agreed-upon

15 interpretation, I instructed the jury to read the term "Downloadable" in the context of the claims.

16 *Id.* The jury's assessment of the term and ultimate conclusion that Sophos's products infringed

17 the '494 claim were reasonable and well supported by the evidence.

18   2.   **Whether the accused products "store" security profile data in a
                            "database"**

19 Sophos asserts that Finjan failed to present evidence that Sophos's products "store" data

20 and therefore did not show that Sophos's products contain a "database" within the court's

21 construction of the term. Mot. for JMOL at 15.

22 Finjan responds that it presented substantial evidence to demonstrate that Sophos's Genes,

23 Blackboard, Scanners, S3, Warzone, and SOFA databases are databases under the Court's

24 construction. Oppo. to JMOL at 23. It notes that Cole testified that the Genes Database stores

25 information used during processing. Trial Tr. at 431:5-432:6. He also testified that the

26 Blackboard Database stored information related to the processing of SXL responses, including the

27 Downloadable security profiles. Trial Tr. at 350:15-351:6; 405:18-411:1; TX-2242 at

28

43

1197SOPHOS_00872234 ("The Blackboard is a database which stores structured data."). Finjan also presented evidence that Sophos's Scanners, Warzone, S3, and SOFA databases meet the "database" construction. Trial Tr. at 378:9-380:11 ("[Sophos Live Cloud] will go through that and create that threat profile that contains those different suspicious activities. It will then store that in the Warzone database. And then that database also updates a Sophos database, a scanners and a Warzone."); *see also id.* at 390:17-391:16, 406:21-407:13; 418:3-7.

Finjan presented substantial evidence that Sophos's databases are "databases" under the court's claim construction. The jury's verdict is supported by substantial evidence.

Sophos's Motion for JMOL is DENIED.

MOTION FOR PARTIAL JUDGMENT

BACKGROUND

Sophos seeks partial judgment and a finding of fact that (1) collateral estoppel applies to its invalidity case; and (2) that the '494 and '844 patents are invalid under 35 U.S.C. § 101. Mot. for Partial Judgment at 2, 9 (Dkt. No. 429). As discussed with regard to Sophos's motion for a new trial, Sophos has not demonstrated that collateral estoppel applies to this case. I will address Sophos's Section 101 argument below. Because I conclude that the '494 and '844 patents are not invalid under Section 101, Finjan's motion for a partial judgment and finding of fact is DENIED.

LEGAL STANDARD

35 U.S.C. § 101 states that "[w]hoever invents or discovers any new and useful process, machine of composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title." The Supreme Court has determined that section 101 has an implicit exception and that "[l]aws of nature, natural phenomena, and abstract ideas are not patentable." *Ass'n for Molecular Pathology v. Myriad Genetics, Inc.*, 133 S.Ct. 2107, 2116 (2013) (internal quotation marks and citation omitted).

In *Alice Corp. Pt. Ltd. v. CLS Bank* Int'l, 134 S.Ct. 2347 (2014), the Supreme Court established a two-step framework to assess whether a particular patent falls within this exception. Step one is to "determine whether the claims at issue are directed to a patent-ineligible concept" such as an abstract idea. *Id.* at 2355. If a patent is not directed at a patent ineligible concept the

44

1   court's inquiry ends and the patent is presumed valid. If a patent's claims are directed at an

2   ineligible concept, the court moves on to step two and "consider[s] the elements of each claim

3   both individually and as an ordered combination to determine whether the additional elements

4   transform the nature of the claim into a patent-eligible application." *Id.* If the patent has

5   additional inventive concepts that transform it into a patent-eligible application, it is presumed

6   valid. But if the patent's claims are directed at an ineligible concept and the patent does not

7   contain additional elements that transform the nature of the claim into a patent-eligible application,

8   the patent is invalid under *Alice.*

9   The Federal Circuit has outlined how *Alice* applies in the specific context of software

10   patents. In applying step one, the court has concluded that claims relating to receiving and

11   categorizing data are generally abstract. *See Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d

12   1350, 1353 (Fed. Circ. 2016) ("we have treated collecting information, including when limited to

13   particular content (which does not change its character as information), as within the realm of

14   abstract ideas."). In contrast, claims that are directed at a particular improvement in computer

15   technology are generally not abstract. *See Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335

16   (Fed. Cir. 2016) ("[C]laims purporting to improve the functioning of the computer itself, of

17   improve an existing technological process" are not directed at abstract ideas.).

18   In *Enfish*, the Federal Circuit concluded that claims directed to a specific type of self-

19   referential table were not abstract because they constituted a "solution to a problem in the software

20   arts" and were "non-abstract improvements to computer technology." *Id.* at 1339. In *McRo, Inc.*

21   *v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1314 (Fed. Cir. 2016) the court concluded that

22   patents directed at automating existing methods for creating 3-D facial animations were not

23   abstract because they "focused on a specific asserted improvement in computer animation, i.e., the

24   automatic use of rules of a particular type." The *McRo* court noted that the claims outlined a

25   particular process and set of rules for achieving a particular improvement in computer technology,

26   and explained that "[i]t is the incorporation of the claimed rules, not the use of the computer, that

27   'improved [the] existing technological process' by allowing the automation of further tasks." *Id.*

28   at 1314.

1   As it did in *McRo*, the Federal Circuit has repeatedly emphasized that a patent is not

2   directed at patent-eligible concepts simply because it uses or is directed at computer technology.

