DECLARATION OF AVIEL D. RUBIN

I, Aviel D. Rubin, declare as follows:

I. INTRODUCTION

1. I have been retained as an independent expert in this lawsuit by the law firm of Irell & Manella LLP on behalf of Juniper Networks, Inc. ("Juniper").

2. I submit this Declaration in support of Juniper's Motion (the "Motion") for Summary Judgment Regarding Claim 9 of U.S. Patent No. 6,804,780 Patent ("the '780 Patent") against Finjan, Inc. ("Finjan"). I previously submitted a declaration regarding Claim 1 of the '780 Patent, which I incorporate herein by reference in full, including all exhibits and references thereto. *See* Dkt. 95-10.

3. I understand that Finjan has accused Juniper of infringing Claims 1 and 9 of the '780 Patent (Dkt. 171 ¶ 67), but this declaration is directed specifically to Claim 9. As discussed below, it is my opinion that the accused Juniper products do not infringe Claim 9.

4. In addition to opinions outlined in this declaration, I may also provide testimony (1) in rebuttal to Finjan's positions, including opinions of its experts and materials they discuss or rely upon, (2) based on any Orders from the Court, (3) based on documents, contentions, or other discovery that Finjan or others have not yet produced or were produced too late to be considered before my report was due, and/or (4) based on witness testimony which has not been given or was given too late to be considered before my declaration was due. I reserve the right to supplement or amend my opinions as further documentation and information is received.

II. BACKGROUND AND QUALIFICATIONS

5. I am being paid at my customary rate of $775 per hour for time spent on this case. I am also being reimbursed for reasonable and customary expenses. My compensation is not dependent in any way on the results of the lawsuit or the substance of my testimony.

6. I provided an overview of my background and qualifications in my previous declaration, which I incorporate herein by reference. *See* Dkt. 95-10 at ¶¶ 6-17. Additional details of my education and employment history, professional service, patents, publications, and other

testimony are set forth in my current curriculum vitae, which can be found here: http://avirubin.com/Avi_Rubins_home_page/Vita.html.

III. MATERIALS CONSIDERED

7. I have considered information from various sources in forming my opinions. Besides drawing from over two decades of experience in the computer industry, I also have reviewed the following documents: (a) the '780 patent; (b) the file history (including IPRs); (c) Finjan's Infringement Contentions and cited materials; (d) the parties' summary judgment filings regarding Claim 1 of the '780 Patent (including all declaration and exhibits) as well as the Court's related Order; (e) the deposition transcripts of various Juniper engineers and Finjan's expert; and (f) the other documents and references cited herein (not limited to the excerpts submitted with Juniper's Motion). I have also reviewed the Declaration of Frank Jas ("Jas"), and I previously spoke with Raju Manthena and Yuly Tenorio about the accused products when preparing the declaration I submitted regarding Claim 1.

IV. LEGAL STANDARDS

8. I have been advised that patent claims are reviewed from the point of view of a hypothetical person of ordinary skill in the art ("POSITA") at the time of the filing of the patent.

9. In my opinion, a POSITA for the '780 patent would be a person with a Bachelor's degree in computer science or related academic fields and three to four years of additional experience in the field of computer security or equivalent work experience. More education can substitute for work experience, and vice versa (e.g., a PhD without work experience outside of the university setting). In arriving at my opinions in this declaration, I have considered the issues from the perspective of a POSITA. This level of skill is approximate and my opinion would not change if a somewhat lower or higher level of skill were adopted; in particular, I note that Finjan's expert Dr. Michael Mitzenmacher previously opined regarding a similar but slightly different level of ordinary skill (Dkt. 129-1 at ¶ 13), and my opinion would not change if Dr. Mitzenmacher's level of ordinary skill were adopted.

10. I am informed that patent infringement under 35 U.S.C. § 271(a) consists of making, using, offering to sell, or selling a patented invention within the United States, or importing a patented invention into the United States, without authorization.

11. I further understand that determining whether there is infringement of a patent includes two steps. First, each asserted claim must be construed to determine its proper scope and meaning to a POSITA. Second, the construed claims are compared with the accused product or service to determine whether every limitation of the claims is found. Unless every limitation is present in the accused product or process, there is no infringement.

12. With respect to construing claims, I understand that claim construction is an issue of law that the Court decides by interpreting claim terms as they would have been understood by a POSITA at the time of the invention. Under this standard, I understand that courts consider the specification, the prosecution history, and any extrinsic evidence regarding how a POSITA would interpret the claims in view of the intrinsic record. For purposes of my analysis in this case, I have interpreted the claims under this standard. I understand that a different standard, referred to as the broadest reasonable interpretation ("BRI"), has been applied in other forums, such as in an IPR proceeding. My opinions regarding the terms below may differ under the BRI standard.

