

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.,

Petitioner,

v.

TELCOM VENTURES LLC,

Patent Owner.

Case No. IPR2025-00977

U.S. Patent 11,770,756

DECLARATION OF CHUCK EASTTOM

TABLE OF CONTENTS

I. INTRODUCTION 1

II. QUALIFICATIONS 2

III. MATERIALS CONSIDERED 6

IV. SCOPE OF OPINIONS 6

V. RELATED DISTRICT COURT CASE 7

VI. LEGAL STANDARDS 9

 A. Claim Construction..... 10

 B. Obviousness..... 11

 C. Motivations to Combine..... 13

VII. LEVEL OF ORDINARY SKILL IN THE ART 14

VIII. CLAIM CONSTRUCTION 15

IX. TECHNOLOGY BACKGROUND..... 16

 A. Near Field Communications (“NFC”) 16

 B. Session Initiation Protocol (“SIP”) 18

X. U.S. PATENT NO. 11,770,756 (“’756 Patent”) (Ex. 1001) 19

 A. Priority Date 19

 B. ’756 Patent Overview 20

 C. The ’756 Patent’s Prosecution History 21

XI. ASSERTED REFERENCES 22

 D. Jain (Ex. 1017) 22

 E. Dua (Ex. 1018) 29

- XII. THE CHALLENGED CLAIMS OF THE '756 PATENT WOULD NOT HAVE BEEN OBVIOUS.....33
 - A. Petitioner’s Ground 1 Fails Because The Claims Would Not Have Been Obvious In View Of Jain.....33
 - 1. Jain Does Not Disclose or Render Obvious “a method of operating a device.”.....33
 - 2. Jain Does Not Disclose or Render Obvious “responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion, enabling by the device a number of functions of the device and disabling by the device a function of the device.”.....42
 - 3. Jain Does Not Disclose or Render Obvious “responsive to the requesting, receiving by the wireless device from the second device the authorization to enable the function for conducting the financial transaction”47
 - 4. Jain Does Not Disclose or Render Obvious “responsive to the wireless device satisfying a proximity condition relative to an entity”51
 - B. Petitioner’s Ground 2 Fails Because The Claims Would Not Have Been Obvious In View Of Dua.....53
 - 1. Dua Does Not Disclose or Render Obvious “responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion, enabling by the device a number of functions of the device.”.....54
 - a. Dua’s “Card-Issuing” Theory Fails55
 - b. Dua’s “External-Storage-Authentication” Theory Fails.....59
 - 2. Dua Does Not Disclose or Render Obvious “responsive to the wireless device satisfying a proximity condition relative to an entity.”61

XIII. SUMMARY AND OTHER REMARKS67

Table of Exhibits

Exhibit No.	Description
2001	Interim Processes for PTAB Workload Management, Acting Director Memorandum (March 26, 2025)
2002	FAQs for Interim Processes for PTAB Workload Management
2003	EDTX Litigation Second Amended Docket Control Order (Jan. 29, 2025)
2004	Docket Navigator Statistics for Judge Rodney Gilstrap
2005	Samsung’s Preliminary Invalidation Contentions (Feb. 3, 2025)
2006	Exhibit 756-C (Samsung’s Subject Matter Eligibility Contentions)
2007	Telcom Ventures Complaint for Patent Infringement
2008	Non-Final Office Action, Application No. 17/730,174
2009	Declaration of Dr. Chuck Easttom
2010	<i>Curriculum Vitae</i> of Dr. Chuck Easttom
2011	Chiradeep BasuMallick, “What is NFC (Near Field Communication)? Definition, Working, and Examples” (Sept. 29, 2022), https://www.spiceworks.com/tech/networking/articles/what-is-near-field-communication/
2012	Liu et al., “Near-Field Communications: A Comprehensive Survey,” IEEE (June 2025)
2013	“The Creation of the NFC Forum and its Vision” (2011) https://cs.stanford.edu/people/eroberts/courses/cs181/projects/2010-11/NFCChips/nfcforum.html
2014	McHugh & Yarmey, “Near Field Communication: Introduction and Implication,” ERIC (2012)

2015	Coskun et al., “The Survey on Near Field Communication,” Sensors (June 5, 2015)
2016	“Cisco SIP IP Phone Administrator Guide, Release 7.5,” Cisco https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/7960g_7940g/sip/7_5/english/administration/guide/ver7_5/sipaxa75.pdf
2017	Rosenberg et al., RFC 3261 SIP: Session Initiation Protocol (June 2002), https://www.ietf.org/rfc/rfc3261.txt
2018	Schulzrinne et al., RFC 3550 RTP: A Transport Protocol for Real-Time Applications (July 2003), https://datatracker.ietf.org/doc/html/rfc3550
2019	Baughner et al., RFC 3711 The Secure Real-time Transport Protocol (SRTP) (Mar. 2004), https://www.rfc-editor.org/rfc/rfc3711.html
2020	Kurose et al., Computer Networking: A Top Down Approach, Chapter 7.4 (March 2012, 6th ed.) https://gaia.cs.umass.edu/kurose_ross/retired/protocols_real_time_interactive.pdf
2021	Rosenberg & Shockey, The Session Initiation Protocol (SIP): A Key Component for Internet Telephony, Computer Telephony, June 2000, at 124 https://gaia.cs.umass.edu/kurose_ross/retired/protocols_real_time_interactive.pdf
2022	Mealling & Daniel, RFC 2915 The Naming Authority Pointer (NAPTR) DNS Resource Record (Sept. 2000) https://www.cs.columbia.edu/sip/articles/SIP_tutorial_CT_Magazine_June2000.pdf
2023	Jeremy George, DNS Configuration, SIP.edu Cookbook (May 12, 2003), https://web.mit.edu/sip/sip.edu/dns.shtml
2024	Series E: Overall Network Operation, Telephone Service, Service Operation and Human Factors, International Telecommunication Union (Nov. 2010), https://www.itu.int/rec/t-rec-e.164-201011-i/en

I. INTRODUCTION

1. My name is Dr. Chuck Easttom, and I have been retained as a technical expert by counsel for Patent Owner Telcom Ventures LLC (“Telcom Ventures” or “Patent Owner”) to investigate and opine as to the validity of U.S. Patent No. 11,770,756 (“the ’756 Patent”) in view of Petitioner Samsung Electronics Co., Ltd.’s (“Petitioner” or “Samsung”) Petition for *Inter Partes* Review (the “Petition”) (Paper 1).

2. This declaration is based on information currently available to me. To the extent that additional information becomes available, I reserve the right to continue my investigation and study, and thus may expand or modify my opinions as my investigation and study continues. I may also supplement my opinions in response to any additional information that becomes available to me, any matters raised by Petitioner and/or opinions rendered by Petitioner’s experts, or in light of any relevant orders from the Board.

3. My opinions are based on my years of education, research and experience, as well as my investigation and study of relevant materials.

4. I am being compensated at the rate of \$550 per hour for my work in this case, including time spent testifying. I am also being reimbursed for reasonable fees and expenses, including hotel and travel expenses, incurred as a result of my work in this case. Neither I nor my company have received any additional compensation

for my work in this inter partes review. My compensation is not tied in any way to the substance of my testimony or the outcome of this Investigation. I have no other financial interest in this inter partes review or to the parties. I am available to offer these opinions at deposition and at trial if called upon to do so.

II. QUALIFICATIONS

5. I have summarized in this section my educational background, work experience, and other relevant qualifications. A true and correct copy of my *curriculum vitae* is attached as Ex. 2010 to Patent Owner's Preliminary Response which includes a list of all other cases in which, during the previous four years, I have testified at trial or by deposition.

6. I have over thirty years of experience in the computer science industry including extensive experience with computer security, mobile devices, and related topics. I have authored forty-five computer science books, including books on mobile devices and on cryptography. I also have authored over eighty research papers and am an inventor with twenty-seven computer science patents.

7. I hold a Doctor of Science (D.Sc.) degree in Cyber Security from Capitol Technology University (Dissertation Topic: "A Comparative Study of Lattice Based Algorithms for Post Quantum Computing"). I also hold a Doctor of Philosophy (Ph.D.) in Technology focused on nanotechnology (Dissertation Topic: "The Effects of Complexity on Carbon Nanotube Failures") from Capitol

Technology University. I also have a Doctor of Philosophy (Ph.D.) in Computer Science from the University of Portsmouth (Dissertation Topic: “A Systematic Framework for Network Forensics Using Graph Theory”). I also hold four Master’s degrees—one in Applied Computer Science, one in Education, one in Defense and Strategic Studies, and one in Systems Engineering.

8. I am currently an Adjunct Lecturer for Georgetown University teaching graduate courses in requirements engineering, artificial intelligence, cybersecurity, and cryptography. I am also an adjunct for Vanderbilt University teaching graduate computer science courses in quantum computing, digital forensics, algorithms, and cybersecurity. I also developed a graduate course in digital forensics for the University of Dallas and taught that course from 2019 to 2022.

9. I am a Senior Member and Distinguished Speaker for the Association of Computing Machinery (“ACM”) and a Senior Member and Distinguished Visitor of the Institute for Electrical and Electronics Engineering (“IEEE”). The IEEE is the world’s largest and most preeminent engineering organization. Among other activities, the IEEE creates industry standards for a wide range of engineering disciplines, including software development. I am also a Distinguished Visitor of the IEEE. I have been involved in IEEE standards creation for several years.

10. I have extensive experience with smart cards, Near Field Communications (“NFC”), the ISO/IEC 7810 standard for identification cards, the

ISO/IEC 7816 standard for electronic cards for identification, the ISO/IEC 14443 standard for contactless integrated circuit cards, the EMV standard, and related standards and technologies.

11. I have worked with smart cards as an authentication method since the Department of Defense began using the Common Access Card in the early 2000s. Near Field Communications were covered in networking courses that I took as part of my second Master's degree and in some of the networking certifications I hold. I have also worked with NFC since at least 2005. Specific certifications I hold that are relevant to NFC and/or mobile devices include:

- Associate of Systems Engineering (ASEP) from INCOSE (International Council on Systems Engineering) 275062
- CompTIA Network + Certified COMP10163630
- CompTIA Network Infrastructure Professional – CNIP
COMP10163630
- EC Council Certified Security Administrator (ECSA) ECC947248
- EC Council Certified Encryption Specialist (ECES)
- CISSP – ISSAP – Certified Information Systems Architecture
Professional #387731
- CISSP – ISSEP Information Systems Security Engineering
Professional #387731

- Oxygen Phone Forensics Certified
- CompTIA Security+ COMP001021522764
- SC-300 - Microsoft Identity and Access Administrator

12. Specific publications that I have authored or participated in related to NFC, chip design, and/or mobile devices include the following:

- Easttom, C. (2005). Introduction to Computer Security. New York City, New York: Pearson Press.

- Easttom, C. & Dulaney, E. (2015). CompTIA Security+ Study Guide: SY0-401. Hoboken, New Jersey: Sybex Press.

- Easttom, C. & Roberts, R. (2018). Networking Fundamentals, 3rd Edition. Goodheart-Wilcox Publishing.

- Easttom, C. (2020). Modern Cryptography: Applied Mathematics for Encryption and Information Security 2nd Edition. New York City, New York: Springer Press.

- Easttom, C. (2021). An In-Depth Guide to Mobile Device Forensics. CRC Press.

- Easttom, C., Mei, N. (2019). Mitigating Implanted Medical Device Cybersecurity Risks. IEEE 10th Annual Computing and Communication Conference UEMCON.

- Easttom, C., Sanders, W. (2019). On the Efficacy of Using Android Debugging Bridge for Android Device Forensics. IEEE 10th Annual Computing and Communication Conference UEMCON.

13. I am qualified to render the opinions set forth herein. Under my definition of a POSITA or Dr. Almeroth's definition, set forth below, I am and was as of the priority date of the '756 Patent, at least one of ordinary skill in the art.

III. MATERIALS CONSIDERED

14. I have reviewed the '756 Patent, including the challenged claims, prosecution history, and relevant patent family. The '756 Patent was marked as Exhibit 1001, and its prosecution history was marked as Exhibit 1011.

15. I also reviewed the Petition, and each of Exhibits 1001-1047 attached to the Petition.

16. In forming my opinions, I have considered the materials listed above and any other documents cited in this declaration. I have also relied on my own education, knowledge, and experience in the relevant art.

17. I have also considered the understanding of a person of ordinary skill around the time of the invention of the '756 Patent.