3   Claims that simply use "existing computers as tools in aid of processes focused on abstract ideas"

4   rather than outlining "computer-functionality improvements" are still abstract. *Elec. Power Grp.*,

5   830 F.3d at 1354; *see also Affinity Labs of Texas, LLC v. DIRECTV, LLC*, 838 F.3d 1253, 1262

6   (Fed. Cir. 2016) (claims were abstract where they were directed to the "general concept of out-of-

7   region delivery of broadcast content through the use of conventional devices, without offering any

8   technological means of effecting that concept."); *BASCOM Glob. Internet Servs., Inc. v. AT&T*

9   *Mobility LLC*, 827 F.3d 1341, 1348 (Fed. Cir. 2016) (claims involving a system for Internet

10   content filtering were abstract because "filtering content . . . is a longstanding, well-known method

11   of organizing human behavior, similar to concepts previously found to be abstract"); *Intellectual*

12   *Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1314 (Fed. Cir. 2016) ("Characterizing e-mail

13   based on a known list of identifiers is no less abstract" than "for people receiving paper mail to

14   look at an envelope and discard certain letters, without opening them, from sources from which

15   they did not wish to receive mail based on characteristics of the mail.").

16   If a patent is directed at an abstract idea, courts must determine at *Alice* step two whether

17   the claims "both individually and as an ordered combination" as well as any "additional features"

18   in the claims amount to an "inventive concept" sufficient to make the claims patent-eligible.

19   *Alice*, 134 S.Ct. at 2357. An inventive concept "cannot simply be an instruction to implement or

20   apply the abstract idea on a computer" and "must be significantly more than the abstract idea

21   itself." *BASCOM*, 827 F.3d at 1349. Claims that "require an arguably inventive set of

22   components or methods" and claims that detail "how the desired result is achieved" may constitute

23   an inventive concept. *Elec. Power Grp.*, 830 F.3d at 1355.

24   The Federal Circuit has found an inventive concept in several software patent cases. In

25   *DDR Holdings, LLC v. Hotels.com, L.P.*, the Federal Circuit concluded that claims that addressed

26   the Internet problem of ads that "lure . . . visitor traffic away" from the host website had an

27   inventive concept. 773 F.3d 1245, 1248, 1259 (Fed. Cir. 2014). The court noted that the claims

28   "specify how interactions with the Internet are manipulated to yield a desired result" because they

46

1   laid out a specific means of resolving this issue: creating a composite website that used the visual

2   elements of the host website but included the third-party advertising content. *Id.* at 1248, 1259.

3   The court also found an inventive concept in *BASCOM*. 827 F.3d at 1350. There, the

4   claims involved "install[ing] a filtering tool at a specific location, remote from the end-users, with

5   customizable filtering features specific to each end user." *Id.* The *BASCOM* court noted that "an

6   inventive concept can be found in the non-conventional and non-generic arrangement of known

7   conventional pieces" and explained that this applied because the claims used a technical feature of

8   a network to outline a "specific method of filtering Internet content." *Id.* And, recently in *Amdocs*

9   *(Israel) Ltd. v. Openet Telecom, Inc.*, the Federal Circuit concluded that claims involving

10   managing accounting and billing data amounted to an inventive concept because they had specific

11   enhancing limitations that "necessarily incorporate[d] the invention's distributed architecture—an

12   architecture providing a technological solution to a technological problem." 841 F.3d, 1288, 1301

13   (Fed. Cir. 2016).

14   Finally, because the *Alice* analysis is quite complex, courts often do several sanity checks

15   when assessing whether a patent or claim is patent eligible. First courts consider whether a claim

16   is so abstract that it would "pre-empt use of [the claimed] approach in all fields, and would

17   effectively grant a monopoly over an abstract idea." *Bilski v. Kappos*, 561 U.S. 593, 612 (2010).

18   If so, the claim is not patent eligible. *Id.* Similarly, courts may ask whether the "claims [] are so

19   result-focused, so functional, as to effectively cover any solution to an identified problem."

20   *Affinity Labs*, 838 F.3d at 1265. Such claims are similarly patent ineligible.

DISCUSSION

22   Sophos argues that Finjan's '494 patent and '844 patent are invalid under Section 101.

23   They assert that these patents fail the *Alice* two-step analysis because their claims are directed at

24   abstract ideas and they do not contain any inventive concepts. Mot. for Partial Judgment at 9-18.

25   This is not the first time that the '494 and '844 patent have been challenged under section

26   101. In two separate cases between Finjan and Blue Coat Systems, Judge Freeman analyzed the

27   '844 patent and the '494 patent to determine whether they were patent eligible under the *Alice*

28   two-step test. In *Finjan, Inc. v. Blue Coat Sys., Inc.* No. 13-cv-03999-BLF, 2015 WL 7351450, at

1   *10 (N.D. Cal. Nov. 20, 2015) (*Blue Coat I*), Judge Freeman concluded that the '844 patent was

2   not directed at an abstract idea because it "has important and specific limitations about providing

3   pro-active protection [that] provide meaningful boundaries on the invention." And, more recently,

4   in *Finjan, Inc. v. Blue Coat Sys., LLC*, No. 15-cv-03295-BLF, 2016 WL 7212322, at *11 (N.D.

5   Cal. Dec. 13, 2016) (*Blue Coat II*), Judge Freeman concluded that the '494 patent was patent

6   eligible because, although its claims are directed at abstract ideas, the claims, "taken as an ordered

7   combination, recite an inventive concept sufficient to render them patent eligible" because they

8   provide "both spatial and temporal alterations" to traditional virus protection programs.

