DOCKET NO.: 1033300-00302US2
Filed on behalf of Apple Inc.
By: Monica Grewal, Reg. No. 40,056 (Lead Counsel)
Ben Fernandez Reg. No. 55,172 (Backup Counsel)
Wilmer Cutler Pickering Hale and Dorr LLP
60 State Street
Boston, MA 02109
Email: monica.grewal@wilmerhale.com
ben.fernandez@wilmerhale.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner,

v.

UNIVERSAL SECURE REGISTRY, LLC,

Patent Owner.

Case IPR2018-00809

U.S. Patent No. 9,530,137

DECLARATION OF DR. VICTOR SHOUP IN SUPPORT OF PETITION FOR *INTER* PARTES REVIEW

TABLE OF CONTENTS

I, Victor Shoup, Ph.D., declare as follows:

1. My name is Victor Shoup.

2. I have been retained by Apple to provide opinions in this proceeding relating to U.S. Patent 9,530,137 ("'137 patent").

I. BACKGROUND

3. I received a Bachelor of Science in Computer Science and Mathematics from the University of Wisconsin at Eau Claire in 1983. I received my Doctorate in Computer Science from the University of Wisconsin at Madison in 1989. I worked as a research scientist at Bellcore from 1995 to 1997 and at IBM Research Zurich from 1997 to 2002. My work included design of cryptographic protocols such as a new public key cryptosystem (now called the Cramer-Shoup cryptosystem) that achieved higher levels of security than were previously thought possible in a practical scheme.

4. I have been Professor of Computer Science at the Courant Institute of Mathematical Sciences at New York University since 2002 (initially as an Associate Professor, and as a Professor since 2007). I teach a variety of graduate and undergraduate courses on cryptography. Since 2012, I have also been a part-time visiting researcher at the IBM T. J. Watson Research Center in Yorktown, New York, where I collaborate with the Cryptography Research Group, which does work on a range of projects from the theoretical foundations of cryptography

to the design and implementation of cryptographic protocols, such as homomorphic encryption.

5. My areas of research include cryptography and number-theoretic algorithms, and I have published over 60 papers in these areas. In the area of cryptography, I have made substantial contributions in the sub-areas of digital signatures, public key encryption, hash functions, distributed computation, session key exchange, and secure anonymous transactions.

6. I was also an editor of the ISO18033-2 standard for public-key encryption, which was published in 2006.

7. I have been on the program committee of numerous international conferences on cryptography, and was the Program Chair at Crypto 2005 (Crypto is the premier international conference on cryptography). I have also acted as a consultant on cryptographic protocols for several companies.

8. In recognition of my contributions to the field of cryptography, I was named a Fellow of the International Association for Cryptographic Research (IACR) in 2016, for fundamental contributions to public-key cryptography and cryptographic security proofs, and for educational leadership.

9. I have given a number of invited lectures on my research in cryptographic protocol design. In 2005, I published a textbook on the mathematical underpinnings of cryptography titled *A Computational Introduction*

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.