IV. SCOPE OF OPINIONS

18. I set forth my opinions throughout this declaration.

19. I understand that Petitioner argues that claims 1-18 (the “Challenged Claims”) would have been obvious over U.S. Patent Application Publication No. 2009/0069049 (“Jain”) (Ground 1) and U.S. Patent Application Publication No. 2006/0165060 (“Dua”) (Ground 2).

20. I disagree. It is my opinion that the Challenged Claims of the ’756 Patent would not have been obvious in view of the asserted references, alone or in combination, for the reasons discussed herein.

V. RELATED DISTRICT COURT CASE

21. Patent Owner filed a complaint against Petitioner in the Eastern District of Texas, styled *Telcom Ventures LLC v. Samsung Electronics Co., Ltd. et al.*, Case No. 2:24-cv-00691-JRG (filed August 21, 2024).

22. I understand Patent Owner asserted a total of eight patents against Petitioner in that action: U.S. Patent Nos. 9,462,411, 9,832,708, 10,219,199, 10,674,432, 11,770,756, 11,924,743, 11,937,172, and 12,028,793.

23. I understand that a jury trial for the suit between Patent Owner and Petitioner is expected to begin on June 1, 2026. Ex. 2003 at 1.

24. I understand that Petitioner filed IPR petitions against all eight patents asserted by Patent Owner. These are:

- IPR2025-00957, regarding U.S. Patent No. 11,937,172
- IPR2025-00972, regarding U.S. Patent No. 10,219,199

- IPR2025-00973, regarding U.S. Patent No. 9,462,411
- IPR2025-00974, regarding U.S. Patent No. 10,674,432
- IPR2025-00975, regarding U.S. Patent No. 9,832,708
- IPR2025-00976, regarding U.S. Patent No. 11,924,743
- IPR2025-00977, regarding U.S. Patent No. 11,770,756 (the instant Petition)
- IPR2025-00978, regarding U.S. Patent No. 12,028,793

25. I also understand Patent Owner is asserting the '756 Patent against Apple Inc. in the Northern District of California, styled *Telcom Ventures LLC v. Apple Inc.*, Case No. 5:25-cv-05041 (filed October 4, 2024).

26. I understand Patent Owner asserted the same eight patents against Apple Inc. in that action.

27. I understand that Apple Inc. has filed IPR petitions against all eight patents asserted by Patent Owner. These are:

- IPR2025-01232, regarding U.S. Patent No. 9,462,411
- IPR2025-01233, regarding U.S. Patent No. 9,832,708
- IPR2025-01234, regarding U.S. Patent No. 10,219,199
- IPR2025-01235, regarding U.S. Patent No. 10,674,432
- IPR2025-01236, regarding U.S. Patent No. 11,770,756
- IPR2025-01237, regarding U.S. Patent No. 11,924,743

- IPR2025-01238, regarding U.S. Patent No. 11,937,172
- IPR2025-01239, regarding U.S. Patent No. 12,028,793

28. I understand Google LLC has filed IPR petitions against seven of the eight patents asserted by Patent Owner in the above litigations. These are:

- IPR2025-01349, regarding U.S. Patent No. 11,924,743
- IPR2025-01389, regarding U.S. Patent No. 11,937,172
- IPR2025-01401, regarding U.S. Patent No. 12,028,793
- IPR2025-01408, regarding U.S. Patent No. 9,832,708
- IPR2025-01409, regarding U.S. Patent No. 11,770,756
- IPR2025-01419, regarding U.S. Patent No. 10,219,199
- IPR2025-01421, regarding U.S. Patent No. 10,674,432

29. As of the signing of this declaration, I have been retained to provide an opinion in all eight IPRs filed by Petitioner against the patents asserted by Patent Owner. I have also been retained to provide an opinion in each of the IPRs filed by Apple Inc. and Google LLC.

VI. LEGAL STANDARDS

30. For purposes of this Declaration, I use the legal principles below as a guide in formulating my opinions. I am not an attorney, and I am not offering any opinions regarding legal matters; however, I have been informed by Telcom

Ventures' counsel of the legal principles relevant to the issues herein and have the following understanding.

31. In an *inter partes* review proceeding, I understand that a party seeking to invalidate a claim must prove invalidity by a preponderance of the evidence, which I understand to mean evidence that convinces someone that it is more likely than not that the particular proposition is true. I understand that the preponderance of the evidence standard applies to all aspects of an allegation of anticipation or obviousness, including the prior art status of the relevant reference(s).

A. Claim Construction

32. I understand the first step in determining whether a patent claim is valid is to properly construe the claims. I understand that the words of a claim are generally given their ordinary and customary meaning (sometimes referred to as their plain and ordinary meaning) as understood by a person of ordinary skill in the art at the time of the invention. I also understand that, as a general matter, a claim should not be limited to a preferred embodiment, but that in certain cases, the scope of the right to exclude may be limited by a narrow disclosure or by positions taken, such as by statements made during patent prosecution. I also understand the claims must be supported by the specification. Also, to the extent that a patent claims priority to an earlier filed application, the claims must be supported by the disclosure in that application. For terms that have not been construed, I understand that they

should be afforded their plain and ordinary meaning to one of ordinary skill in the art.

33. I understand that the plain and ordinary meaning of a claim term is the meaning that a person of ordinary skill in the art would have understood at the time of the effective date in view of the specification and the prosecution history.

B. Obviousness

34. I understand that a claimed invention is not patentable under 35 U.S.C. § 103 if the differences between the invention and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Obviousness, as I understand it, is based on the scope and content of the prior art, the differences between the prior art and the claim, the level of ordinary skill in the art, and objective indicia of non-obviousness to the extent they exist.

35. I understand that whether there are any relevant differences between the prior art and the claimed invention is to be analyzed from the perspective of a person of ordinary skill in the art at the time of the invention. A person of ordinary skill in the art is a hypothetical person who is presumed to be aware of all of the relevant art at the time of the invention. The person of ordinary skill is not an automaton, and may be able to fit together the teachings of multiple patents

employing ordinary creativity and the common sense that familiar items may have obvious uses in another context or beyond their primary purposes.

36. I understand that if a reference or proposed combination of references does not disclose or suggest all of the elements of a claim, the combination cannot render the claim obvious. I also understand that in order to combine prior art references to show obviousness, a person of ordinary skill in the art, without knowledge of the claimed invention, or without the use of hindsight, must have been motivated to combine the prior art by some suggestion or teaching in the prior art, the knowledge of one of skill in the art, or the nature of the problem to be solved.

37. I understand that an invention would have been obvious if a designer of ordinary skill in the art, facing the wide range of needs created by developments in the field, would have seen an obvious benefit to the solutions tried by the applicant. When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, it may have been obvious to a person of ordinary skill to try the known options. If a technique has been used to improve one device, and a person of ordinary skill in the art would have recognized that it would improve similar devices in the same way, using the technique may have been obvious. I understand, however, that routine experimentation does not necessarily preclude patentability.

38. I understand that obviousness of a patent claim cannot properly be established through hindsight, and that elements from different prior art references, or different embodiments of a single prior art reference, cannot be selected to create the claimed invention using the invention itself as a roadmap. I understand that the claimed invention as a whole must be compared to the prior art as a whole, and courts and the Board must avoid aggregating pieces of prior art through hindsight that would not have been combined absent the inventors' insight.

C. Motivations to Combine

39. I understand that, in deciding obviousness, it is appropriate to consider whether some teaching, suggestion, or motivation would have led a person of ordinary skill in the art to combine the invalidating references. I also understand that a reason to combine the teachings is needed even in a single-reference obviousness ground. I understand that there must be a showing of a suggestion or motivation to modify the teachings of that reference. I also understand that it is appropriate to look to a variety of factors when evaluating reasons to combine teachings or modify the teachings of a reference in an obviousness analysis, and that it is important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine or modify the prior art elements in the manner claimed. I understand that in determining obviousness, it may be helpful to consider whether there is some teaching, suggestion, or motivation to combine or modify teachings

and a reasonable expectation of success in doing so. I understand, however, that the teaching, suggestion, or motivation to combine inquiry is not required and may not be relied upon in lieu of the obviousness analysis outlined above. I understand that a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was independently known in the prior art. I also understand that this is so because inventions in most, if not all, instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known.

VII. LEVEL OF ORDINARY SKILL IN THE ART

40. I understand that patent claims are to be interpreted from the viewpoint of one of ordinary skill in the relevant art. To determine the level of skill that would be “ordinary,” I understand that a person of ordinary skill (“POSITA”) must generally have the capability of understanding the general principles that are applicable to the pertinent art.

41. In my opinion, a POSITA would have had at least a bachelor’s degree in electrical engineering, computer engineering, or a related field, with about two years of experience in wireless communications. More work or practical experience may qualify one not having the requisite education as a person with ordinary skill in the art while a higher level of education could offset less experience. I was at least a

person of ordinary skill in the art as of the effective filing dates of the Asserted Patents under this definition.

42. I have reviewed Dr. Almeroth's Declaration (Ex. 1002). I understand that Dr. Almeroth contends that a POSITA would have had "at least a Bachelor of Science in electrical engineering, computer engineering, or similar fields and at least two years of practical experience in the field of secure wireless communication applications." Ex. 1002 ¶ 79. I disagree that a POSITA should be required to have experience in secure wireless communications as Dr. Almeroth contends. The claims of the '756 Patent do not require that the communications be "secure" such as encryption or encoding of the wireless communications. *E.g.*, '756 Patent, cl. 1. I was at least a person of ordinary skill in the art as of the effective filing dates of the Asserted Patents under Dr. Almeroth's definition. Thus, I met the requirements of a POSITA under either my definition or Dr. Almeroth's definition as of the priority date of the '756 Patent.

VIII. CLAIM CONSTRUCTION

43. I understand that Petitioner contends the "[n]o express constructions are required to find the '756 patent claims invalid." Pet. at 7. Other than explaining the plain and ordinary meaning, which I do below, I do not offer an opinion on the correct construction of any disputed terms, because, in my opinion, the Challenged

Claims are not taught or suggested by the prior art. I reserve the right to respond to any future claim construction argument asserted by Petitioner or Dr. Almeroth.

IX. TECHNOLOGY BACKGROUND

44. Below, I provide a brief overview of the history of contactless smart cards, or proximity cards, and the use of the same technologies in devices.

A. Near Field Communications (“NFC”)

45. Near Field Communication (“NFC”) is a broad term for short-range wireless communication technology that allows devices to exchange data when they are brought very close together. It is an extension of Radio Frequency Identification (“RFID”) technology, designed for secure, quick, and convenient data transfer.

46. NFC-capable devices can communicate with other NFC-capable devices in either active or passive mode. In active mode, both devices generate their own radio frequency field to transmit data. Ex. 2011 at 4. In passive mode, one device generates the radio frequency field while the other responds without a power source. *Id.*

47. A paper by Liu et al. provides a history of NFC, stretching back to the first understanding of the wave theory of light. Ex. 2012 at 4. That paper includes an overview of NFC history which is shown here:

TABLE I: Timeline of NFC Milestones

1678	•	Huygens presented his “Wave Theory of Light”.
1801	•	Young presented the double-slit diffraction experiment.
1815	•	Fresnel presented a series of memoirs about his understanding of diffraction.
1821	•	Fraunhofer constructed the first diffraction grating.
1887	•	Hertz demonstrated the existence of radio waves.
1891	•	Lord Rayleigh calculated the Rayleigh distance $\frac{A^2}{2\lambda}$.
1947	•	Cutler <i>et al.</i> reformulated the Rayleigh distance as $\frac{2A^2}{\lambda}$.
1956	•	Polk calculated the Fresnel distance.
1983	•	The first patent on RFID-based NFC was granted.
1984	•	Winters formulated the initial theory of MIMO.
1994	•	The first patent on MIMO was granted.
1996	•	Foschini laid down crucial theoretical foundations for MIMO.
1999	•	Driessen and Foschini utilized a spherical wave-based model to characterize LoS MIMO.
2003	•	Jiang <i>et al.</i> proposed to use spherical wave-based models to describe short-range MIMO.
2010	•	Marzetta proposed the concept of massive MIMO.
2015	•	Channel measurement results on massive MIMO necessitated the use of a spherical wave-based channel model.
2016	•	Prather proposed the concept of holographic MIMO.
2017	•	Hu <i>et al.</i> re-showed the potential of large intelligent surfaces in enhancing wireless transmissions.
2018	•	Amiri <i>et al.</i> proposed the concept of ELAA.
2023	•	The first tutorial review of NFC was presented.