9   Judge Freeman's analysis of each patent is instructive. As discussed below, I conclude

10   that both the '494 and '844 patents are patent-eligible. I agree with Judge Freeman's conclusion

11   in *Blue Coat II* that, although the '494 patent is directed at abstract ideas, it contains inventive

12   concepts and is therefore patent eligible. I similarly conclude that the '844 patent is directed at

13   abstract ideas, but like the '494 patent, contains inventive concepts that make it patent eligible.

14   Notably, this is not the same conclusion Judge Freeman reached in *Blue Coat I*, where she held

15   that the '844 patent is not directed at an abstract-idea because it has specific limitations that place

16   meaningful boundaries on the invention. 2015 WL 7351450, at *10. However, in her more recent

17   *Blue Coat II* order, she acknowledged that her analysis of the '844 patent may no longer hold

18   given the intervening precedent from the Federal Circuit. My analysis of the '844 patent defers to

19   the more recent Federal Circuit cases and Judge Freeman's analysis with regard to the '494 patent.

20   I.   **THE '494 PATENT**

21   A.   **Background**

22   In *Blue Coat II*, Judge Freeman provided a detailed background and explanation of the

23   '494 patent. For ease of reference, I incorporate her factual background here:

> Finjan owns the '494 patent, which is entitled "Malicious Mobile
> Code Runtime Monitoring System and Methods." The '494 patent
> was filed on November 7, 2011 and issued on March 18, 2014, but
> belongs to a long line of continuation and continuation-in-part
> applications which originated from patent applications filed in 1996.
> One of these parent applications resulted in U.S. Patent No.
> 6,092,194 (the "'194 patent"), which the '494 patent identifies in its
> specification and states is "incorporated by reference." '494 patent,
> col. 1 ll. 33-38.

48

The '494 patent generally relates to systems and methods for protecting devices on an internal network from code, applications, and/or information downloaded from the Internet that perform malicious operations. *Id.*, Abstract. According to the '494 patent, at the time of invention, virus protection strategies for networked computers "met with limited success at best" because virus scanning was localized and reactive: virus protection programs were installed on individual computers and only protected against known viruses. *Id.*, col. 2 ll. 11-21. Because of this, these "program[s] [would] inevitably [be] surmounted by some new virus," at which point they would need to be updated or replaced and the cycle would begin again. *Id.* In addition, certain types of viruses were "not well recognized or understood, let alone protected against." *Id.*, col. 2 ll. 22-24. This included viruses that were hidden in executable programs such as "Downloadables." *Id.*, col. 2 ll. 23-30. "Accordingly, there remains a need for efficient, accurate, and flexible protection of computers and other network connectable devices from malicious Downloadables." *Id.*, col. 2. Ll. 45-48.

The '494 patent purports to address this problem by detecting whether downloadable content contains potentially malicious code before it is allowed to be run on the destination computer. *See id.*, col. 5 l. 60-col. 6 l. 6. At a high level, the disclosed embodiments describe a protection engine that generally resides on a network server and inspects incoming downloads for executable code. *See id.*, col. 2 l. 20-col. 3 l. 4; '194 patent, col. 3 ll. 10-21. The claims are directed to a narrow aspect of this, which involve a solution consisting of three basic steps that appear to be most closely detailed in the '194 patent:

First, an incoming Downloadable is intercepted. '494 patent, col. 21 l. 20, col. 22 l. 8. The '194 specification describes an "Internal Network Security System" which sits in between an external computer network and the internal computer network and "examines Downloadables received from external computer network 105, and prevents Downloadables deemed suspicious from reaching the internal computer network 115." '194 patent, col. 3 ll. 10-13.

Second, the Downloadable is scanned and "security profile data," which includes "a list of suspicious computer operations that may be attempted by the Downloadable," is derived. '494 patent, col. 21 ll. 21-23, col. 22 ll. 10-13. The '194 specification discloses a "code scanner" component that scans through a Downloadable and generates the "security profile data" (also referred to as "Downloadable Security Profile (DSP) data," '194 patent, col. 4 ll. 17-18). '194 patent, col. 5 ll. 41-42. Figure 7 of the '194 specification illustrates this process:
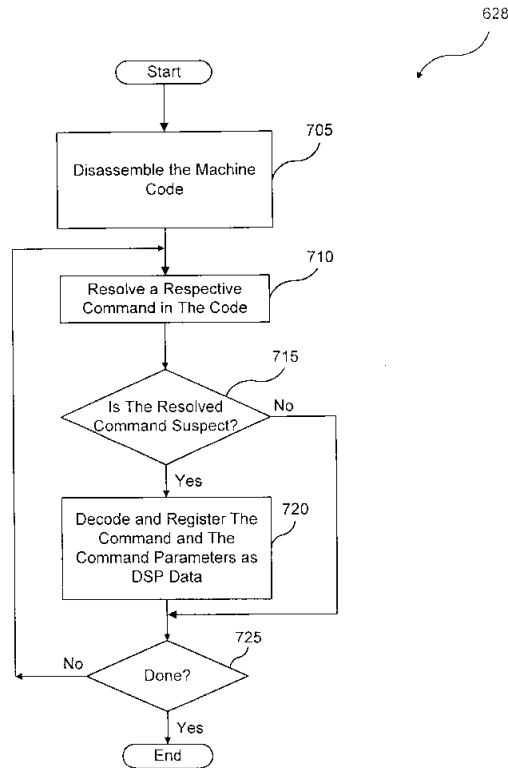
FIG. 7

