

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. IPR2025-00974
U.S. Patent No. 10,674,432

DECLARATION OF CHUCK EASTTOM

TABLE OF CONTENTS

I.	INTRODUCTION	4
II.	QUALIFICATIONS	5
III.	MATERIALS CONSIDERED	9
IV.	SCOPE OF OPINIONS	9
V.	RELATED DISTRICT COURT CASE	10
VI.	LEGAL STANDARDS	12
	A. Claim Construction.....	13
	B. Obviousness.....	14
	C. Motivations to Combine.....	16
VII.	LEVEL OF ORDINARY SKILL IN THE ART	17
VIII.	CLAIM CONSTRUCTION	18
IX.	TECHNOLOGY BACKGROUND.....	19
	A. Near Field Communications (“NFC”)	19
	B. Session Initiation Protocol (“SIP”)	21
X.	U.S. PATENT NO. 10,674,432 (“’432 Patent”) (Ex. 1001)	22
	A. Priority Date	22
	B. ’432 Patent Overview	23
	C. The ’432 Patent’s Prosecution History	24
XI.	ASSERTED REFERENCES	26
	A. Jain (Ex. 1017)	26
	B. Dua (Ex. 1018)	33
XII.	THE CHALLENGED CLAIMS OF THE ’432 PATENT WOULD NOT HAVE BEEN OBVIOUS.....	36
	A. Petitioner’s Ground 1 Fails Because the Claims Would Not Have Been Obvious in View of Jain	36
	1. Jain Does Not Disclose and Would Not Have Rendered Obvious “a method of operating a smartphone in performing a plurality of financial transactions.”	37
	2. Jain Does Not Disclose and Would Not Have Rendered Obvious “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” 46

a. Turning on the Transaction Card’s Antenna is not the Claimed “Enabling a Mode to Communicate” 47

b. Petitioner Lacks a Sufficient Motivation to Combine Elements of Method 700 and Method 900 48

3. Jain Does Not Disclose and Would Not Have Rendered Obvious “enabling a mode to communicate by the smartphone information requesting an authorization” and “receiving by the smartphone second data from the first device responsive to said transmitting by the smartphone the first data” 50

4. Jain Does Not Disclose and Would Not Have Rendered Obvious “detecting by the smartphone that a proximity condition is satisfied.” 55

B. Petitioner’s Ground 2 Fails Because The Claims Would Not Have Been Obvious In View Of Dua.....56

1. Dua Does Not Disclose and Would Not Have Rendered Obvious “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.” 57

a. Dua’s “Card-Issuing” Theory Fails 57

b. Dua’s “External-Storage-Authentication” Theory Fails.....62

2. Dr. Almeroth fails to establish that Dua discloses detecting that a proximity criterion is satisfied.....64

XIII. SUMMARY AND OTHER REMARKS 70

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 Invalidity Contentions (Feb. 3, 2025)
2006	Exhibit 432-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 the claims in U.S. Patent No. 10,674,432 (“the ’432 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 proceeding. 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 a hearing 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 '432 Patent, at least one of ordinary skill in the art.

III. MATERIALS CONSIDERED

14. I have reviewed the '432 Patent, including the challenged claims, its prosecution history, and the relevant patent family. The '432 Patent was marked as Exhibit 1001, and its prosecution history was marked as Exhibit 1009.

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 in the art at the time of the invention of the '432 Patent.

IV. SCOPE OF OPINIONS

18. I set forth my opinions throughout this declaration.

19. I understand that Petitioner argues that Claims 1-17 of the ‘432 Patent (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 ‘432 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 LC 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:

- IPR2025-00974, regarding U.S. Patent No. 10,674,432 (the instant Petition)

- 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
- IPR2025-00975, 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
- IPR2025-00978, regarding U.S. Patent No. 12,028,793

25. I also understand Patent Owner is asserting the '432 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 a person 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 in the art (“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 of 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 ¶82. I disagree that a POSITA should be required to have experience in secure wireless communications as Dr. Almeroth contends. The claims of the '432 Patent do not require that the communications be "secure" such as encryption or encoding of the wireless communications. *E.g.*, '432 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 '432 Patent.

VIII. CLAIM CONSTRUCTION

43. I understand that Petitioner contends that "[n]o express constructions are required to find the '432 Patent claims invalid." Pet. at 7. Other than explaining the plain and ordinary meaning of certain terms, 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 at 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 the 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. 10,674,432 (“’432 Patent”) (Ex. 1001)

A. Priority Date

55. Through a series of continuation applications, the ’432 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. Ex. 1001.

56. I understand that Dr. Almeroth 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. Ex. 1002 ¶¶36-37.

B. '432 Patent Overview

57. The '432 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, 1:22-27; 6:14-25. The specification recognizes that the devices in the art were rigidly configured to perform a predetermined number of functions. *Id.*, 1:36-41. The '432 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.*, 1:45-51. 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.*, 1:41-44.