48. Despite the long history of the physics and technology supporting NFC, NFC itself is relatively new. For example, the NFC Forum was created in 2004 to ensure maximum compatibility across all implementations of NFC technology. Ex. 2013 at 1. But the NFC Forum was not even founded until many years after the first standards related to smart cards were published. As late as 2012, *see* Ex. 2014 at 1, and even 2015, some sources still referred to NFC as an “emerging technology.” Ex. 2015 at 1.

49. Within the umbrella of NFC, there are numerous individual standards that are more specific. One such standard is ISO/IEC 14443. The ISO/IEC 14443

standard has four parts. Part 1 defines the physical properties of the card (e.g., size, durability, environmental tolerance). Part 2 specifies how the card is powered by the RF field of the reader and how modulation/coding are done for transmitting and receiving signals. Part 3 describes card initialization and how multiple cards in the field are identified and selected (anti-collision protocol). Part 4 defines higher-level data exchange protocols, including how commands and responses are structured.

50. The specificity of individual NFC standards means that any such standard is self-sufficient. In other words, a POSITA consulting one of these standards, such as ISO/IEC 144443, would have a complete solution for near field communications and would not need to look to other standards or technologies.

B. Session Initiation Protocol (“SIP”)

51. One of the prior art grounds identified by Petitioner, Dua, makes extensive reference to Session Initiation Protocol. *E.g.*, Dua ¶[0042]. A brief background of that protocol is provided for reference.

52. The standard SIP is the Session Initiation Protocol is an Internet Engineering Task Force (“IETF”)-standardized application-layer protocol defined in RFC 3261. Ex. 2016 at 1. It sets forth standards for establishing, managing, and terminating real-time multimedia communication sessions over IP, including VoIP. It functions as a request-response protocol, similar to HTTP, and uses text-based messages to control calls involving voice, video, and other digital media.

53. RFC 3261 describes SIP technology as

an application-layer control protocol that can establish, modify, and terminate multimedia sessions (conferences) such as Internet telephony calls. SIP can also invite participants to already existing sessions, such as multicast conferences. Media can be added to (and removed from) an existing session. SIP transparently supports name mapping and redirection services, which supports personal mobility [27] - users can maintain a single externally visible identifier regardless of their network location.

Ex. 2017 at 5.

54. SIP itself does not transmit media (like voice or video). Instead, protocols such as Real-Time Transfer Protocol (“RTP”) and secure RTP (“sRTP”) are used to transmit data. Ex. 2018 at 1 (describing RTP); Ex. 2019 at 1 (describing sRTP).

X. U.S. PATENT NO. 11,770,756 (“’756 Patent”) (Ex. 1001)

A. Priority Date

55. Through a series of continuation applications, the ’756 Patent claims the benefit of U.S. Patent Application No. 12/264,711—later issued as U.S. Patent No. 9,462,411, which has a filing date of November 4, 2008.

56. I understand that Petitioner does not challenge this priority date for purposes of the Petition, and I have assumed that each of the challenged claims is entitled to a priority date of November 4, 2008. Pet. at 3.

B. '756 Patent Overview

57. The '756 Patent describes mobile wireless devices and methods of using a mobile wireless device to perform financial transactions, but only when certain conditions or criteria are met, such as the satisfaction of a proximity condition and a value of a parameter, e.g., a physiological parameter, satisfying a criterion. Ex. 1001, 1:25-30; 6:13-23. The specification recognizes that devices in the art were rigidly configured to perform a predetermined number of functions. *Id.*, 1:39-44. The '756 Patent addresses this rigidity problem by providing devices and methods that “may be used to enable adaptively one or more modes/functions of a device” based upon the satisfaction of certain criteria. *Id.*, 1:49-54. The specification explains that the invention advantageously allows “a mobile wireless device [to] act as a ‘wallet’ (over and above other functions) only when it is time to pay for an item and not act as a wallet when there is no need to do so.” *Id.*, 1:44-57.

58. The '756 Patent also describes estimating “a value of at least one other parameter that may be associated with the wireless communications device . . . and/or an entity (living or otherwise) that is associated with and/or is proximate to the wireless communications device.” *Id.*, 6:15-19. Such parameters include “velocity, acceleration, ToD, ToM, ToY, humidity, temperature, height, level of brightness, level of darkness, a blood pressure, a heart rate, a blood content, a physiological state, a psychological state, etc.” *Id.*, 6:20-23. These parameters can

be estimated using “sensors that may, according to some embodiments, be device-based and/or network assisted/based means and/or sensors.” *Id.*, 6:28-30. The disclosed wireless communications devices may be “configured to selectively enable the first communications mode/function” responsive to a value of such a parameter. *Id.*, 6:40-44.

C. The '756 Patent's Prosecution History

59. I have reviewed the prosecution history of the '756 Patent.

60. U.S. Patent Application No. 17/653,748 was filed March 7, 2022 and issued as U.S. Patent No. 11,770,756 on September 26, 2023.

61. In a non-final rejection, the Examiner rejected the claims as unpatentable under § 103 over U.S. Patent Application Publication No. 2009/0058637 in view of U.S. Patent Application Publication No. 2003/0172028 and for double patenting over claims 1, 7, and 17 of U.S. Patent No. 11,304,118. Ex. 1011 at 104, 106. Applicants then amended the independent claims to include “responsive to the value that is determined . . . enabling . . . a number of functions . . . and disabling a function” and filed a terminal disclaimer to traverse the rejections. *Id.* at 135–37. The Examiner allowed the claims of the '756 Patent following this amendment and filing of the terminal disclaimer. The Examiner stated in the Notice of Allowance that the closest prior art of record, U.S. Patent Application Publication No. 2009/0058637, alone or in combination failed to teach

or suggest “responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion, enabling by the device a number of functions of the device and disabling by the device a function of the device.” *Id.* at 207.

XI. ASSERTED REFERENCES

D. Jain (Ex. 1017)

62. United States Patent Application No. 2009/0069049 to Jain is titled “Interfacing Transaction Cards with Host Devices.” Jain was published on March 12, 2009 and filed on September 5, 2008. Jain focuses throughout on the functionality in a transaction card and independence from any particular mobile device to support transaction capabilities. One example is the following: “[f]or example, the transaction card 112 may execute a contactless transaction with the POS device 114 independent of the mobile device 110a.” Jain ¶[0023].

63. Figure 3 of Jain shows an exemplary transaction card.

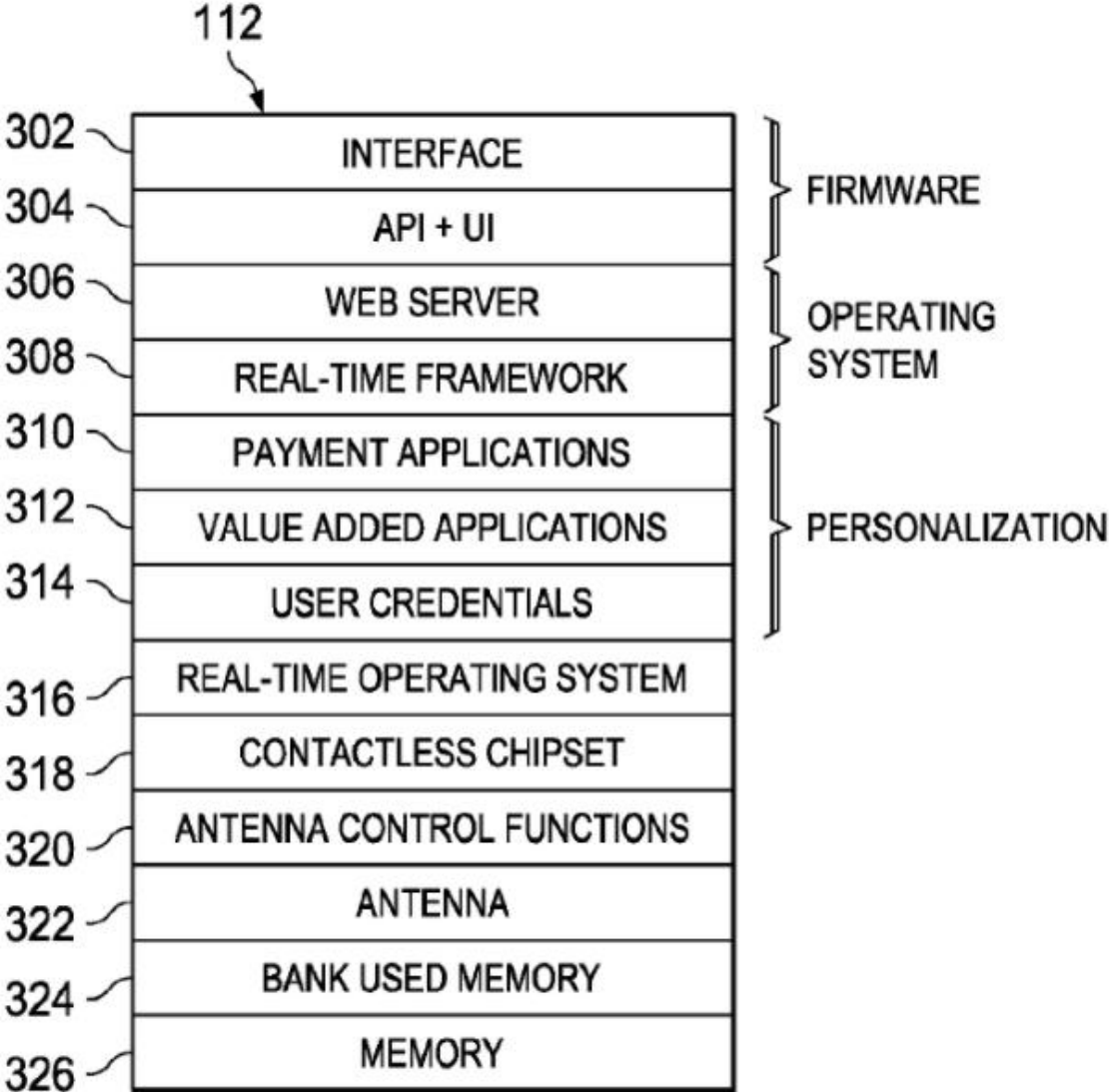


FIG. 3

Jain, Fig. 3; ¶¶[0009], [0049].

64. Jain focused on the relevant technology being in the transaction card so that the card could be used with a wide range of mobile devices. An example in Jain is the following: “[a]s used in this disclosure, the mobile devices 110 are intended to encompass cellular phones, data phones, pagers, portable computers, SIP phones,

smart phones, personal data assistants (PDAs), digital cameras, MP3 players, camcorders, one or more processors within these or other devices, or any other suitable processing devices capable of communicating information with the transaction card 112.” Jain ¶[0021].

65. Throughout multiple disclosures in Jain, the transaction card operates independently of any mobile host device. Jain, Abstract; ¶¶[0005], [0018], [0023], [0049], [0076]; cls. 1, 16. This approach allows Jain’s transaction card to interact with a wide range of mobile devices, and the mobile devices need not be altered in any way to support transactions.

66. Figure 1 of Jain explains how Jain’s transaction system functions using an intelligent card independent of any mobile device: “FIG. 1 is a block diagram illustrating an example transaction system 100 for wirelessly executing transactions using an intelligent card independent of a host device.” Jain ¶[0018].