Id., Fig. 7. At the beginning of the process, the code scanner "disassemble[s] the machine code of the Downloadable." *Id.*, col. 9 ll. 23-24. Next, the code scanner iterates through the machines code, (1) resolving the next command in the machine code, (2) "determin[ing] whether the resolved command is suspicious," and, if so, (3) "decod[ing] and register[ing] the suspicious command and its command parameters as DSP data." *Id.*, col. 9 ll. 20-42. The format of the DSP data is "based on command class (e.g., file operations, network operations, registry operations, operating system operations, resource usage thresholds)." *Id.*, col. 9 ll. 38-42. Examples of operations deemed potentially hostile include:

> File operations: READ a file, WRITE a file; Network operations: LISTEN on a socket, CONNECT to a socket, SEND data, RECEIVE data, VIEW INTRANET; Registry operations: READ a registry item, WRITE a registry item; Operating system operations: EXIT WINDOWS, EXIT BROWSER, START PROCESS/THREAT, KILL PROCESS/THREAD CHANGE PROCESS/THREAD PRIORITY, DYNAMICALLY LOAD A CLASS/LIBRARY, etc.; and Resource usage thresholds: memory, CPU, graphics, etc.

Id., col. 5 l. 59-col. 6 l. 4.

Third, the "security profile data" is stored in a database. '494 patent, col. 21 ll. 24-25, col. 22 ll. 14-16. The '194 specification discloses that, after DSP data is generated, it is stored in a "DSP data" data object according to the Downloadable's ID.

50

'194 patent, col. 6 ll. 9-10 ("[t]he code scanner 325 then stores the DSP data into DSP data 310 (corresponding to its Downloadable ID)"). The DSP data is then stored in "security database 240," along with other data such as security policies, a list of known Downloadables, and a list of known Certificates. *See id.*, col. 3 ll. 47-50, col. 4 ll. 15-18.

The '194 specification discloses that DSP, data stores in the database can be compared, along with other information, against a security policy to determine whether the Downloadable should be permitted to be run on the destination computer. *See id.*, col. 6 ll. 13-20. However, the claims themselves do not recite this, nor any subsequent use of the security profile data, after it gets stored in the database. '494 patent, col. 21 ll. 22-23, col. 22 ll. 8-17.

Finjan currently asserts claims 1, 10, 14, [] and 18. [] Independent claims 1 and 10 recite:

> 1. A computer-based method, comprising the steps of:
> Receiving an incoming Downloadable;
> Deriving security profile data for the Downloadable, including a list
> Of suspicious computer operations that may be attempted by the Downloadable; and Storing the Downloadable security profile data in a database.

> 10. A system for managing Downloadables, comprising:
> a receiver for receiving an incoming Downloadable;
> a Downloadable scanner coupled with said receiver, for deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and a database manager coupled with said Downloadable scanner, for storing the Downloadable security profile data in a database.

Id., col. 21 ll. 22-23, col. 22 ll. 8-17. Claim 14 additionally requires that the Downloadable include a program script. *Id.*, col. 22 ll. 26-27. . . . Claim 18 requires that the Downloadable scanner comprise a disassembler. *Id.*, col. 22 ll. 37-39.

Blue Coat II, 2016 WL 7212322, at *1-3.

B.   **Scope of Review**

As Judge Freeman explained in *Blue Coat II*, when assessing the scope of a patent the Section 101 inquiry must focus on the language of the Asserted Claims themselves. *Id.* at *7. "[T]he complexity of the implementing software or the level of detail in the specification does not transform a claim reciting only an abstract concept into a patent-eligible system or method." *Accenture Glob. Servs., GmbH v. Guidewire Software, Inc.*, 728 F.3d 1336, 1345 (Fed. Cir. 2013). "Nevertheless, the specification, as a helpful tool in understanding claim scope, is not to be ignored entirely." *Blue Coat II*, 2016 WL 7212322, at *7; *see also Enfish*, 822 F.3d at 1335 ("The

51

1 'directed to' inquiry applies a stage-one filter to claims, considered in light of the specification,

2 based on whether their character as a whole is directed to excluded subject matter.") (internal

3 quotation marks and citation omitted).

4   Accordingly, Judge Freeman did not review the '494 claims in a vacuum, but reviewed

5 them in the context of the '494 specification and the specification for the '194 patent, which the

6 '494 patent incorporates by reference. *Blue Coat II*, 2016 WL 7212322, at *8 ("[I]n assessing

7 patent eligibility here, the Court must restrict itself to the language of the asserted claims of the

8 '494 patent, which recite, in relatively broad terms only three basic functions: receiving, deriving,

9 and storing. Nevertheless, each of these functions should be read in light of the specification,

10 including its detailed descriptions of how a 'Downloadable' is 'receiv[ed]' or how 'security profile

11 data' is deriv[ed].' "). Further because Finjan was the non-moving party, Judge Freeman

12 construed the claims in the light most favorable to Finjan, which meant "err[ing] on the side of

13 incorporating more-not-less-particularities from the specification into its understanding of the

14 claims, while still refraining from importing limitations from the specification into the claim." *Id.*

15   Judge Freeman's analysis applies equally here: while the review must be limited to the

16 claims of the '494 patent, these claims should be read in the context of the patent's specifications,

17 as well as the '194 patent's specifications. *Id.* (Concluding that the entire '194 patent is

18 incorporated into the '494 patent because the '494 patent "indicates that it is incorporating the

19 entire '194 patent, and provides enough information for the reader to locate this information.")

20   C.   ***Alice* Step One**

21   Sophos argues that the '494 Patent is invalid because its claims are directed at the abstract

22 ideas of "receiving data, extracting information from that received data, then storing that

23 information." Mot. for Partial Judgment at 10. It adds that the claims do not "recite any specific

24 way" of accomplishing these steps and so the claims would "prohibit all other persons from

25 making the same thing by any means whatsoever." *Id.* at 11.