13. I also understand that if literal infringement cannot be established because one or more elements are not literally present in an accused product or process, a product or process may nevertheless be found to infringe under the doctrine of equivalents ("DOE"). For infringement under DOE, I understand that each accused product or process must contain an element at least equivalent to each and every limitation of the asserted claim. I also understand that one may, but is not required to, use the "function-way-result" test to determine equivalence. Under the function-way-result test, I understand that an inquiry is made into whether the accused product or service performs substantially the same function in substantially the same way to achieve the substantially same result as the claim element.

V. STATE OF THE ART

14. A "hashing function" is a mathematical operation that has been well-known since at least since the 1970s. *See, e.g.*, Ex. 17 at, *e.g.*, 507-08.[1] At its most generic level, a hashing function is a mathematical operation used to deterministically map an input to an output of a given size, known as a "hash." Typically, hashing functions are designed to minimize "collisions," meaning that each input ideally hashes to a unique output. Additionally, in computer security applications, hash functions are generally expected to be non-invertible, meaning that it is computationally impractical to determine an input given only the corresponding hash. One corollary of this non-invertible property is that minor changes to an input produce drastically different hashes.

15. Several hashing functions were well-known known by the 1990s, including the MD5 and SHA1 hashing functions. *See, e.g.*, U.S. Patent No. 5,638,446 (filed Aug. 28, 1995) at 4:59-61 ("a one-way hash function known in the art as MD-5 (Rivest, R., 'The md5 message digest algorithm', RFC 1321 (April 1992)"); U.S. Patent No. 5,815,709 (filed Apr. 23, 1996) at 7:39-40 ("Secure hashing algorithms such as the NISTA SHA . . . "). Another common hashing function is SHA256, developed by the U.S. National Security Agency, just like SHA1.

16. All of these hashing functions were generally designed to perform the same function as described above. The table below shows the MD5 Hash result for the words "Example" and "example," which produce entirely different hashes even though the change in the input is relatively minor:

Input	MD5 Hash
Example	0a52730597fb4ffa01fc117d9e71e3a9
example	1a79a4d60de6718e8e5b326e338ae533

The table below illustrates that, even though different hashing functions may have similar functions and properties, their results can differ dramatically. I have compared the hash of the same input—the word "Example"—to two different hashing functions, the MD5 and SHA256:

[1] Citations to "Ex. __" refer to the Exhibits attached to the Declaration of Rebecca Carson.

Hashing Function	Hash of "Example"
MD5	0a52730597fb4ffa01fc117d9e71e3a9
SHA256	d029f87e3d80f8fd9b1be67c7426b4cc1ff47b4a9d0a8461c826a59d8c5eb6cd

17. The table below shows the MD5 hash of the terms "Te," "st," and "Test":

Input	MD5 Hash
Te	2408730ad248ad4e4aa36fb14f5e0631
st	627fcdb6cc9a5e16d657ca6cdef0a6bb
Test	0cbc6611f5540bd0809a388dc95a615b

As illustrated by this table, the hashes for "Te" and "st" cannot be combined to recreate the hash of "Test"—i.e., the hash of the combination of the component inputs ("Test") is different from the hashes of the components themselves ("Te" and "st"), and one cannot determine the hash of the combination by simply combining the hashes of the components.

18. The useful properties of hashing functions led to their routine use in a number of different ways in computer science and security, including data integrity, authentication, and data fingerprinting (e.g., antivirus checks). With respect to authentication, for example, publication of a file's hash allowed a user who downloaded the file to independently confirm that the file was downloaded correctly. If the hash of the file as calculated by the user did not match the published hash, then there had obviously been some error or other issue in transmission. *See, e.g.*, U.S. Patent No. 5,638,446 at Abstract (teaching a process of using hashes wherein "If these two hash's match, then the user is assured that the file did originate with the author and is uncorrupted").

19. In light of the authentication use case described above, the benefit of using a hash as a file's ID was well-known before the earliest claimed priority date of the '780 patent. In fact, the benefits of using a hash as a file's ID were so well-known that hash identifiers were proposed as a candidate Uniform Resource Name as the Internet was being developed. *See* Ex. 16 at 5-6.

20. Using a hash ID for "fingerprinting" was also well-known, particularly with respect to antivirus analyzers that would typically compare a file's unique hash (hence "fingerprint) to a list of hashes for known malware. *See, e.g.*, U.S. Patent No. 5,685,875 (filed Oct. 21, 1994) at

DOCKET ALARM

Explore Litigation Insights

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

Real-Time Litigation Alerts

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

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

Advanced Docket Research

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

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

Analytics At Your Fingertips

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

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

API

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

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

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

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.