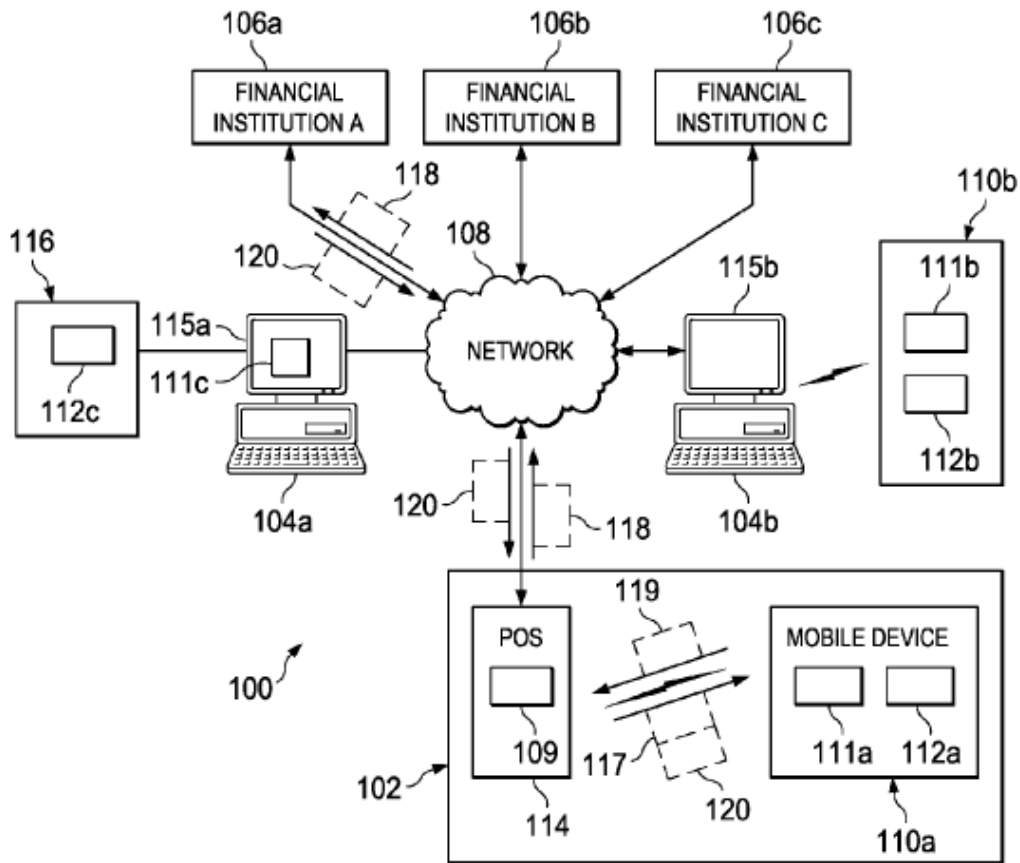


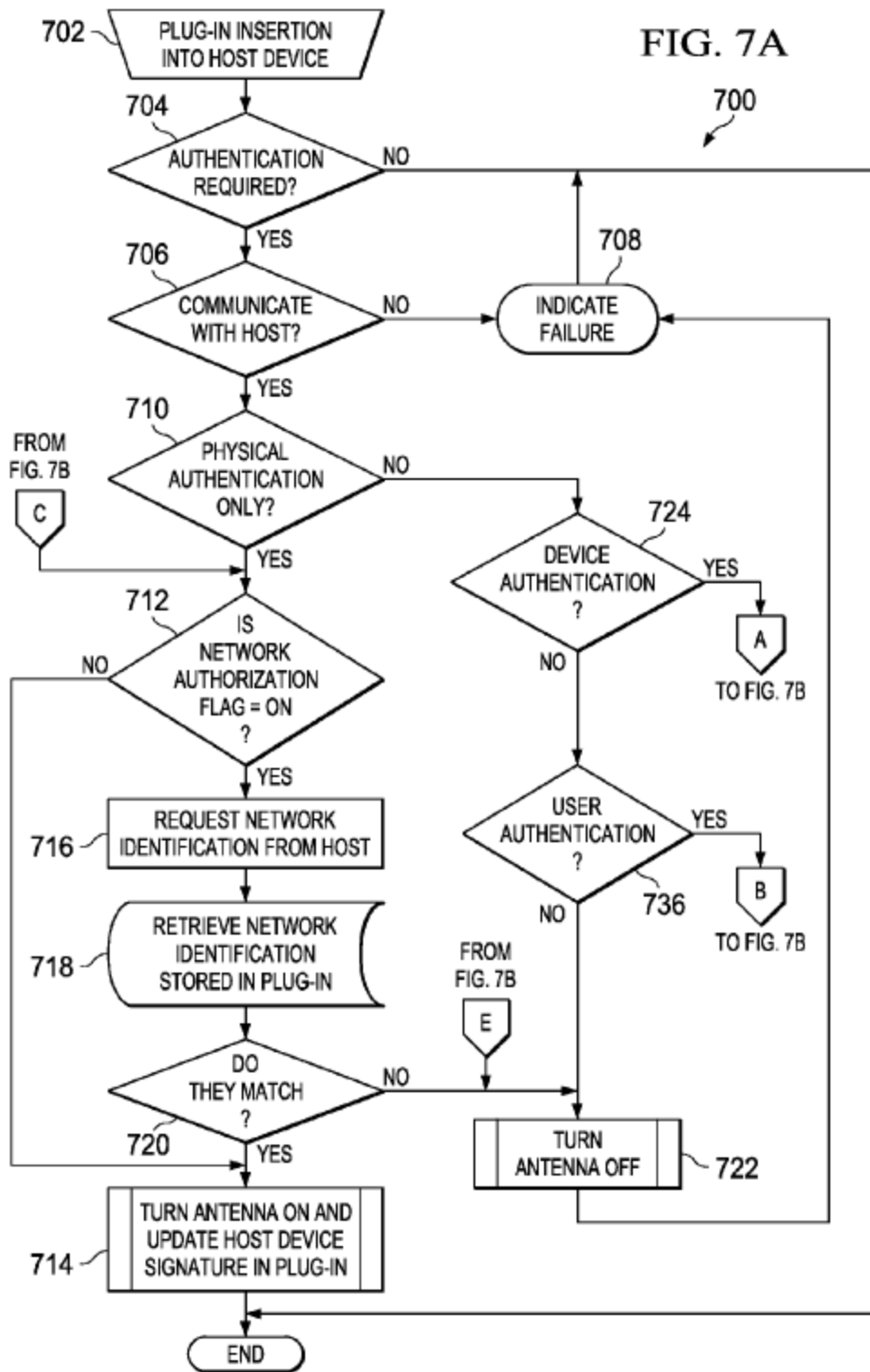
FIG. 1

67. The independence of the transaction card is perhaps most clearly disclosed in the following: “[i]n other words, the transaction card 112 may wirelessly execute transactions without aspects of the transaction being executed by the mobile device 110.” Jain ¶[0022].

68. The independence of the transaction card is further disclosed: “In some implementations, the transaction card 112 can be implemented differently. The transaction card 112 may be implemented as a Key FOB and remains live outside the mobile device 110 as a FOB. In this case, the transaction card 112 may be passive

and powered from an induction magnetic field generated by the POS 114.” Jain ¶[0029]. In fact, Jain discusses the transaction card as a master, and the mobile device as a slave. Jain ¶[0018].

69. Jain begins with connecting the transaction card to a mobile device which initiates a bootstrap process. Jain ¶¶[0065], [0072], [0077]. Figure 7 of Jain depicts that bootstrapping process:



70. This process only occurs when the transaction card is connected to the mobile device. After that point, the mobile device has been authenticated, and transactions can proceed.

71. The mobile device can be a cell phone, pager, portable computer, PDA, MP3 player, camcorder, digital camera, or other mobile device. Jain ¶[0021]. The mobile device provides a graphical user interface for the user to see and provide information. Jain ¶[0022].

72. There is a POS system that transmits a request to execute a transaction to the transaction card. Jain ¶[0019].

73. Jain provides an even more detailed description of the transaction card and its relationship to the mobile device in the following:

The transaction card 112 can include any software, hardware, and/or firmware configured to wirelessly execute transactions with the POS device 114. For example, the transaction card 112 may execute a contactless transaction with the POS device 114 independent of the mobile device 110 a. In other words, the transaction card 112 may wirelessly execute transactions without aspects of the transaction being executed by the mobile device 110. The transaction card 112 may execute transactions with the POS device 114 using short range signals such as NFC (e.g., ISO 18092/ECMA 340), ISO 14443 type A/B, ISO 15693, Felica, MiFARE, Bluetooth, Ultra-wideband (UWB), Radio Frequency Identifier (RFID), contactless signals, proximity signals, and/or other signals compatible with retail payment terminals (e.g., POS 114). In some implementations, the transaction card 112 may include one or more chipsets that execute an operating system

and security processes to independently execute the transaction. In doing so, the mobile device 110 does not require additional hardware, software, and/or firmware to wirelessly execution a transaction with the POS 114 such as an NFC transaction.

Jain ¶[0023].

74. The mobile device is essentially a host for Jain's transaction card. The mobile device provides a graphical user interface (GUI) so the user can see information, *see* Jain ¶¶[0019], [0022], and interfaces with the transaction card. Jain ¶¶[0021], [0022], [0025]. The mobile device may also provide access to cellular communications. Jain ¶¶[0021], [0023], [0042], [0043], [0068].

E. Dua (Ex. 1018)

75. United States Patent Application No. 2006/0165060 to Dua is titled "Method and Apparatus for Managing Credentials Through a Wireless Network." The Examiner considered Dua during the prosecution of the '756 Patent and identified Dua on the face of the '756 Patent as considered art. Dua at 2. The Examiner also discussed Dua during the prosecution of two other applications that depend from the same original application as the '756 Patent. Dua was considered during prosecution of U.S. Patent No. 10,674,432. Ex. 1009 at 169. The Examiner also considered Dua during the prosecution of U.S. Patent No. 10,660,015. Ex. 1008 at 212.

76. Dua was filed on January 21, 2005 and published on July 27, 2006. Dua describes a methodology for conducting transactions, including financial, over a wireless network. Dua, Abstract. Dua describes itself as follows: “[t]he ultimate goal of the present invention is to securely, accurately and rapidly distribute credentials to the proper wireless devices based upon the actions of credential issuers.” Dua ¶[0038]. Figure 1 of Dua provides an overview of the system according to one embodiment:

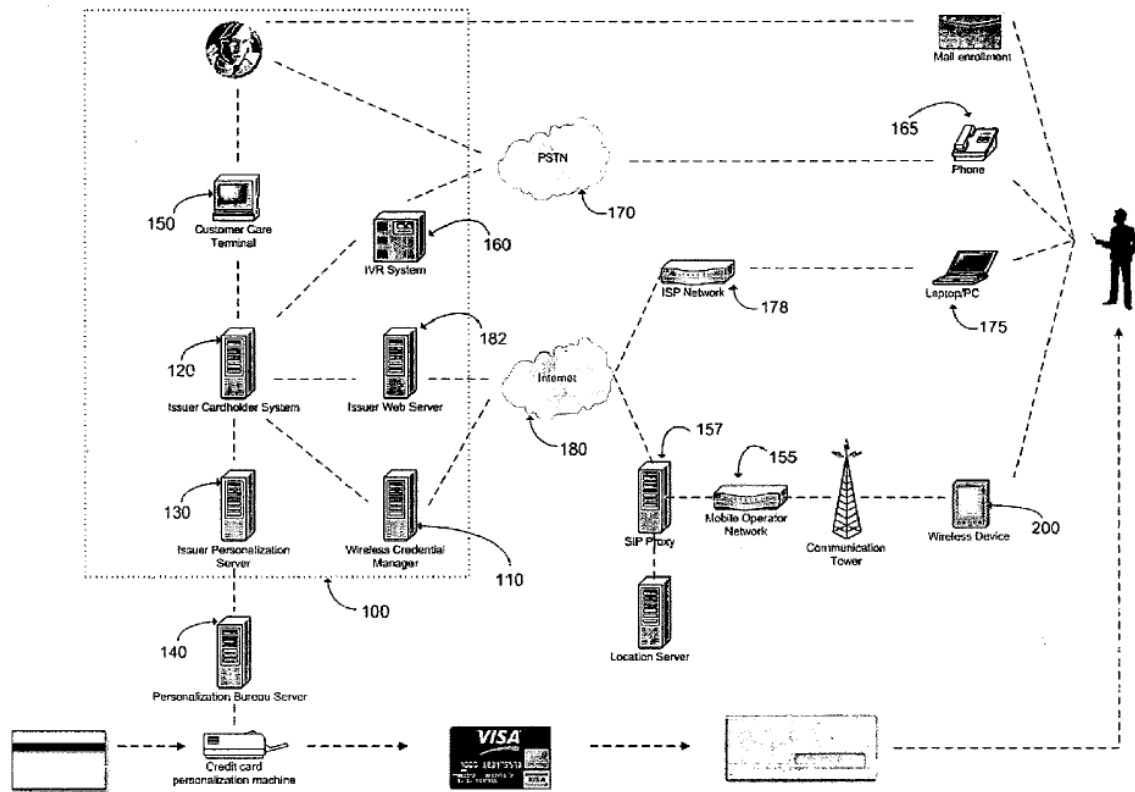


FIG. 1

Dua, Fig. 1.