26   Finjan responds that the '494 patent is not directed at an abstract idea because it is "deeply

27 rooted in computer technology, improves computer functionality and addresses the specific

28 problem of malicious Downloadables which were non-existent prior to the claimed inventions."

United States District Court
Northern District of California

1   Oppo. to Mot. for Partial Judgment at 16 (Dkt. No. 438). Finjan asserts that Sophos fails to look

2   at the claims as a whole and improperly analyzes and overgeneralizes each step. *Id.* at 17. It

3   argues that the '494 claims, "by covering the generation of a list of suspicious computer

4   operations related to the Downloadable, are directed to an improvement to computer functionality

5   and are different from prior, conventional antivirus technology." *Id.* at 21.

6   I agree with Sophos that the '494 claims are directed at an abstract idea. While the claims

7   are meant to be utilized in the particular context of malware protection, the asserted claims

8   themselves only list the abstract ideas of "receiving data, extracting information from that received

9   data, then storing that information." Mot. for Partial Judgment at 10. As Judge Freeman noted in

10   *Blue Coat II*, this remains true even when the claims are viewed in the context of the details

11   outlined in the '194 patent. *Blue Coat II*, 2016 WL 7212322, at *9 ("At their heart, they claim

12   nothing more than a solution that scans through data (e.g., the disassembled code from the code

13   scanner, '194 patent, col. 5 ll. 41-45, col. 9 ll. 20-42), identifies certain characteristics (e.g., the

14   operations that match its pre-existing list of operations, '194 patent, col. 5 l. 45 - col. 6 l. 4), and

15   stores the results of the analysis (e.g., the list of suspicious operations encountered, stored as

16   formatted DSP data, '194 patent, col. 6 ll. 9-10)".) These steps are similar to the way a person

17   could categorize and sort elements in a non-computer context – for example, a clerk in a mailroom

18   may perform conceptually similar tasks. And, while the specific claims (1, 10, 14, and 18)

19   provide some limitations on the context in which this process is performed, the overall purpose

20   and focus of the claims remains directed at the abstract idea of receiving and analyzing data, and

21   storing that information.

22   This analysis is in line with Federal Circuit precedent, which makes clear that claims that

23   utilize computer technology as a tool to perform an abstract idea, but do not themselves improve

24   computer function, remain abstract. *See e.g.*, *BASCOM*, 827 F.3d at 1348 (claims related to

25   filtering content on the Internet were directed to an abstract idea); *Intellectual Ventures I*, 838 F.3d

26   at 1314 (claims related to filtering email for viruses and unwanted spam were directed at an

27   abstract idea). The '494 claims place the abstract idea of receiving, analyzing, and storing data

28   into the computer context but do not outline a specific improvement to the way computers operate.

1   *Elec. Power Grp.,* 830 F.3d at 1354. "They recite use of generic computer components to perform

2   data collection and analysis generally. They do not recite an improvement to a particular

3   computer technology used in malware detection – they do not, for example, claim an improvement

4   to a specific, preexisting malware detection algorithm or recite special data structures that

5   fundamentally improve the process of detecting malware." *Blue Coat II*, 2016 7212322, at *10.

6   Under *Alice* step-one, the '494 claims are directed at an abstract idea. *Alice*, 134 S.Ct. at 2355.

7   D.   *Alice* **Step Two**

8   Under step two the court considers whether the claim elements, "both individually and as

9   an ordered combination" recite an "inventive concept" which "transform[s] the nature of the claim

10 into a patent-eligible application." *Id.* at 2355.

11   Sophos argues that the '494 patent simply recites the basic steps of "receiving," "deriving,"

12 and "storing" performed with a "receiver," "scanner" and "database manager" and that there is

13 "nothing inventive about these routine computer functions and components, either alone or in an

14 ordered combination." Mot. for Partial Judgment at 16. Finjan responds that the claims recite an

15 inventive concept because they are "directed to providing a concrete and inventive solution to a

16 real world problem by addressing the need for behavior-based detection of malicious code in

17 Downloadables (i.e. downloaded executable application), as opposed to signature-based

18 techniques or other types of files." Oppo. to Mot. for Partial Judgment at 22.

19   I agree with Finjan (and Judge Freeman in *Blue Coat II)* that the claims recite an inventive

20 concept when taken as an ordered combination and considered in context. The '494 patent notes

21 that, prior to its invention, malware protection programs were only able to detect and protect

22 against known viruses and were installed on particular user computers. '494 patent, col. 2 ll. 11-

23 21. The '494 patent details a new kind of virus protection: one that is located on a network

24 computer, rather than the end-user computer, and which is able to detect unknown viruses by

25 identifying suspicious components in unique and novel code. The '494 patent therefore includes a

26 "non-conventional and non-generic arrangement of known, conventional pieces" such that, when

27 taken as an ordered combination, it recites an inventive concept. *BASCOM*, 827 F.3d at 1350.

28   While viewing the '494 patent in the light most favorable to Finjan, the patent is

54

1   innovative because, instead of conducting malware analysis on an end-user computer, the '494

2   patent describes a system where malware scanning take place on a separate, intermediate network.

3   In *Blue Coat II*, Judge Freeman acknowledges that this is not made explicit by the '494 claims

4   themselves, but explains that the patent specifications make clear that the claim steps take place on

5   a network. *Blue Coat II*, 2016 WL 7212322, at *11 ("All embodiments of the protection engines

6   disclosed in the '494 and '194 specifications reside on a network server. *See* '494 patent, col. 2 l.

