IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE, INC.,
Petitioner,

v.

PROXENSE, LLC
Patent Owner

Case No. IPR2025-00075 (joined with IPR2024-00783)
U.S. Patent No. 9,679,289

DECLARATION OF MARKUS JAKOBSSON, PH.D

I. INTRODUCTION AND SCOPE OF ENGAGEMENT

1. My name is Markus Jakobsson. I have been retained by counsel for Patent Owner Proxense, LLC ("Proxense") to provide my opinions regarding whether claims of U.S. Patent Nos. 9,679,289 (hereafter the "289 Patent") and 10,073,960 (hereafter the "960 Patent) recite terms understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure enabling an application, function or service, absent an algorithm disclosed in the Specifications of the respective patents.

II. QUALIFICATIONS AND COMPENSATION

2. I make this Declaration based upon my own personal knowledge, information, and belief, and I would and could competently testify to the matters set forth in this Declaration if called upon to do so.

3. Attached hereto as **Appendix A** is a true and correct copy of my Curriculum Vitae (CV). I am being compensated at the rate of $875 per hour for my time, plus reasonable out-of-pocket expenses. My compensation does not depend upon the outcome of the IPR proceedings, the contents of this Declaration, any testimony that I may provide, or the ultimate outcome of this litigation.

4. I am currently the Chief Scientist at Artema Labs, a crypto startup concerned with the security and confidentiality of digital representations of ownership. My research relates to how to make online transfers of ownership secure against abuses of various types, among other things.

5. I have founded or co-founded several successful computer security companies. I am the CEO at ZapFraud, a cybersecurity company that develops techniques to detect deceptive emails, such as Business Email Compromise emails. At ZapFraud, 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 am also the founder of Carbyne Biometrics, a biometric authentication company; Secure Technology, a target advertising company; RavenWhite Security, a device authentication company; FatSkunk, a mobile malware detection company (acquired by Qualcomm in 2013); Extricatus, a security consulting company (now defunct); CSExpert, a security consulting company; and RightQuestion, a telecom security company.

7. I received a Master of Science degree in Computer Engineering from the Lund Institute 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.

8. 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.

9. 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.

10. 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, Chief Scientist at Agari from 2016 to 2018, Chief of Security and Data Analytics at Amber Solutions from 2018 to 2020, and Chief Scientist at ByteDance from 2020 to 2021.

11. 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.

12. Amber Solutions is a cybersecurity company that develops home and office automation technologies. At Amber Solutions, my research addressed confidentiality, user interfaces and authentication techniques in the context of ubiquitous and wearable computing, and involved the tracking of users, for purposes of personalization and emergency response, using wireless technologies such as Bluetooth and Bluetooth Low Energy (BLE).

13. ByteDance is a media company concerned with secure processing of data, and is the owner of TikTok. At ByteDance, my research addressed fraud prevention, confidentiality, user interfaces and authentication techniques in the context of the many products offered by ByteDance.

14. I have additionally served as a member of the fraud advisory board at LifeLock (an identity theft protection company); a member of the technical advisory board at CellFony (a mobile security company); a member of the technical advisory board at PopGiro (a user reputation company); a member of the technical advisory board at MobiSocial dba Omlet (a social networking company); and a member of the technical advisory board at Cequence Security (an anti-fraud company, previously named Stealth Security). I have provided anti-fraud consulting to KommuneData (a Danish government entity), J.P. Morgan Chase, PayPal, Boku, and Western Union.

15. I have authored six books and over 100 peer-reviewed publications, and have been a named inventor on over 300 patents and patent applications.

16. My work has included research in the area of applied security, mobile security, cryptographic protocols, authentication, malware, social engineering, usability and fraud.

17. I have been engaged as a technical expert in over 75 computer-related cases, including numerous cases involving Internet security, mobile security, encryption and/or authentication.

III. SUMMARY OF OPINIONS

18. As discussed in detail below, I do not believe the terms "RDC communicating wirelessly with [] at least one external device within [a] proximity zone", "integrated, wireless communication interface communicating wirelessly with [] at least one external device within [a] proximity zone", "local, secured information stored by [] integrated, secure memory", and "enablement signal" are understood by person of ordinary skill in the art to have a sufficiently

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.