77. Figure 2 of Dua provides a flowchart illustrating the steps in the process for issuing a credential according to a preferred embodiment:

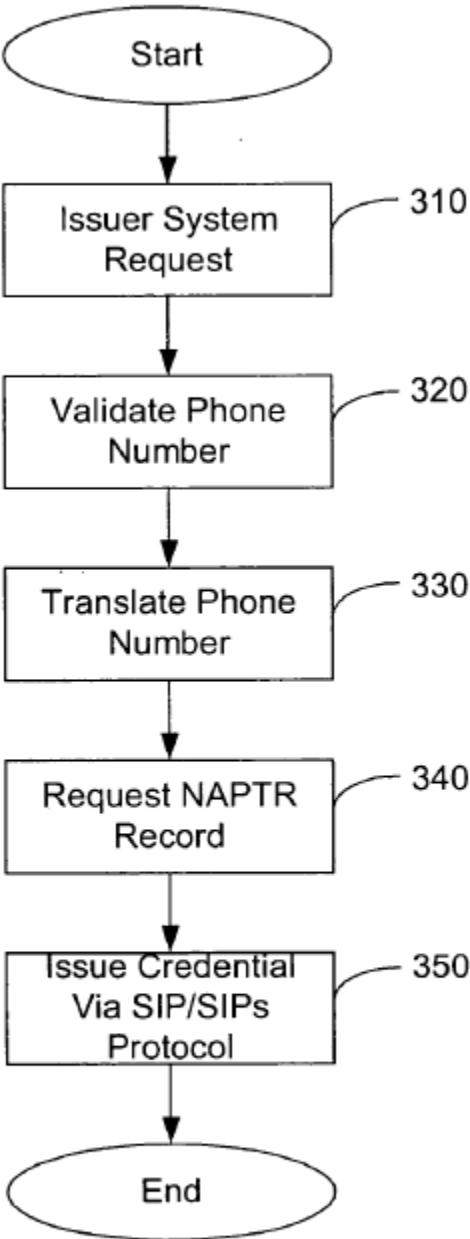


FIG. 2

Dua, Fig. 2.

78. Dua depends heavily on SIP (Session Initiation Protocol). SIP is mentioned 375 times in Dua. RFC 3261 was the active standard for SIP at the time that Dua was filed. SIP focuses on establishing communication. Ex. 2017 at 1. Once said communication is established, then another protocol such as RTP or sRTP is used to transmit any data. Ex. 2020 at 10; Ex. 2021 at 3-4. In fact, Dua itself makes this clear:

Associated with SIP is the SDP, defined in RFC 2327. SIP is used to invite one or more participants to a session, while the SDP-encoded body of the SIP message contains information about what media encodings (for example, voice, video) the parties can and will use. After this information is exchanged and acknowledged, all participants are aware of the participants' IP addresses, available transmission capacity, and media type. Then, data transmission begins, using an appropriate transport protocol. Typically, the RTP is used.

Dua ¶[0110].

79. In Dua, credentials are issued by the issuer's system and then transmitted to the wireless device. Dua ¶[0040]. Credentials are distributed by the Wireless Credential Manager. Dua ¶[0043].

80. Dua makes frequent reference to Naming Authority Pointer ("NAPTR"). NAPTR records provide a mapping from a domain to the Service Records ("SRV") record for contacting a server with the specific transport protocol

in the NAPTR service field. Ex. 2022 at 3-4; Ex. 2023 at 3. NAPTR is closely related to E.164, an international public telecommunication numbering plan. Ex. 2024 at 3.

XII. THE CHALLENGED CLAIMS OF THE '756 PATENT WOULD NOT HAVE BEEN OBVIOUS

A. Petitioner's Ground 1 Fails Because The Claims Would Not Have Been Obvious In View Of Jain

81. The following paragraphs address examples of why the challenged claims would not have been obvious in view of Jain.

82. While I address certain limitations to demonstrate that each of the challenged claims is not unpatentable, I reserve the right to supplement this declaration to include additional information and opinions related to any and all challenged claims and claim elements.

1. Jain Does Not Disclose or Render Obvious "a method of operating a device."

83. Claim 1 requires "a method of operating a device." Claim 6 similarly requires "a device that is configured to perform operations." Claim 11 requires "a method of operating a wireless device." Claim 14 requires "a wireless device that is configured to perform operations." The preambles of these independent claims are limiting because they disclose the "device" or "wireless device" recited later in the claims.. *See, e.g.*, '756 Patent, cls. 1[a] (claiming "sensing by *the device*") (emphasis added); 6[a] (same); 11[a] (claiming "sensing by *the wireless device*") (emphasis added); 14[b] (claiming "using a sensor of *the wireless device*"). The independent

claims also require that the device or wireless device comprise a smartphone. *See* '756 Patent, cls. 1[e] (“wherein the device comprises a smartphone”); 6[e] (same); 11[i] (“wherein the wireless device comprises a smartphone”); 14[e] (same). All dependent claims of the '756 Patent depend from these independent claims, and therefore, all claims of the '756 Patent require a smartphone.

84. It is this claimed smartphone that performs all of the claim limitations of the process of establishing a capability of the smartphone to perform a financial transaction followed by using the established capability to perform a financial transaction. '756 Patent, cls. 1, 6, 11, 14.

85. The '756 Patent contemplates a smartphone or “wireless communication device” that is itself capable of both a first and second communications mode. *Id.* at 3:13-22; 7:17-27. Similarly, it is the “mobile subscriber device 14” of the '756 Patent that itself can “authorize and complete a financial transaction such as the payment of a toll and/or of an item at a check out line.” *Id.* at 9:22-26. The '756 Patent contemplates a single device capable of completing a financial transaction and communicating on multiple modes or air interfaces. But rather than point to a single mobile device in Jain that meets these limitations, Dr. Almeroth points to two separate pieces of hardware that purportedly meet these limitations. *E.g.*, Ex. 1002 ¶122 (pointing to the receipt of an activation code *of the mobile device* as the claimed “receiving by the device from the second

device the authorization to enable the function for conducting the financial transaction”) (emphasis added); Ex. 1002 ¶128 (pointing to the activation of a reader mode *of the transaction card* as the claimed “responsive to the device satisfying a proximity condition relative to an entity”) (emphasis added).

86. Whenever the ’756 Patent does refer to multiple devices engaged in short-range communications, it is two separate, fully functional devices. For example:

The entry of the first device 14 within area 22 can selectively enable a mode and/or a function at device 14 and can optionally enable a mode and/or a function at device 15 based, according to some embodiments, on a proximity criterion to area 24. For example, if device 14 owned and/or operated by a user is at a first store within area 22 and the device 15 owned/operated by, for example, the user’s spouse is at a second store within area 24, then the user’s spouse at device 15 can complete a purchase within area 24 based on the user’s presence with device 14 within area 22.

’756 Patent, 10:36-46.

87. Thus, whenever the ’756 Patent refers to multiple devices, each is still capable of performing both short-range wireless communications and a second mode of communication such as cellular communications.

88. Dr. Almeroth argues that Jain discloses both the “[wireless] device” and “method of operating a [wireless] device.” Ex. 1002 ¶96. Dr. Almeroth argues that Jain discloses the “[wireless] device” and “method of operating a [wireless] device”

because Jain “interfaces mobile device with a transaction card that ‘convert[s] the mobile device . . . to a contactless payment device loaded with a financial vehicle . . . that may be . . . a credit card” Ex. 1002 ¶98 (quoting Jain ¶[0029]).

89. I disagree. Jain does not disclose and would not have rendered obvious “a method of operating a device” of claim 1, “a device that is configured to perform operations” of claim 6, “a method of operating a wireless device” of claim 11, or “a wireless device that is configured to perform operations” of claim 14 because Jain does not disclose a single device (i.e. a smartphone) with the claimed functionality as required by the claims.

90. Unlike the claims at issue, which rely on a single device—a smartphone—to perform a series of steps, Dr. Almeroth switches between the mobile device of Jain and the transaction card of Jain when rendering his opinions. For example, with regard to “receiving by the device from the second device the authorization to enable the function for conducting the financial transaction,” Dr. Almeroth identifies: “[i]n response to the request of step 920, mobile device 110 “*receiv[es]*” an activation code (i.e., ‘*authorization*’) from the financial institution (i.e., ‘*second device*’). Ex. 1002 ¶121. Later, Dr. Almeroth references paragraphs [0019], [0023] of Jain with regard to “conducting by the device the financial transaction by paying for a product.” *Id.* ¶135. However, these paragraphs relate solely to the transaction card—“[t]he transaction card 112 may transmit

authentication information to the POS 114,” *see* Jain ¶[0019]), and “[f]or example, the transaction card 112 may execute a contactless transaction with the POS device 114 independent of the mobile device 110a.” Jain ¶[0023].

91. As part of his assertions regarding the mobile device and transaction card, Dr. Almeroth argues that the mobile device “can include a transaction card” such that the transaction card is part of the mobile device. Ex. 1002 ¶¶96, 99. I disagree. Jain touts that the “mobile device 110 does not require additional hardware, software, and/or firmware” *because* the transaction card itself already has the required functionality, such as NFC. *See* Jain ¶[0022]; *see also id.* ¶[0018] (“An intelligent card is a device configured to . . . access or otherwise execute services (e.g., transactions) independent of the host device.”). In fact, Jain discloses a transaction card that “include[s] any software, hardware, and/or firmware configured to wirelessly execute transactions with the POS device 114” *independent of the mobile device*. Jain ¶[0023] (explaining that “the transaction card 112 may include one or more chipsets that execute an operating system and security processes to independently execute the transaction”). For example, the Jain transaction card itself includes hardware to transmit short-range signals, such as NFC, and the mobile device does not. *Id.* In fact, Jain uses the phrase “independent of the mobile device” or “independent of the host device” several times. Jain, Abstract, ¶¶[0005], [0018], [0023], [0049], [0076], cls. 1, 16). A POSITA would understand that the

independence of the transaction card from the mobile/host device is an essential element of Jain.

92. Dr. Almeroth argues that Jain discloses embodiments in which “a customer’s mobile device 110a with transaction card 112a wirelessly execute transactions with a nearby POS device 114.” Ex. 1002 ¶97 (citing Jain ¶[0019]; Fig. 1). However, the full sentence cited by Dr. Almeroth does not support his conclusion. Paragraph [0019] states that “[t]he offline store 102 includes a mobile device 10a [sic, 110a] having a transaction card 112a and a Point of Sale (POS) device 114 that executes transactions with customers.” This sentence relied upon by Dr. Almeroth is describing a system with multiple separately numbered components including a mobile device connected to a transaction card. It does not disclose that the mobile device has an “included” transaction card. Figure 1, reproduced below, similarly fails to support Dr. Almeroth’s conclusion. While the transaction card 112a is shown within mobile device 110a, mobile device 110a is itself shown inside of offline store 102. By Dr. Almeroth’s logic, the presence of the mobile device 110a inside the store temporarily would make the mobile device 110a and the store 102 itself a single component.