7   20-col. 3 l. 4; '194 patent, col. 3 ll. 10-21. In addition, the '194 specification discloses that the

8   code scanner, the particular component that performs the analysis to derive the data security

9   profile, resides in the Internal Network Security System, which sits in between the external

10   computer network and end-user computers. '194 patent, Fig. 1; col. 3 ll. 10-13.). As Judge

11   Freeman concluded, this arrangement represents a novel use of specific computer systems in a

12   "non-conventional and non-generic arrangement" to improve malware protection systems for

13   computer networks. *Id.*; *BASCOM*, 827 F.3d at 1350.

14   Further, the '494 patent is innovative because it describes a method of scanning and

15   extracting particular suspicious elements of a file rather than scanning only entire files. Again, in

16   *Blue Coat II*, Judge Freeman explains that this is not laid out explicitly in the claims, but that a

17   person of ordinary skill in the art would understand the claims to detail this process:

18   "[D]eriving security profile data," if construed in a light most
             favorable to Finjan, at least requires a process of parsing through a
19   Downloadable and creating a list of all potentially suspicious
             computer operations. The claims themselves recite that "security
20   profile data" must include "a list of suspicious computer operations
             that may be attempted by the Downloadable." '494 patent col. 21 ll.
21   22-23, col. 22 ll. 11-12. By necessity, then, "deriving" must include
             some means of extracting and identifying these operations. Only the
22   '194 specification uses the phrase "downloadable security profile
             data," and the only embodiment of deriving security profile data that
23   it discloses involves a precise process of decomposing code and
             extracting operations. '194 patent, col. 9 ll. 20-42, Fig. 7. Thus, a
24   person of ordinary skill in the art would understand "deriving
             security profile data" to refer to this type of process.
25
     Blue Coat II, 2016 WL 7212322, at *11. This process is innovative because it allows a malware
26
     detection program to detect new viruses, previously unknown files that contain suspicious
27
     operations, rather than identifying only known viruses. '494 patent, col. 2 ll. 56-64.
28

                                                      55

1   Looking at the '494 patent as a whole, the claims recite an inventive concept because they

2   detail a system that involves scanning malware on an intermediate network, rather than an end-

3   user computer, and because they detail a process for identifying unknown viruses by extracting

4   specific suspicious operations from files. The '494 patent is not patent-ineligible under *Alice*.

5   II.   **THE '844 PATENT**

6   Sophos moves for a finding that the '844 patent is not patent-eligible under section 101. I

7   conclude that the '844 patent is patent eligible because, although its claims are directed at abstract

8   ideas, it contains inventive concepts.

9   A.   **Background on '844 patent**

10   Finjan owns the '844 patent, entitled "System and Method for Attaching a Downloadable

11   Security Profile to a Downloadable." The '844 patent was filed on December 22, 1997 and issued

12   on November 28, 2000. The '844 patent is part of the family of patents derived from the '194

13   patent. As with the '494 patent, the '844 patent incorporates the '194 patent by reference. '844

14   patent, col. 1 ll. 12-15.

15   Generally, the '844 patent relates to methods and systems for protecting computer

16   networks from malicious Downloadables. *Id.* col. 1 ll. 62-65. As the '844 patent explains, at the

17   time of its invention, virus protection software was relatively effective at identifying and blocking

18   Internet computer viruses but was unable to identify viruses "attached to or configured as

19   Downloadable application programs." *Id.* col. 1 ll. 41-45. A Downloadable is an "executable

20   application program" such as Java applets, JavaScript, and plugins. *Id.* col. 1 ll. 45-56.

21   Downloadables are "typically requested by an ongoing process such as by an Internet browser or

22   web client" or may "add to the functionality of an already existing application program." *Id.* col. 1

23   ll. 47-48; ll. 55-56. Because Downloadables are necessary to run many applications, "a system

24   and method are needed to protect a network from hostile Downloadables." *Id.* col. 1 ll. 58-59.

25   The '844 patent attempts to assist in addressing this problem by detailing a system in which an

26   "inspector" analyzes particular elements of Downloadables to assess whether they contain

27   suspicious code or operations. '844 patent at col. 2 ll. 3-19. The inspector then generates a

28   Downloadable security profile ("DSP") – detailing the suspicious operations of the Downloadable,

56

1   and then links this DSP to the Downloadable. *Id.* The DSP may include a list of suspicious

2   operations or a list of suspicious code patterns, and may include a certificate identifying the

3   content inspection engine that created the DSP. *Id.*

4   Finjan asserts claims 1, 15, and 16 against Sophos. Independent claims 1 and 15 read as

5   follows:

> 1. A method comprising:
> receiving by an inspector a Downloadable; generating by the
> inspector a first Downloadable security profile that identifies
> suspicious code in the received Downloadable; and linking by the
> inspector the first Downloadable security profile to the
> Downloadable before a web server makes the Downloadable
> available to web clients.

> 15. An inspector system comprising:
> memory storing a first rule set; and a first content inspection engine
> for using the first rule set to generate a first Downloadable security
> profile that identifies suspicious code in a Downloadable, and for
> linking the first Downloadable security profile to the Downloadable
> before a web server makes the Downloadable available to web
> clients.

Id., col. 11 ll. 13-20; col. 11 ll. 62-col. 12 ll. 2. Claim 16 additionally requires that the inspector

system include a list of suspicious operations. *Id.*, col. 12 ll. 3-4.

     B.   *Alice* **step-one**

     Sophos argues that the '844 patent is directed at an abstract idea of "receiving data,

extracting information from that received data, and linking that information to the received data."

