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 for Summary Judgment Regarding Claim 1 of U.S. Patent No. 6,804,780 Patent ("Motion") against Finjan, Inc. ("Finjan").

3. I understand that Finjan has accused Juniper of infringing claims 1 and 9 of U.S. Patent No. 6,804,780 ("the '780 Patent"). *See* First Amended Complaint (Dkt. No. 88) ¶ 64. I further understand that Juniper's Motion is directed to claim 1 of the '780 Patent ("Claim 1"). As discussed in detail below, it is my opinion that Juniper does not infringe Claim 1.

II. BACKGROUND AND QUALIFICATIONS

4. 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.

5. I provide below an overview of my background and qualifications. 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.

A. Education & Career

6. I received my Ph.D. in Computer Science and Engineering from the University of Michigan, Ann Arbor in 1994, with a specialty in computer security and cryptographic protocols. My thesis was titled "Nonmonotonic Cryptographic Protocols" and concerned authentication in long-running networking operations.

7. I am currently employed as Professor of Computer Science at Johns Hopkins University, where I perform research, teach graduate courses in computer science and related subjects, and supervise the research of Ph.D. candidates and other students. Courses I have

taught include Security and Privacy in Computing and Advanced Topics in Computer Security. I am also the Technical Director of the Johns Hopkins University Information Security Institute, the University's focal point for research and education in information security, assurance, and privacy. The University, through the Information Security Institute's leadership, has been designated as a Center of Academic Excellence in Information Assurance by the National Security Agency and leading experts in the field. The focus of my work over my career has been computer security, and my current research concentrates on systems and networking security, with special attention to software and network security.

8. After receiving my Ph.D., I began working at Bellcore in its Cryptography and Network Security Research Group from 1994 to 1996. During this period I focused my work on Internet and Computer Security. While at Bellcore, I published an article titled "Blocking Java Applets at the Firewall" about the security challenges of dealing with JAVA applets and firewalls, and a system that we built to overcome those challenges.

9. In 1997, I moved to AT&T Labs, Secure Systems Research Department, where I continued to focus on Internet and computer security. From 1995 through 1999, in addition to my work in industry, I served as Adjunct Professor at New York University, where I taught undergraduate classes on computer, network and Internet security issues.

10. I stayed at AT&T until 2003, when I left to accept a full time academic position at Johns Hopkins University. I was promoted to full professor with tenure in April, 2004.

11. I serve, or have served, on a number of technical and editorial advisory boards. For example, I served on the Editorial and Advisory Board for the International Journal of Information and Computer Security. I also served on the Editorial Board for the Journal of Privacy Technology. I have been Associate Editor of IEEE Security and Privacy Magazine, and served as Associate Editor of ACM Transactions on Internet Technology. I am currently an Associate Editor of the journal Communications of the ACM. I was an Advisory Board Member of Springer's Information Security and Cryptography Book Series. I have served in the past as a member of the DARPA Information Science and Technology Study Group, a member of the Government Infosec Science and Technology Study Group of Malicious Code, a member of the

AT&T Intellectual Property Review Team, Associate Editor of Electronic Commerce Research Journal, Co-editor of the Electronic Newsletter of the IEEE Technical Committee on Security and Privacy, a member of the board of directors of the USENIX Association, the leading academic computing systems society, and a member of the editorial board of the Bellcore Security Update Newsletter.

12. I have spoken on information security and electronic privacy issues at more than 50 seminars and symposia. For example, I presented keynote addresses on the topics "Security of Electronic Voting" at Computer Security 2004 Mexico in Mexico City in May 2004; "Electronic Voting" to the Secure Trusted Systems Consortium 5th Annual Symposium in Washington DC in December 2003; "Security Problems on the Web" to the AT&T EUA Customer conference in March, 2000; and "Security on the Internet" to the AT&T Security Workshop in June 1997. I also presented a talk about hacking devices at the TEDx conference in October 2011 and also another TEDx talk on the same topic in September 2015.

13. I was founder and President of Independent Security Evaluators (ISE), a computer security consulting firm, from 2005-2011. In that capacity, I guided ISE through the qualification as an independent testing lab for Consumer Union, which produces Consumer Reports magazine. As an independent testing lab for Consumer Union, I managed an annual project where we tested all of the popular anti-virus products. Our results were published in Consumer Reports each year for three consecutive years.

14. I am currently the founder and managing partner of Harbor Labs, a software and networking consulting firm.

B. Publications

15. I am a named inventor on ten U.S. patents in the information security area.

16. I have also testified before Congress regarding the security issues with electronic voting machines and in the U.S. Senate on the issue of censorship. I also testified in Congress on November 19, 2013 about security issues related to the government's Healthcare.gov web site.

17. I am author or co-author of five books regarding information security issues: *Brave New Ballot,* Random House, 2006; *Firewalls and Internet Security* (second edition),

Addison Wesley, 2003; *White-Hat Security Arsenal*, Addison Wesley, 2001; *Peer-to-Peer*, O'Reilly, 2001; and *Web Security Sourcebook*, John Wiley & Sons, 1997. I am also the author of numerous journal and conference publications, which are reflected in my CV.

III. MATERIALS CONSIDERED

18. 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 prosecution file history (including IPRs); (c) Finjan's Infringement Contentions (Exhibits B-1 and B-2); (d) the deposition transcripts of the Juniper engineers deposed in this matter, and (e) the other documents and references cited herein (not limited to the excerpt attached submitted with Juniper's Motion). I have also reviewed the Declaration of Yuly Nerida Becerra Tenorio and spoken with Raju Manthena, Principal Engineer at Juniper, about the accused products.

IV. LEGAL STANDARDS

19. 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.

20. 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 hypothetical POSITA. This level of skill is approximate and my opinion would not change if a somewhat lower or higher level of skill were adopted.

21. 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.

22. 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, I understand that once the scope of the asserted claims has

been determined, 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. For method claims, I understand that one infringes by performing each and every step in the patented method.

23. 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. For infringement under the doctrine of equivalents, 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

24. A "hashing function" is a mathematical operation that has been well-known since at least since the 1970s. *See, e.g.*, Ex. 13 at, *e.g.*, 507-08.[1] At its most generic level, a hashing function is 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 hashes to a unique output. Additionally, in computer science applications, hash functions are 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.

25. 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

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

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.