

**UNITED STATES PATENT AND TRADEMARK OFFICE**

---

**BEFORE THE PATENT TRIAL AND APPEAL BOARD**

---

APPLE INC.  
*Petitioner,*

v.

UNIVERSAL SECURE REGISTRY LLC  
*Patent Owner*

---

Case IPR2018-00811  
U.S. Patent No. 8,856,539

---

**PATENT OWNER'S EXHIBIT 2001  
DECLARATION OF MARKUS JAKOBSSON  
IN SUPPORT OF PATENT OWNER'S PRELIMINARY RESPONSE**

1. I have been retained on behalf of Universal Secure Registry LLC (“Patent Owner”) in connection with the above-captioned *inter partes* review (IPR). I have been retained to provide my opinions in support of USR’s Preliminary Response. I am being compensated for my time at the rate of \$625 per hour. I have no interest in the outcome of this proceeding.

2. In preparing this declaration, I have reviewed and am familiar with the Petition for IPR2018-00811, U.S. Patent No. 8,856,539, and its file history, and all other materials cited and discussed in the Petition (including the declaration of Dr. Victor Shoup) and cited and discussed in this Declaration. I understand the Petition asserts that claims 1-3, 5-8, 16-24, 26-30, 37, and 38 are anticipated by European Patent Application 1,028,401 A2 (Ex. 1030, “Schutzer”) under 35 U.S.C. § 102, and claims 12, 31, and 34 are obvious in view of Schutzer under 35 U.S.C. § 103 (together “the Challenged Claims”).

3. The statements made herein are based on my own knowledge and opinion. This Declaration represents only the opinions I have formed to date. I may consider additional documents as they become available or other documents that are necessary to form my opinions. I reserve the right to revise, supplement, or amend my opinions based on new information and on my continuing analysis.

## I. QUALIFICATIONS

4. My qualifications can be found in my Curriculum Vitae, which includes my detailed employment background, professional experience, and list of technical publications and patents. Ex. 2002.

5. I am currently the Chief of Security and Data Analytics at Amber Solutions, Inc, a cybersecurity company that develops home and office automation technology. At Amber, my research studies and addresses abuse, including social engineering, malware and privacy intrusions. My work primarily involves identifying risks, developing protocols and user experiences, and evaluating the security of proposed approaches.

6. I received a Master of Science degree in Computer Engineering from the Lund Instituted of Technology in Sweden in 1993, a Master of Science degree in Computer Science from the University of California at San Diego in 1994, and a Ph.D. in Computer Science from the University of California at San Diego in 1997, specializing in Cryptography. During and after my Ph.D. studies, I was also a Researcher at the San Diego Supercomputer Center, where I did research on authentication and privacy.

7. From 1997 to 2001, I was a Member of Technical Staff at Bell Labs, where I did research on authentication, privacy, multi-party computation, contract exchange, digital commerce including crypto payments, and fraud detection and

prevention. From 2001 to 2004, I was a Principal Research Scientist at RSA Labs, where I worked on predicting future fraud scenarios in commerce and authentication and developed solutions to those problems. During that time I predicted the rise of what later became known as phishing. I was also an Adjunct Associate Professor in the Computer Science department at New York University from 2002 to 2004, where I taught cryptographic protocols.

8. From 2004 to 2016, I held a faculty position at the Indiana University at Bloomington, first as an Associate Professor of Computer Science, Associate Professor of Informatics, Associate Professor of Cognitive Science, and Associate Director of the Center for Applied Cybersecurity Research (CACR) from 2004 to 2008; and then as an Adjunct Associate Professor from 2008 to 2016. I was the most senior security researcher at Indiana University, where I built a research group focused on online fraud and countermeasures, resulting in over 50 publications and two books.

9. While a professor at Indiana University, I was also employed by Xerox PARC, PayPal, and Qualcomm to provide thought leadership to their security groups. I was a Principal Scientist at Xerox PARC from 2008 to 2010, a Director and Principal Scientist of Consumer Security at PayPal from 2010 to 2013, a Senior Director at Qualcomm from 2013 to 2015, and Chief Scientist at Agari from 2016 to 2018. Agari is a cybersecurity company that develops and

commercializes technology to protect enterprises, their partners and customers from advanced email phishing attacks. At Agari, my research studied and addressed trends in online fraud, especially as related to email, including problems such as Business Email Compromise, Ransomware, and other abuses based on social engineering and identity deception. My work primarily involved identifying trends in fraud and computing before they affected the market, and developing and testing countermeasures, including technological countermeasures, user interaction and education.

10. I have founded or co-founded several successful computer security companies. In 2005 I founded RavenWhite Security, a provider of authentication solutions, and I am currently its Chief Technical Officer. In 2007 I founded Extricatus, one of the first companies to address consumer security education. In 2009 I founded FatSkunk, a provider of mobile malware detection software; I served as Chief Technical Officer of FatSkunk from 2009 to 2013, when FatSkunk was acquired by Qualcomm and I became a Qualcomm employee. In 2013 I founded ZapFraud, a provider of anti-scam technology addressing Business Email Compromise, and I am currently its Chief Technical Officer. In 2014 I founded RightQuestion, a security consulting company.

11. I have additionally served as a member of the fraud advisory board at LifeLock (an identity theft protection company); a member of the technical

# 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.