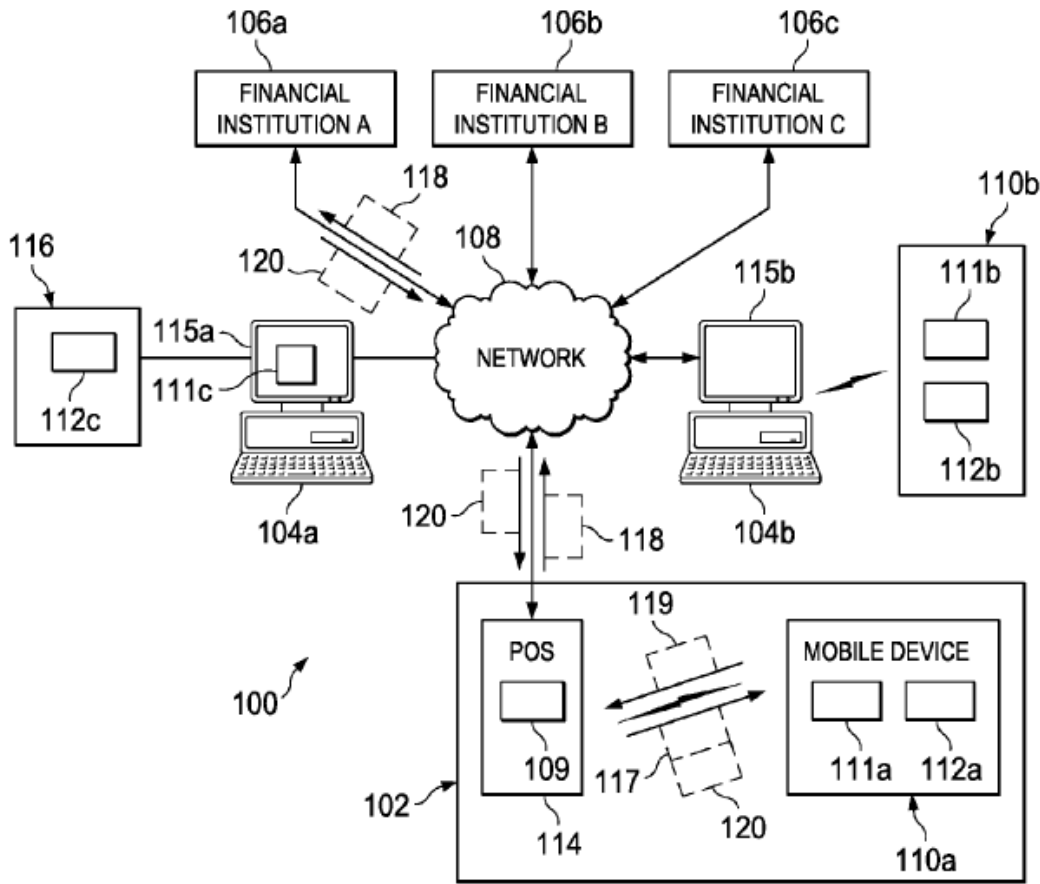


FIG. 1

93. Contrary to Dr. Almeroth’s assertion, Jain specifically requires a *distinct* transaction card that is “*independent*” of the mobile device. Jain ¶[0076] (“The intelligent card 806 is configured to . . . execute transactions *independent of the host device 810.*”) (emphasis added); *see also id.* ¶[0023] (“[T]he transaction card 112 may wirelessly execute transactions *without aspects of the transaction being executed by the mobile device 110.*”) (emphasis added). Jain also makes clear that the transaction card alone, rather than the combination of the transaction card

and mobile device, is essential to executing transactions. *See id.* ¶[0018] (“**By providing the intelligent card**, the system 100 may wirelessly execute transactions”) (emphasis added). Accordingly, because Jain discloses an independent transaction card separate from the mobile device which completes the claimed short-range communications, the transaction card cannot be considered part of the mobile device such that the combination of the two devices discloses the claimed “smartphone.”

94. Dr. Almeroth also argues that “integration [of the transaction card into the mobile device] achieves the benefits disclosed in Jain, but a separate, independent transaction card does not need to be implemented.” Ex. 1002 ¶99. As an example, Dr. Almeroth points to the utilization of the mobile device’s components by the transaction card. *Id.* But Jain emphasizes, as a stated **benefit** of Jain’s invention, that using a separate and distinct transaction card capable of executing transactions independently of the mobile device allows for greater versatility in the types of host mobile devices—a benefit that would be lost if the transaction card were integrated into the mobile device. *See* Jain ¶[0021] (identifying digital cameras, pagers, MP3 players, camcorders and portable computers as possible mobile devices); *see also id.* ¶[0037] (“For example, the user may want to re-personalize the transaction card 112 **to change host devices, to have multiple host devices**, and/or other reasons.”) (emphasis added). Contrary to Dr. Almeroth’s

assertion, the translation functionality emphasizes the ability of the independent transaction card to interface with a wide variety of host devices. Furthermore, Jain discloses that the “mobile device does not require additional hardware, software, and/or firmware to wirelessly execut[e] a transaction,” which is a benefit directly attributable to the transaction card being independent of the mobile device. *See* Jain ¶[0023]. Any integration of the transaction card with the mobile/host device would be entirely contrary to Jain and would eliminate a primary benefit of Jain, the ability for the transaction card to work with multiple devices. *See id.* ¶[0037].

95. Next, Dr. Almeroth alleges that the integration of the mobile device and the transaction card would have been obvious because “separability of the transaction card *is not always advantageous*.” Ex. 1002 ¶100 (emphasis added). Dr. Almeroth then asserts that smartphone vendors would have avoided removability of the transaction card due to (1) reduced modularity of the transaction card and (2) reduction of risk of losing the transaction card through inadvertent loss or theft. *Id.* But Jain does not support Dr. Almeroth’s argument. Jain emphasizes that the modularity of the transaction card is a *benefit* rather than a detriment. *See* Jain ¶[0037]. Further, Petitioner admits that Jain implements an authentication process to guard against lost transaction cards, such as by way of a PIN. Pet. at 12 (citing Jain ¶¶[0072], [0075]; Fig. 7B (annotated); Ex. 1002 ¶¶101-102). Under Dr. Almeroth’s

theory, the inadvertent loss of a transaction card is simply replaced by the inadvertent loss of a mobile device, which provides no added benefit.

96. Therefore, Jain fails to disclose or render obvious “a method of operating a device” of claim 1, “a device that is configured to perform operations” of claim 6, “a method of operating a wireless device” of claim 11, or “a wireless device that is configured to perform operations” of claim 14.

2. ***Jain Does Not Disclose or Render Obvious “responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion, enabling by the device a number of functions of the device and disabling by the device a function of the device.”***

97. Claims 1 and 6 require “***responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion***, enabling by the device a number of functions of the device and disabling by the device a function of the device.” Claims 11 and 14 similarly require “***responsive to the value that is sensed satisfying the threshold criterion***, enabling a number of functions of the wireless device and disabling a function of the wireless device.” Claims 2 through 5 depend from claim 1, and thus also include this limitation. Claims 7 through 10 depend from claim 6, and thus also include this limitation. Claims 12 and 13 depend from claim 11, and thus also include this limitation. Claims 15 through 18 depend from claim 14, and thus also include this limitation. Petitioner and Dr. Almeroth treat these limitations as substantively identical to limitation 1[c]. Pet. at

31-32. Dr. Almeroth argues that Jain discloses this limitation. Ex. 1002 ¶ 115. I disagree.

98. Under limitation 1[c], the claimed “enabling” and “disabling” steps must occur “responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion.” In order to satisfy the “responsive to” and “enabling” elements of limitation 1[c], Dr. Almeroth first points to method 700 and asserts that “step 714: ‘turn antenna on and update host device signature in plug-in’” is the “*enabling by the device a number of functions of the device*” which allegedly occurs “in response to user authentication (in steps 738-742 of FIG. 7B) (*i.e.*, “*responsive to satisfying a threshold criterion*”). Ex. 1002 ¶ 107 (citing Jain ¶¶[0072]-[0075], Fig 7B) (emphasis in original). That is, Dr. Almeroth equates the user authentication of Fig. 7B with the claimed “satisfying a threshold criterion” and, thus, the claimed “enabling” and “disabling” steps must be responsive to the user authentication described in Fig. 7B.

99. When alleging that Jain performs the claimed “disabling” step, Dr. Almeroth then equates the claimed “enabling” step to a different disclosure within Jain, method 900 and Figure 9. Ex. 1002 ¶¶108-112. Dr. Almeroth identifies the activation of the mobile device’s antenna described in method 900 as the claimed “enabling” step. *Id.* ¶108. Dr. Almeroth does not explain the abandonment of the first identified “enabling” step within method 700 for this identified “enabling” step

within method 900. Dr. Almeroth proceeds to rely on the activation of the mobile device's antenna described in method 900 as the claimed "enabling" step when arguing that Jain meets the "disabling" step of the limitation under two separate theories. *Id.* But Dr. Almeroth cannot explain how any step of method 900 is performed "responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion" because Jain does not impose this requirement prior to executing method 900. *See* Jain ¶[0081]; Fig. 9.

100. It is my opinion that method 900 is unrelated to method 700. Jain discloses two separate and distinct processes: method 700, which describes "automatically bootstrapping an intelligent card in response to at least insertion into a host device," and "method 900 for activating a wireless transaction system including an intelligent card." Jain ¶¶[0072], [0080]. These two methods use two distinct methods utilizing different antennae to achieve unique ends.¹ *See* Jain ¶[0063] ("As illustrated, the intelligent card 400 includes *an antenna 402 . . .*") (emphasis added); *see also id.* ¶[0073] ("[A]t step 714, the antenna is turned on and the intelligent card is updated with host-device signature."); *see also id.* ¶[0081]

¹ Antenna 322 on the transaction card is "a short range wireless antenna connected to an NFC inlay via a software switch such as a NAND Gate or other element." Jain ¶[0061].

(“Method 900 begins at step 902 where a request to *activate a transaction card* is received . . . If an *account activation* is included . . .”) (emphasis added); *see also id.* (“For example, the transaction card 112d of Fig. 2 may wirelessly transmit an activation request to the financial institution 106 *using the cellular radio technology of the mobile host device.*”) (emphasis added).

101. Dr. Almeroth attempts to tie method 700 and method 900 together by pointing to paragraph [0072] of Jain to argue that “[o]nly after bootstrapping/authentication (FIG. 7) is complete can activation (FIG. 9) begin” Ex. 1002 ¶ 108. But paragraph [0072] does not support Dr. Almeroth’s interpretation. The activation described in paragraph [0072] is activation *of the transaction card’s antenna* described in the immediately following paragraph, not the unrelated activation described in several paragraphs later in Fig. 9 and method 900. *See* Jain ¶[0073] (“As for the example, the transaction card 112 *may activate the antenna for wireless transactions*”) (emphasis added). Turning on the transaction card’s antenna by the process of method 700 (and any alleged user authentication) does not impact the execution of method 900. Thus, method 900 cannot be executed “responsive to” the alleged user authentication in method 700.

102. Furthermore, Dr. Almeroth cannot explain how activating the antenna in method 900 of Figure 9 is “responsive to . . . the value . . . for the parameter” by solely relying on method 900. Jain does not disclose an authentication process in

method 900 that meets the claimed “value . . . for the parameter.” Jain only discloses the use of an activation code provided by the financial institution or locally stored answers to preprogrammed questions in method 900. Jain ¶[0081]. But the activation code and the locally stored answers do not meet the claimed “parameter” within limitations 1[d], 6[d], 11[h], or 14[i]. *See, e.g.*, ’756 Patent, cl. 1[d] (“wherein the parameter that is sensed using the device-based sensor, comprises a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state;”). And Dr. Almeroth does not allege that the activation code or the locally stored answers satisfy the claimed “value . . . for the parameter.”

103. Dr. Almeroth conflates method 700 and method 900 to meet the claimed “enabling” and “responsive to” elements of the limitation, but method 900 relied upon by Dr. Almeroth as the claimed “enabling” step is not performed “responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion.” Dr. Almeroth fails to explain why a POSITA would have been motivated to combine methods 700 and 900. In fact, he does not even suggest a POSITA would combine methods 700 and 900; rather, he treats these separate processes as if they were one process. For at least these reasons, Jain fails to disclose or render obvious “responsive to the value that is determined by the

device for the parameter that is sensed satisfying a threshold criterion, enabling by the device a number of functions of the device and disabling by the device a function of the device” of independent claims 1 and 6, “responsive to the value that is sensed satisfying the threshold criterion, enabling a number of functions of the wireless device and disabling a function of the wireless device” of claim 11, and “responsive to the value satisfying the threshold criterion, enabling a number of functions at the wireless device and disabling a function of the wireless device” of claim 14.

3. *Jain Does Not Disclose or Render Obvious “responsive to the requesting, receiving by the wireless device from the second device the authorization to enable the function for conducting the financial transaction”*

104. Independent claim 11 requires “responsive to the requesting, receiving by the wireless device from the second device the authorization to enable the function for conducting the financial transaction.” Independent claim 14 similarly requires “responsive to the requesting, receiving from the second device the authorization to enable the function for conducting the financial transaction.” Petitioner and Dr. Almeroth treat these limitations as substantively identical to limitation 3[b]. Pet. at 31-32. Claims 12 and 13 depend from claim 11, and thus also include this limitation. Claims 15 through 18 depend from claim 14, and thus also include this limitation. Dr. Almeroth argues that Jain discloses this limitation. Ex. 1002 ¶125. I disagree.

