Paper No. __________
Filed March 14, 2014

Filed on behalf of:
By: James C. Yoon
Matthew A. Argenti
WILSON SONSINI GOODRICH & ROSATI
650 Page Mill Road
Palo Alto, California 94304
Tel.: 650-493-9300
Fax: 650-493-6811
Email: jyoon@wsgr.com
Email: margenti@wsgr.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Groupon Inc.
Petitioner

v.

Maxim Integrated Products, Inc.
Patent Owner

Patent No. 5,805,702

DECLARATION OF PAUL C. CLARK, DSc.

Table of Contents

I, Paul C. Clark, DSc., declare as follows:

1. The following declaration is based on my personal knowledge and all facts and statements contained herein are true and accurate to the best of my knowledge, information and belief.

2. In preparing this declaration, I have reviewed U.S. Patent No. 5,805,702 (hereinafter "the '702 patent") (submitted as Ex. 1001), the prosecution history to date and cited references. I have also relied upon my personal knowledge and experience of over 30 years. My curriculum vitae is attached as Appendix A, and also as Exhibit 1003.

I. QUALIFICATIONS

3. I earned a Bachelor of Science in Mathematics from the University of California, Irvine in 1986. In 1988, I earned a Master of Science in Electrical Engineering and Computer Science from the University of Southern California. In 1994, I earned my Doctorate of Science in Computer Science with a concentration in Security, Graphics, and Intellectual Property Law from The George Washington University.

4. I am currently the President and Chief Technology Officer of SecureMethods Inc. and Paul C. Clark LLC. in Bethesda, Maryland. I have held this position for over 14 years. In these roles, I serve as managing director where I manage the operation, sales, and commercial product development staff. SecureMethods provides a comprehensive scalable, COTS-based secure architecture, implemented through the use of the SM Gateway. The SM Gateway is a next-generation security appliance developed by SecureMethods that is available on UNIX-based platforms using commercial, government, and Type I cryptography, implemented in both hardware and software. In my capacity as President and Chief Technology Officer of SecureMethods, I have technical and

operational oversight of all projects and corporate technical operations. I provide guidance to senior technical personnel relating to design, implementation, and troubleshooting for a wide range of systems both internal and external. My work includes network systems and security, cryptographic applications, certification, key management, authentication, and integrity strategies for network applications. I also provide a wide range of high end technical and legal consulting services. My firm specializes in complex software and hardware systems for commercial and Department of Defense ("DoD") clients.

5. Prior to SecureMethods, Inc., I was a Chief Scientist at DynCorp Networks Solutions from 1995 to 1999, where I designed and deployed the next generation of architecture for high volume network database and storage systems for customers such as the DoD.

6. Prior to my tenure at DynCorp, I was a Senior Security Engineer at Trusted Information Systems, where I was involved in the implementation of Privacy Enhanced Mail (PEM) with public and secret key encryption, NIST's Smartcard API (SCAPI) which incorporated cryptographic operations for PEM, among other encryption-related technological and product development. I also designed and implemented high assurance security systems, including trusted operating systems and applications for the NSA and the defense Advanced Research Projects Agency ("DARPA"). My work at Trusted Information Systems involved cryptography, multilevel operating systems, smartcards, and other security technologies.

7. From 1989 to September 1990, as more fully set forth in my curriculum vitae, I worked as a Technical Lead at GTE Government Systems. While at GTE, I designed and implemented network and load generators for OS/2 LAN Manager to measure network performance load metrics for the Central

Intelligence Agency ("CIA"). I also developed X Windows interfaces for a large-scale event-driven network system for the NSA.

8. From 1985 to 1989, I worked as a Systems Engineer at Ultrasystems Defense and Space. As more fully set forth in my curriculum vitae, at Ultrasystems I designed and implemented large-scale simulation and network-based systems for the United States Department of Defense ("DoD"). A high-speed database server I designed and implemented was used for realtime intelligence collection by the National Security Agency ("NSA").

9. In addition, I am currently an Adjunct Professor in the Electrical Engineering and Computer Science Department at The George Washington University where I teach doctoral level cryptography and computer security courses.

10. I was also a member of the Federal Advisory Committee for Key Management Infrastructure (KMI) and was Chairman of the Interoperability Working Group for Cryptographic Key Recovery from approximately 1996 to 1998. I also served as a Cooperative Research and Development Agreements (CRADA) partner to bring development of elements of a Public Key Infrastructure (PKI) through combined efforts with the National Institute of Standards and Technology (NIST).

11. I have also been an invited speaker at a number of conferences including: the RSA Security Conference in 1994 where I presented on Random Number Threats to Cryptographic Systems and a Keynote Speaker for the Washington, D.C. Bar Association on Security for Networked computing environments.

12. Lastly, I have co-authored a number of publications in the computer and security areas. A representative list of my publications is included in my

DOCKET ALARM

Explore Litigation Insights

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

Real-Time Litigation Alerts

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

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

Advanced Docket Research

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

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

Analytics At Your Fingertips

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

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

API

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

LAW FIRMS

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

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

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

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

fastcase®
Smarter legal research.