58. The '432 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.*, 6:14-20. 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.*, 6:20-25. 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.*, 6:25-31. 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.*, 6:41-50.

C. The ’432 Patent’s Prosecution History

59. I have reviewed the prosecution history of the ’432 Patent.

60. U.S. Patent Application No. 16/251,834 was filed January 18, 2019 and issued as the ’432 Patent on June 2, 2020. Ex. 1009 at 58, 356.

61. The Office issued a first Office Action on May 9, 2019. Ex. 68-77. Claims 1-8 were rejected on the ground of non-statutory obviousness-type double patenting as being unpatentable over claims 1, 6, 8-10, 16, 18-19 of Patent No. 10,219,199. Ex. 1009 at 71. Claims 1-8 were rejected under 35 U.S.C. 103 as being unpatentable over DiMartino et al (US 8,249,935) in view of LaBiche (US 2008/0140667). Ex. 1009 at 72.

62. Applicant filed a response on October 9, 2019. Ex. 1009 at 147-155. In the response, Applicant amended its claims and argued: “For example, neither DiMartino nor LaBiche, nor the combination thereof teach or suggest transmitting by the smartphone first data to a first device, the first data relating to a plurality of financial transactions to be conducted, wherein the transmitting is performed over

an air interface that differs from the first air interface over which information is sent with respect to a first transaction.” Ex. 1009 at 154.

63. The Office issued a final Office Action on December 17, 2019. Ex. 1009 at 166-179. In the final Office Action, Claims 1-19 were rejected under 35 U.S.C. 103 as being unpatentable over Dua (US 2006/0165060) in view of Creamer et al (US 2004/0143550). Ex. 1009 at 169.

64. On February 26, 2020, Applicant and the Examiner conducted an interview. Ex. 1009 at 230-231. Subsequently, on March 9, 2020, Applicant filed a request for continued examination along with a response to the final Office Action. Ex. 1009 at 233-254. Applicant noted that “Amended claim 1 recites in pertinent part: 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...” Ex. 1009 at 253. Applicant also stated:

The Final Office Action asserted that paragraphs [0026], [0089], and [0495] of Dua taught "the service parameters interaction based on the transaction reads on a physiological parameter". None of these paragraphs, however, nor anywhere else in Dua or Creamer, teach or suggest "enabling a mode to communicate ... responsive to at least one physiological parameter ... "as recited in amended claim 1. Independent claims 5, 9, and 14 include similar language.

Ex. 1009 at 253.

65. A notice of allowance was issued on April 22, 2020. Ex. 1009 at 269-278. 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 the original).

XI. ASSERTED REFERENCES

A. Jain (Ex. 1017)

66. 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 110 a.” Jain ¶[0023].