Mot. for Partial Judgment at 18. It asserts that the three steps of "receiving", "generating a

security profile" and "linking" are entirely abstract and do not identify any specific means or

method for accomplishing the claimed linking. *Id.* at 19. It acknowledges that in *Blue Coat I*,

Judge Freeman concluded that the '844 patent is not directed at an abstract idea, but contends that

this conclusion was incorrect.

     Finjan responds that Sophos is improperly second guessing Judge Freeman's decision from

Blue Coat I. Oppo. to Mot. for Partial Judgment at 12. It asserts that the '844 patent is not

directed at an abstract idea because it is "directed to a non-abstract idea and improvement of

computer technology related to the protection of a computer system from malicious code found on

the Internet. *Id.*

57

1   In assessing this issue in *Blue Coat I*, Judge Freeman found a hypothetical patentable claim

2   published by the USPTO particularly persuasive. *Blue Coat I*, 2015 WL 7351450, at *9. The

3   hypothetical claim involved "receiving an electronic communication," "storing the

4   communication," and "extracting . . . malicious code from the electronic communication to create

5   a sanitized electronic communication." *Id.* The USPTO's guidance explained its understanding

6   that this hypothetical claim was not directed at an abstract idea:

7
> The claim is directed towards physically isolating a received
> communication on a memory sector and extracting malicious code

8
> from that communication to create a sanitized communication in a
> new data file. Such action does not describe an abstract concept, or

9
> a concept similar to those found by the courts to be abstract . . . the
> invention claimed here is directed towards performing isolation and

10
> eradication of computer viruses, worms, and other malicious code, a
> concept inextricably tied to computer technology and distinct from

11
> the types of concepts found by the courts to be abstract."

12   *Id.* at *10.

13   However, as Judge Freeman acknowledged in *Blue Coat II*, this analysis may not line up

14   with the Federal Circuit cases that have been published since the *Blue Coat I* decision. *Blue Coat*

15   *II*, 2016 WL 7212322, at *10 (noting that *Blue Coat I* "predated many of the Federal Circuit

16   decision that now guide the Court's step one analysis" and that "[i]f, to any extent, the Court's

17   reasoning in [*Blue Coat I*] conflicts with Federal Circuit precedent, Federal Circuit precedent

18   controls).

19   As *Enfish*, *McRo*, *Electric Power Group*, *BASCOM*, and *Intellectual Ventures I*, all

20   published after *Blue Coat I*, make clear, a patent does not pass step-one of *Alice* simply because it

21   involves concepts inextricably tied to computer technology. *See, e.g.*, *Enfish*, 822 F.3d at 1336.

22   The court must ask "whether the focus of the claims is on the specific asserted improvement in

23   computer capabilities . . . or, instead, on a process that qualifies as an 'abstract idea' for which

24   computers are invoked merely as a tool." *Id.*

25   In light of Judge Freeman's more recent analysis in *Blue Coat II*, and the intervening

26   Federal Circuit cases, I conclude that the '844 patent is directed at an abstract idea. As with the

27   '494 patent, although the receiving, generating, and linking steps are used in the particular context

28   of malware protection software, they remain familiar and general abstract concepts. *Blue Coat II*,

58

1   2016 WL 7212322, at *9 ("These are fundamental concepts germane to any type of content

2   analysis."). *Intellectual Ventures I*, 838 F.3d at 1314 ("The Supreme Court has held that

3   'fundamental . . . practice[s] long prevalent' are abstract ideas"). The claims identify a process of

4   scanning data; identifying particular characteristics of that data and creating a "profile"; and then

5   linking that profile to the data. '844 patent, col. 2 ll. 49-53. As with the '494 patent, this process

6   is similar to how a human might process potentially suspicious mail – for example, a mail

7   inspector might analyze a threatening letter, make a note explaining the particularly suspicious

8   elements of the letter, and link this note to details about the sender. The inspector could then refer

9   to the note in the future when receiving additional mail from the same address.

10   The '844 claims are similar to those found abstract in *BASCOM* and *Intellectual Ventures

11   I*. *BASCOM*, 827 F.3d at 1348 (claims that filtered Internet content were directed at abstract idea);

12   *Intellectual Ventures I*, 838 F.3d at 1314 (claims that filtered email for viruses and spam were

13   directed at abstract idea). That the '844 claims relate to computer technology, and specifically,

14   malware protection, does not mean that they are not directed at abstract ideas. "[A]s a whole" the

15   process described in the '844 patent is focused on the abstract idea of data collection and analysis,

16   and does not present a specific improvement to computer operations. *Enfish*, 822 F.3d at 1335.

17   Accordingly, under *Alice* step-one, I conclude that the '844 claims are directed at an abstract idea.

18   C.   *Alice* **step-two**

19   Under *Alice* step two I must assess whether the claims "individually and as an ordered

20   combination" outline an "inventive concept" sufficient to "transform the nature of the claim into a

21   patent-eligible application." *Alice*, 134 S.Ct. at 2355.

22   Finjan asserts that the '844 claims are inventive because they are "directed to the concrete

23   idea of protecting a computer system against malicious code from the Internet." Oppo. to Mot. for

24   Partial Judgment at 13. It explains that the claims detail the process of "receiving a downloadable

25   and inspecting it before it is downloaded onto a computer," "(2) generating a security profile that

26   identifies suspicious code," and "linking the Downloadable security profile to the Downloadable

27   before it is made available to web clients."

28   Sophos rebuts that there is nothing about "protection" in the claims, which only recite the

United States District Court
Northern District of California

1   basic steps of "receiving a file, generating the security profile and linking it to the file at a

2   particular time." Reply to Mot. for Partial Judgment at 15 (Dkt. No. 447).