105. To meet this limitation, Dr. Almeroth points to steps 920-924 of method 900 which describes the process of activating a card in Jain. Ex. 1002 ¶¶120-122. At step 920, the transaction card, via the mobile device, “wirelessly transmits a request for the activation code using the cellular radio technology” of the mobile device to the financial institution. Jain ¶[0081]. Next, the transaction card identifies a locally stored activation code at step 922 and compares this locally stored activation code to the received activation code from the financial institution at step 924. *Id.* If the activation codes match, the transaction card is activated by step 926. *Id.* Dr. Almeroth points to receiving the activation code from the financial institution as the claimed “receiving by the device from the second device the authorization.” Ex. 1002 ¶121.

106. But Dr. Almeroth fails to explain how this requested activation code can be the claimed “authorization to enable the function for conducting the financial transaction” and does not address that the requested activation code, on its own, does not function as an authorization at all. When activating a transaction card through the process disclosed by method 900, Jain does not require that the financial institution first verify that the user is indeed authorized before sending the activation code. *See* Jain ¶[0081] (“[A]t step 920, the transaction card wirelessly transmits a request for the activation code using the cellular radio technology of the host device . . . If the locally stored information matches the provided information at

decisional step 924, then at step 926, the transaction card is activated). Jain relies on the transaction card itself to perform the authentication. To perform the authentication, Jain relies on a comparison between the code that is sent by the financial institution and the code that is stored on the transaction card. *See id.* Accordingly, the **transaction card** makes the determination. *See id.* ¶[0080]. (“In general, an **intelligent card** may execute one or more activation processes in response to, for example, a selection from a user.”) (emphasis added).

107. From the disclosure, a POSITA would have understood that Jain allows a financial institution to send a code to an unauthorized user because the transaction card must compare the two codes and determine that the codes match before activation occurs. In other words, the financial institution sends the activation code regardless of whether the requesting transaction card is authorized. *See id.* Accordingly, Dr. Almeroth has failed to demonstrate that the activation code alone sent by the financial institution cannot be the claimed “authorization.”

108. Next, Dr. Almeroth argues that a POSITA would “understand that the smartphone receives an **authorization** by receiving an activation code from the financial institution.” Ex. 1002 ¶123 (emphasis in original). According to Dr. Almeroth, a POSITA would have found it obvious “that the financial institution **would not** provide a valid activation code to a smartphone that is not authorized to perform payment services with the financial institution.” *Id.* (citing Jain ¶[0081];

FIG. 9) (emphasis added). But Jain explicitly discloses that the financial institution *would* provide a valid activation code to an unauthorized user because the requested activation code must still match the locally stored code. *See* Jain ¶[0081] (“If the provided information does not match the locally stored information, then execution ends.”). A POSITA would have understood from Jain that the only reason Jain performs this check with the locally stored code is because Jain allows for and contemplates requests from unauthorized users, e.g., fraudulent transaction cards. *See, e.g., id.* ¶[0026] (“In response to one or more events matching or otherwise violating rules, the transaction card 112 may execute one or more processes to substantially prevent or otherwise notify the financial institutions 106 of potentially fraudulent activity.”). To combat this, if an unauthorized user received a valid activation code, the transaction card would not be activated because the requested code and the locally stored code would not match and execution would end. *See id.* ¶[0081].

109. It is my opinion that the requested activation code cannot be considered the claimed “activation” because the execution of method 900 could still end without activation of the transaction card despite receiving the purported “activation” if the requested activation code does not match the locally stored code. *See id.*

110. Finally, Dr. Almeroth states that a POSITA would “find such implementation [i.e., treating the requested activation code as an authorization] well

known, thereby rendering it obvious.” Ex. 1002 ¶127 (citing Ex.1019 ¶¶[0145]-[0146]). Dr. Almeroth also points to a purported gain in system security as evidence that this implementation would have been obvious. *Id.* But Jain explicitly contravenes this implementation by requiring the authorization to occur at the mobile device rather than at the financial institution. *See* Jain ¶[0081]. Even Dr. Almeroth’s cited references highlight the difference of the provider “confirm[ing] [that] the information is ‘valid’” as opposed to the transaction card of Jain confirming that the information is valid. Ex. 1019 ¶¶[0145]-[0146]. Accordingly, the activation code received by the mobile device merely *facilitates* authorization—it is not *the* authorization.

111. Dr. Almeroth fails to establish that Jain discloses or renders obvious “responsive to the requesting, receiving by the wireless device from the second device the authorization to enable the function for conducting the financial transaction” in independent claim 11 or “responsive to the requesting, receiving by the wireless device from the second device the authorization to enable the function for conducting the financial transaction” of independent claim 14.

4. *Jain Does Not Disclose or Render Obvious “responsive to the wireless device satisfying a proximity condition relative to an entity”*

112. Independent claim 11 requires “responsive to the wireless device satisfying a proximity condition relative to an entity.” Independent claim 14

similarly requires “responsive to the wireless device satisfying a proximity condition relative to an entity.” Petitioner and Dr. Almeroth treat these limitations as substantively identical to limitation 4[a]. Pet. at 31-32. Claims 12 and 13 depend from claim 11, and thus also include this limitation. Claims 15 through 18 depend from claim 14, and thus also include this limitation. Dr. Almeroth argues that Jain discloses this limitation. Ex. 1002 ¶129. I disagree.

113. In support of his position, Dr. Almeroth first misquotes Jain. Dr. Almeroth alleges that “[t]he *smartphone* first ‘wirelessly receive[s] a request from the POS device 114 to execute a transaction and/or provide a response.’ Jain ¶[0023].” Ex. 1002 ¶128 (emphasis added). That is not what Jain says. Jain says that “*the transaction card 112* may execute one or more of the following: wirelessly receive a request from the POS device 114 to execute a transaction and/or and [sic] provide a response.” Jain ¶[0023] (emphasis added). Jain describes *the transaction card* as capable of “execut[ing] transactions with the POS device 114 using short range signals such as NFC.” Jain ¶[0023]; *see also id.* ¶[0061] (“The antenna 322 may be a short range wireless antenna connected to an NFC inlay via a software switch such as a NAND Gate or other element.”). Because the transaction card has the NFC capability, “the transaction card 112 may wirelessly execute transactions *without aspects of the transaction being executed by the mobile device 110.*” *Id.* But the claimed “satisfying” step must be performed by the device and not the

transaction card. For the same reasons as above with respect to Section XII.A.1, Jain similarly does not disclose the claimed “responsive to the wireless device satisfying a proximity condition relative to an entity.” *See supra* Section XII.A.1.

114. Next, Dr. Almeroth argues that Jain renders this limitation obvious. Ex. 1002 ¶131. But Dr. Almeroth fails to explain why a POSITA would have contravened the teaching of Jain to implement an NFC capability on the mobile device instead of the transaction card. *See* Jain ¶[0023]. Therefore, Jain fails to disclose or render obvious “responsive to the wireless device satisfying a proximity condition relative to an entity” in independent claims 11 and 14.

B. Petitioner’s Ground 2 Fails Because The Claims Would Not Have Been Obvious In View Of Dua

115. The following paragraphs address examples of why the challenged claims would not have been obvious in view of Dua.

116. While I address certain limitations to demonstrate that each of the challenged claims is not unpatentable, I reserve the right to supplement this declaration to include additional information and opinions related to any and all challenged claims and claim elements.

1. *Dua Does Not Disclose or Render Obvious “responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion, enabling by the device a number of functions of the device.”*

117. Claims 1 and 6 require “*responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion*, enabling by the device a number of functions of the device and disabling by the device a function of the device.” Claim 11 similarly requires “*responsive to the value that is sensed satisfying the threshold criterion*, enabling a number of functions of the wireless device and disabling a function of the wireless device.” Claim 14 similarly requires “*responsive to the value satisfying the threshold criterion*, enabling a number of functions at the wireless device and disabling a function of the wireless device.” Claims 2 through 5 depend from claim 1, and thus also include this limitation. Claims 7 through 10 depend from claim 6, and thus also include this limitation. Claims 12 and 13 depend from claim 11, and thus also include this limitation. Claims 15 through 18 depend from claim 14, and thus also include this limitation. Petitioner and Dr. Almeroth treat these limitations as substantively identical to limitation 1[c]. Pet. at 31-32.

118. During the prosecution of the related '432 Patent, Applicant successfully and correctly argued that Dua did not “teach or suggest ‘enabling a mode to communicate . . . responsive to at least one physiological parameter . . . ’ as

recited in amended claim 1.” Ex. 1009 at 253. The examiner stated in the notice of allowance that:

Dua alone or in combination fails teaches or fairly suggest [sic];
responsive to at least one physiological parameter having been sensed by at least one sensor of the smartphone, enabling a mode to communicate by the smartphone information requesting an authorization;
while the mode is enabled, transmitting by the smartphone first data to a first device, the first data relating to a plurality of financial transactions to be conducted;
. . .independent of performing said first transaction, receiving by the smartphone a communications service from a wireless network, using a second air interface that differs from the first air interface, wherein said transmitting by the smartphone first data and said receiving by the smartphone second data are performed over an air interface that differs from the first air interface.

Ex. 1009 at 275-276 (emphasis in original).

119. Dr. Almeroth argues that Dua discloses this limitation under either a “Card-Issuing Theory” or an “External-Storage-Authentication Theory.” Ex. 1002 ¶215. I disagree.

a. Dua’s “Card-Issuing” Theory Fails

120. According to Dr. Almeroth, Dua’s Card-Issuing Theory discloses that “[t]he wallet application establishes a Session Initiation Protocol (“SIP”) communication session (i.e., “*enabling . . . a number of functions*”) between the wireless device and the issuer’s WCM for this authentication process (i.e., “*enabling . . . a number of functions*”). Ex. 1002 ¶186 (citing Dua ¶¶[0046], [0104], [0128], [0178]). Dr. Almeroth points to the establishing of the SIP session and

subsequent authentication as the claimed “enabling . . . a number of functions.” *Id.* I disagree.

121. In rendering his opinion, Dr. Almeroth ignores that the “enabling . . . a number of functions” must be “*responsive to* determining that the at least one parameter that is sensed satisfies a criterion.” Dr. Almeroth does not cite any disclosure from Dua that requires an authentication to take place prior to establishing SIP communication. Dua does not require a PIN to start the SIP process or following the opening of the wallet application when issuing a credential. *See* Dua ¶[0129] (disclosing initiating a SIP message exchange without first requiring a PIN). Rather, paragraph [0180] of Dua discloses that “*subsequent to*” establishing a SIP communication session, “the issuer’s system *will authenticate the mobile user’s identity in real-time.*” Dua ¶[0180] (emphasis added).

122. To overcome this deficiency, Dr. Almeroth alleges that there is a relationship between opening the wallet application “[a]fter finding a valid fingerprint” and the establishment of SIP communications. *See* Ex. 1002 ¶186. But the relationship between establishing SIP communications and opening the wallet application via PIN entry is not supported by Dua. Dua does not and would not rely on the PIN entry opening the wallet to secure the SIP communication session because the SIP communication session has its own authentication scheme. *See id.* ¶[0180] (describing the authentication process occurring *during* the SIP session)

(emphasis added); *see also id.* ¶¶[0202]-[0209] (describing the “major security mechanisms suited for the protection of a SIP session”). Nor does the wireless device automatically start the SIP process following opening the wallet initiation via PIN entry because a user can “access stored credentials” within the wallet application without proceeding to the card issuance process. *See id.* ¶[0129].

123. Moreover, Dua allows for the direct delivery of credentials without requiring a PIN. *See* Dua ¶[0053] (“For example, a subscriber might wish to install a wallet application on wireless device 200 and register the telephone number as the identifier for the wallet application. Multiple issuers can in turn deliver payment methods, identification, or other types of electronic credentials to the wallet application on the wireless device 200 via the Internet using the phone number as the destination address.”); *id.* ¶[0056] (“According to the teachings of this invention, credential issuers may request from applicants (e.g. over the telephone) a properly formatted E.164 phone number in order to target the delivery of credential(s) to a wallet application on wireless device 200.”).

124. Dr. Almeroth focuses on a process in Dua under which the user must enter a PIN to issue a credit card to the wallet application. *Id.* ¶176 (citing Dua ¶¶[0128]-[0129], [0178], [0180], [0250]). But the disclosure of those paragraphs explicitly contemplates communication between a Wireless Credential manager (WCM) and a “SIP-enabled mobile device 500 via the Internet” in which the “WCM

510 may initiate communication with a wallet application on Bob's wireless device 500." Dua ¶¶[0128]-[0129]. This disclosure permits "direct communication between the end-points (WCM and wallet application) for the purpose of transferring confidential information." Dua ¶[0178]. And most critically for my disagreement with Dr. Almeroth, "[t]he established session may initially be used to exchange encryption keys and/or other security information. *Subsequent to that*, the issuer's system will authenticate the mobile user's identity in real-time to ensure that the person on the receiving end is in fact the person that requested the digital credential." Dua ¶[0180] (emphasis added). The connection is established and communication between the wallet application and the WCM has begun prior to the disclosed authentication.