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

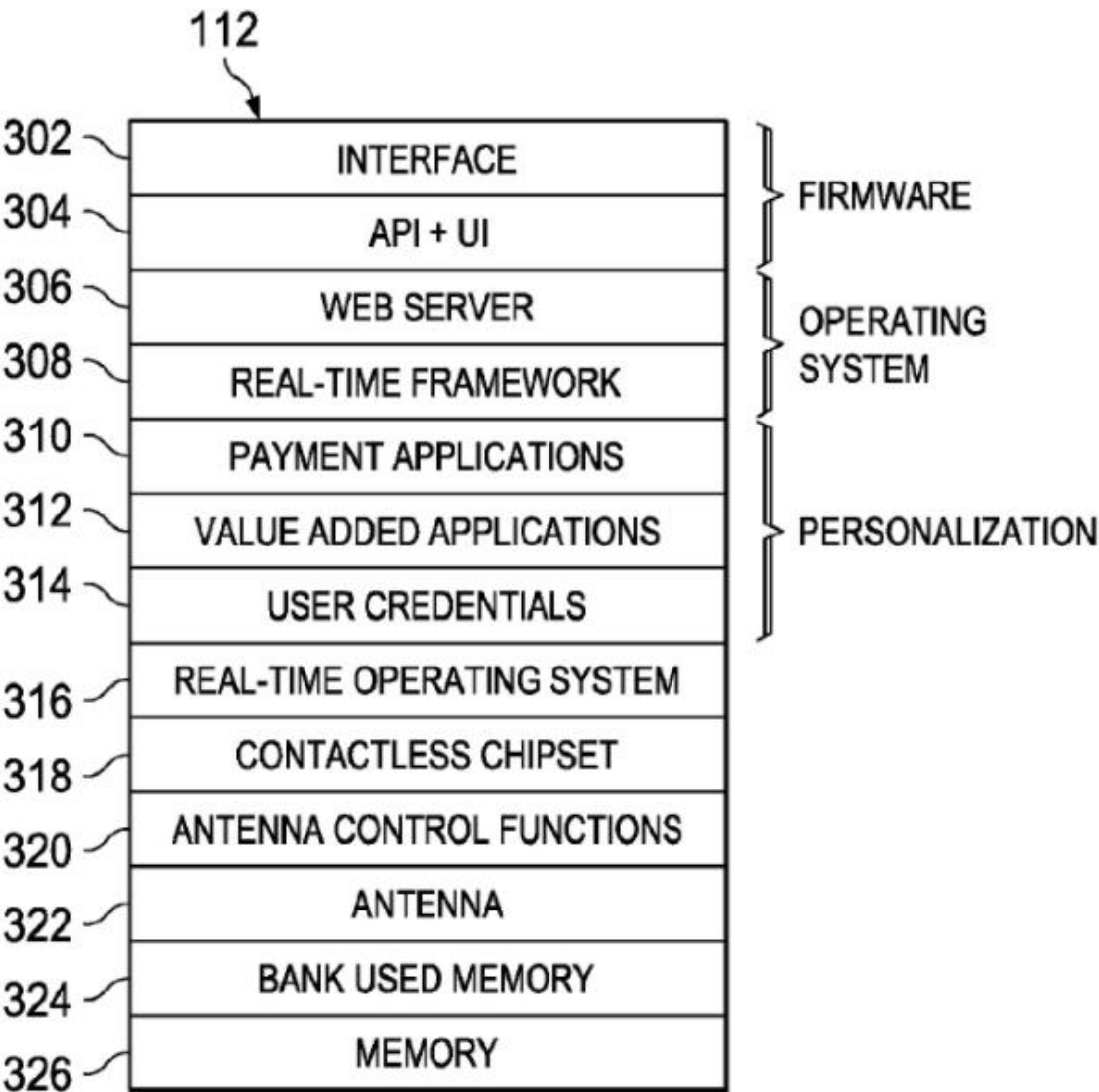


FIG. 3

Jain, Fig. 3; ¶¶[0009], [0049].

68. 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].

69. 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.

70. 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].