3   I agree with Finjan that the '844 patent claims, when taken as an ordered combination,

4   recite an inventive concept. As the '844 patent notes, at the time of its invention, malware security

5   programs were not configured to recognize viruses attached to or configured as Downloadables.

6   '844 patent, col. 1 ll. 41-45. Because Downloadables are common and provide significant

7   functionalities and value, "a system and method are needed to protect a network from hostile

8   Downloadables." Col. 1 ll. 58-59.

9   The '844 patent aims to supply such a method and system. It outlines a process of

10   receiving a Downloadable, generating a downloadable security profile, and linking this profile to

11   the Downloadable before the Downloadable is made available to the end-user. *Id.* col. 11 ll. 13-

12   20. It also outlines a system that includes a content inspection engine that uses a first rule set to

13   identify suspicious code in a Downloadable, generate a Downloadable security profile, and link

14   that security profile to the Downloadable before it is made available to web clients. *Id.* col. 11 ll.

15   61- col. 12 ll. 2.

16   The '844 patent claims harness specific network architecture and use it in non-

17   conventional ways. The claims implement an "inspector" system that receives the Downloadable,

18   generates a Downloadable security profile, and links this profile to the Downloadable before the

19   Downloadable is made available to web clients. *Id.* col. 11 ll. 61- col. 12 ll. 2. Although not

20   made explicit in the claims, because the inspector must link the Downloadable security profile to

21   the Downloadable before it is made available to web clients, the inspector must necessarily be

22   remote from end-users. By performing these scanning and linking steps at a remote location, the

23   '844 patent outlines a system that helps protect the end-user by scanning hostile Downloadables

24   before they are downloaded onto an end-user computer. As virus scanning historically was done

25   on end-user computers, this use of a remote inspector helps make the '844 patent inventive.

26   The '844 patent also outlines a system for identifying new and known hostile

27   Downloadables. The claims require the inspector to generate a Downloadable security profile. As

28   discussed above, and as Judge Freeman explained in *Blue Coat II*, this "at least requires a process

60

1   of parsing through a Downloadable and creating a list of all potentially suspicious computer

2   operations." *Blue Coat II*, 2016 WL 7212322, at *11. This process allows a system to identify

3   unknown hostile Downloadables by scanning for suspicious or hostile operations rather than

4   scanning only entire viruses. The claims also require the inspector to link the security profile to

5   the Downloadable before the Downloadable is made available to web clients. This linking step

6   establishes a system that allows inspectors, in future scans of the Downloadable, to identify known

7   or previously scanned Downloadables and to compare the Downloadable security profile to a

8   security policy. The system therefore allows future inspectors to identify hostile Downloadables

9   without scanning the Downloadable for suspicious operations and generating a new security

10   profile. Because, as the '844 patent explains, early security software was not configured to

11   recognize Downloadables, the process outlined in the '844 patent of scanning Downloadables for

12   suspicious operations and setting up a system to allow for future identification of known hostile

13   Downloadables is a novel technical solution to a previously unaddressed issue.

14   Taking the '844 patent as a whole, the claims recite an inventive concept because they

15   detail a specific technical solution to assist in protecting computer networks from hostile

16   Downloadables, something security systems were previously not configured to do. Although the

17   '844 patent uses well-known systems, "an inventive concept can be found in the non-conventional

18   and non-generic arrangement of known, conventional pieces." *BASCOM*, 827 F.3d at 1350. The

19   '844 patent's specific applications to scanning and analyzing Downloadables, and non-

20   conventional use of a remote inspector to perform scanning and linking of a security profile before

21   the Downloadable is made available to web clients, represent an "inventive concept" because the

22   patent describes a "specific technical solution beyond simply using generic computer concepts in a

23   conventional way." *Id.*

24   The '844 patent does not "pre-empt use of [the claimed] approach in all fields" or

25   "effectively grant a monopoly over an abstract idea." *Bilski*, 561 U.S. at 612. The claim elements

26   are specifically limited to scanning Downloadables, generating Downloadable security profiles,

27   and linking those profiles to the Downloadables. These claims do not preclude use of the

28   scanning, generating data, and linking elements outside the malware security software field and so

61

do not pre-empt all uses of these abstract ideas. Further, the claims are not "so result-focused, so functional, as to effectively cover any solution to an identified problem." *Affinity Labs*, 838 F.3d at 1265. The '844 patent claims outline one technical solution to the problem of protecting computer networks from hostile Downloadables but leave room for many others. Viewing the '844 patent in the light most favorable to the non-movant, Finjan, I conclude that the claims describe an inventive concept, and that the claims are patent eligible.
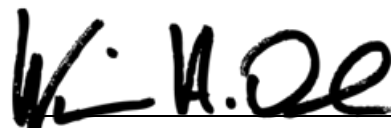
Because the '494 patent and '844 patent include inventive concepts they are not patent ineligible. Sophos's Motion for a Partial Judgment and Finding of Fact is DENIED.

<div align="center">

CONCLUSION

</div>

As outlined above, Finjan's Motion for Attorneys' Fees and Costs is DENIED; Sophos's Motion for a New Trial, or in the Alternative, Remittitur is DENIED; Finjan's Motion to Amend the Judgment and for an Injunction is DENIED, however its request for Pre- and Post-Judgment Interest is GRANTED and will be awarded at the treasury bill rate; Sophos's Renewed Motion for Judgment as a Matter of Law is DENIED; and Sophos's Motion for a Partial Judgment and Finding of Fact is DENIED.

IT IS SO ORDERED.

Dated: March 14, 2017

William H. Orrick
United States District Judge

62