125. Dr. Almeroth's discussion of the use of biometric sensors for authentication and decryption fares no better. Dr. Almeroth provides no discussion of such authentication as a prerequisite for communication. Ex. 1002 ¶181 (citing Dua ¶¶[0366], [0414], [0534], [0050], [0399], [0429]). His identified citations themselves again speak to authenticating the user for the transaction, not communication. *E.g.*, Dua ¶[0366] ("[d]ata in the wallet application is encrypted and protected with a special wallet PIN code which is set by the wireless device owner during the setup of the application"); ¶[0414] ("online PIN verification also gives certain credential issuers a stronger means by which to validate a person's identify

during a transaction”); ¶[0534] (“the user would be required to provide a E.164 number for a wireless device in order to establish the wallet account on a server hosted and managed by the wallet service provider.”). In fact, these citations again make reference to the use of a connection to provide authentication. Dua ¶[0050] (“the resolved Internet address is used to establish secure real-time communication between WCM 110 and the wallet application on wireless device 200 using the Session Initiation Protocol (SIP) . . . to transfer encrypted credentials.”).

126. Dr. Almeroth then asserts alternative arguments that Dua satisfies this limitation. For instance, Dr. Almeroth argues that functions such as data decryption that are purportedly performed during credit card issuance meet the claimed “enabling” and “disabling” steps. Ex. 1002 ¶¶187-90. But Dua’s credential issuance is performed through a SIP session which is not “responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion.” *See* Dua ¶¶[0129], [0180].

127. Accordingly, Dua’s “Card-Issuing” Theory fails to render this limitation obvious.

b. Dua’s “External-Storage-Authentication” Theory Fails

128. Dr. Almeroth also argues that, under Dua’s “External-Storage-Authentication Theory,” “retrieval of credentials from the external storage is only possible after performing fingerprint authentication.” Ex. 1002 ¶191 (citing Dua

¶¶[0353]-[0354], [0366], [0429]). Dr. Almeroth again to establishing a SIP session during credential issuance as the claimed “enabling a number of functions.” Ex. 1002 ¶191. Again, I disagree because the SIP session is not responsive to fingerprint authentication.

129. Dr. Almeroth makes the same argument related to the Card Issuing Theory, i.e., that establishing the SIP session is responsive to opening the wallet application following a fingerprint or PIN authentication. *Id.* ¶192. As shown above, Dua only requires a PIN “*subsequent to*” establishing a SIP communication session when issuing a credential. *See* Dua ¶[0180] (emphasis added); *see also* Section XII.B.1.a. Dr. Almeroth also argues that the same alternative functions described in the Card-Issuing Theory meet this limitation. Ex. 1002 ¶¶193-95. Dr. Almeroth attempts to tie these functions to credential issuance which occurs through the SIP session. These functions are separate and unrelated to Dua’s credential issuance which is not “responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion.” *See* Dua ¶¶[0129], [0180].

130. Therefore, Dua fails to disclose or render obvious, in either its “Card-Issuing” Theory or its “External-Storage-Authentication” Theory, “responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion, enabling by the device a number of functions of the device and disabling by the device a function of the device” of independent claims 1 and 6,

“responsive to the value that is sensed satisfying the threshold criterion, enabling a number of functions of the wireless device and disabling a function of the wireless device” of claim 11, and “responsive to the value satisfying the threshold criterion, enabling a number of functions at the wireless device and disabling a function of the wireless device” of claim 14.

2. *Dua Does Not Disclose or Render Obvious “responsive to the wireless device satisfying a proximity condition relative to an entity.”*

131. Independent claim 11 requires “responsive to the wireless device satisfying a proximity condition relative to an entity.” Independent claim 14 similarly requires “responsive to the wireless device satisfying a proximity condition relative to an entity.” Petitioner and Dr. Almeroth treat these limitations as substantively identical to limitation 4[a]. Pet. at 31-32. Claims 12 and 13 depend from claim 11, and thus also include this limitation. Claims 15 through 18 depend from claim 14, and thus also include this limitation.

132. Dr. Almeroth asserts that Dua discloses this limitation. Ex. 1002 ¶223. I disagree.

133. Dr. Almeroth alleges that Dua “short range wireless link with the point-of-sale reader includes NFC.” *Id.* Not so. The sole reference to NFC in Dua is in the background of the technology section. Dua ¶[0016] (“Wireless devices with integrated RFID proximity chips or Near Field Communication (NFC) technology

may also provide users the ability to transfer information to a reader device.”). Even after acknowledging its existence, Dua then omits NFC entirely from the list of network protocols contemplated by the invention of Dua, which include “GSM/GPRS, CDMA2000, W-CDMA, EDGE, HDR, 1xRTT, UMTS, IMT-2000, 802.11a, 802.11b, 802.11g, or BLUETOOTH.” Dua ¶[0041]. In fact, in every example where Dua discusses available “wireless” protocols, Dua omits any discussion or even mention of NFC. *See* Dua ¶[0318] (“Connectivity between the wireless device and the reader/POS terminal could be made via 802.11a/b/g, Bluetooth, or other RF protocols.”); *see also id.* ¶[0457] (“The user may accomplish [transferring credentials between devices] using . . . the short-range transmission capability of both devices (e.g. Bluetooth, infra-red, etc); *see also id.* ¶[0102] (listing Internet protocols such as “Transmission Control Protocol (TCP), Transmission Layer Security (TLS), User Datagram Protocol (UDP), Internet Protocol (IP), Domain Name System (DNS), and others.”); *see also id.* ¶[0103] (“SIP can provide a set of services that is more diverse, compelling and profitable than any of the contemporary wireless protocols including WAP, SMS and MMS.”); *see also id.* ¶[0263] (“As such, WCM 110 is preferably compatible with IPv4 and IPv6 networks. WCM 110 also supports the following transport protocols: UDP/TCP/TLS/SCTP. WCM 110 also supports multiple domain names.”); *see also id.* ¶[0429] (“A number of server authentication and data encryption protocols may

be employed to secure credentials and other confidential information such as Wireless Transport Layer Security (WTLS), Transport Layer Security (TLS), and Secure Socket Layer (SSL). Wireless Identity Module (WIM) could be used for digital signatures enabling authenticated payments.”); *see also id.* ¶[0494] (“The connection between the wallet application and the storage service could utilize an application protocol such as HTTP, SIP, or others.”).

134. In fact, while Dua only makes a passing mention of NFC in the background section, Dua frequently embraces the use of Bluetooth. As one example:

For example, if a user wants a digital debit card, the user may be prompted by a bank employee to bring his wireless device in proximity of an RFID reader, which will send a command to the wallet application signifying that it is going to receive a new credential via Bluetooth. The bank system and the wireless device may exchange encryption keys via RF in order to establish a secure Bluetooth connection with the bank network (the process for establishing Bluetooth connectivity is similar to what is outlined later in the Wallet Transfer section).

Dua ¶[0321].

135. Another example is found in the following excerpt from Dua:

The user would first login to his existing wallet application using his PIN or biometric ID. From the settings menu, the user would choose the "secure wallet transfer" option. The user might be given the ability to select which short-range transmission capability to use for communication with the new device (in case the device supports different types). For this example, we will assume that the user selects Bluetooth. The wallet application on the existing device will display a randomly generated 20 digit key that the

user will be required to enter in the wallet application on the new device in order to authenticate the existing device and wallet.

Dua ¶[0458].

136. Using Bluetooth for short-range communications is disclosed in Dua, *see* Dua ¶¶[0463]-[0465], [0468], [0485]; however, NFC is never disclosed for any communication in Dua. It is my understanding that neither Petitioner nor Dr. Almeroth point to or rely on the Bluetooth disclosures in Dua with regard to this claim limitation.

137. In fact, the “local environment,” also referred to as a “proximity environment,” of Dua does not contemplate NFC. *See* Dua ¶¶[0314]-[0315]. The “proximity environment” disclosed “serve[s] as a replacement for single-purpose cards and tokens” during which the device “can transmit . . . information to a reader using the short range transmission capability of the wireless device (e.g. RF).” Dua ¶[0315]. Dua explains that, in this proximity environment, “a wireless device loaded with a wallet application[] *that also has an integrated RFID chip* can simply be waved slowly in close proximity to a reader device to facilitate a transaction.” *Id.* (emphasis added). Despite Dr. Almeroth’s claims that a POSITA would have found it obvious to implement NFC, Dua specifically omits NFC from this embodiment even though Dua previously referenced NFC in the background. Dr. Almeroth’s statement that Dua’s “wireless device’s short range wireless link with the point-of-

sale reader includes NFC” is based simply on a background mention of NFC that is unrelated to (and excluded from) the actual system of Dua. Ex. 1002 ¶ 223 (citing Dua ¶[0016]).

138. Dr. Almeroth then argues that a POSITA would have found it obvious to detect that a proximity condition is satisfied via detecting NFC signals from a POS terminal. Ex. 1002 ¶224. Dr. Almeroth points to claims 33, 36, and 50 in Dua as a motivation to implement NFC. *Id.* (citing Dua, cls. 33, 36, 50). But none of these claims in Dua contemplate a short-range communications protocol, let alone NFC. Dua’s claims 33 and 36 make no mention of a communications protocol. *See* Dua, cl. 33 (“The method of claim 1, wherein said credential corresponds to an account not previously opened by a customer.”); *see also id.*, cl. 36 (“The method of claim 35, wherein said electronic payment transfer is a business-to-business transfer.”). And Dua’s claim 50 describes the wireless connection between a wireless device and *an issuer*, not a supposed NFC connection between a wireless device and a point-of-sale terminal. *See also id.*, cl. 50 (“A system for transmitting a credential *from an issuer to a wireless device . . .*”) (emphasis added). Dr. Almeroth also points to Dua’s disclosure of a peer-to-peer communication session as suggesting NFC communications. Ex. 1002 ¶224 (quoting Dua ¶[0359]). But preceding disclosures in Dua confirm that Dua contemplates RF communications and fails to include NFC communications. *See* Dua ¶[0354] (“If a matching key is found within

the wallet application, the corresponding loyalty information will be transmitted to the reader from the wireless device *via RF.*”) (emphasis added).

139. Further, Dua’s disclosure contradicts Dr. Almeroth’s view, as Dua specifically recites its own concepts for protocols that could be used for connectivity instead of relying on NFC. For example, Dua discloses that for short-range communications, “[c]onnectivity could initially be established by exchanging encryption keys via RFID that allow the devices to establish connectivity via an alternate channel securely so no other device can listen in to the communication. Keys could also initially be exchanged via infra-red technology.” *Id.* ¶[0318]. Dua also identifies a 30-second connectivity time-out period—the type of independent connectivity requirement that would not have motivated a POSITA, reading Dua, to implement un contemplated technologies like NFC. *Id.* ¶[0383], [0384]. These examples illustrate that it would not have been obvious to a POSITA to seek out and rely on undiscussed NFC standards relating to proximity.

140. Because Dua does not disclose the proximity condition of the ’756 Patent, Dr. Almeroth provides pages of discussion of how NFC itself has such a condition. But Dua ultimately does not contemplate NFC as part of its claimed invention. And Dr. Almeroth’s efforts to combine the Dua system with NFC boil down to an unsupported bare allegation that a single mention of NFC in Dua’s background would have motivated a POSITA to disregard Dua’s disclosures of

separate peer-to-peer communication protocols and look to an NFC standard. I disagree with his view for the reasons I have explained. Dr. Almeroth has not established that Dua discloses nor renders obvious “responsive to the wireless device satisfying a proximity condition relative to an entity” of independent claims 11 and 14.

XIII. SUMMARY AND OTHER REMARKS

141. It is my opinion that Petitioner has failed to show that any of the Challenged Claims set forth in Grounds 1 and 2 are unpatentable as obvious as explained above.

142. My opinions expressed in this Declaration are based on the information available to me at this time. To the extent any additional information becomes available, I reserve the right to supplement my opinions contained herein.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on the information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed on September 17, 2025.



Chuck Easttom