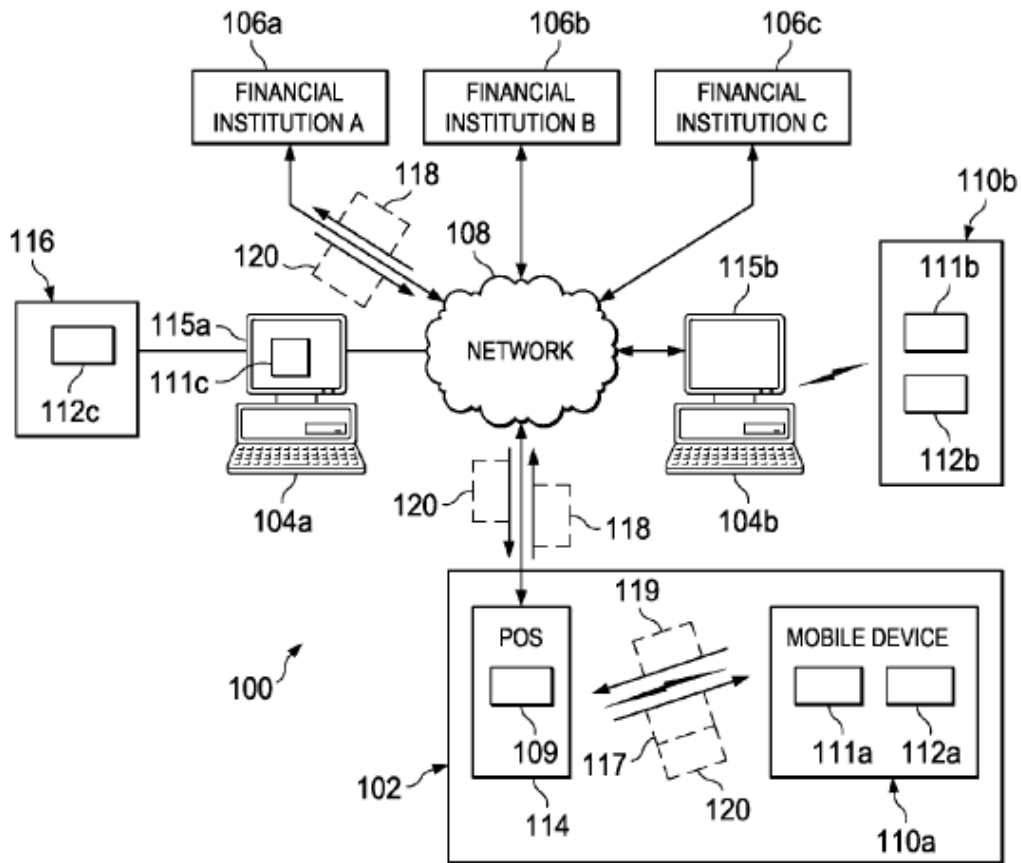


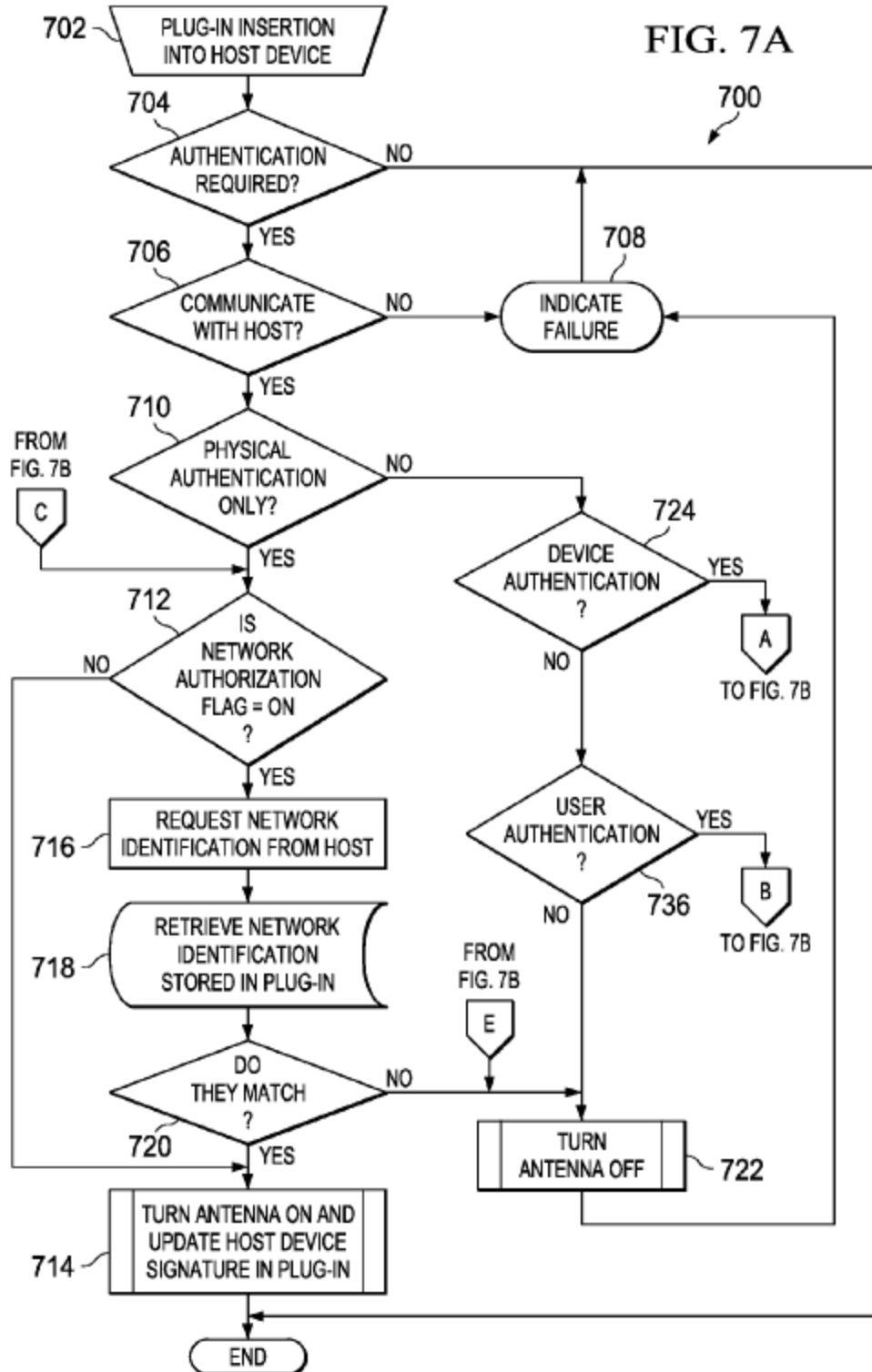
FIG. 1

71. 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 ¶[0023].

72. 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].

73. 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:



74. 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.

75. 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].

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

77. 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].

78. 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].

B. Dua (Ex. 1018)

79. United States Patent Application No. 2006/0165060 to Dua is titled "Method and Apparatus for Managing Credentials Through a Wireless Network." As noted above, the Examiner considered Dua during the prosecution of the '432 Patent and identified Dua on the face of the '432 Patent as considered art. Dua at 2.

80. 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:

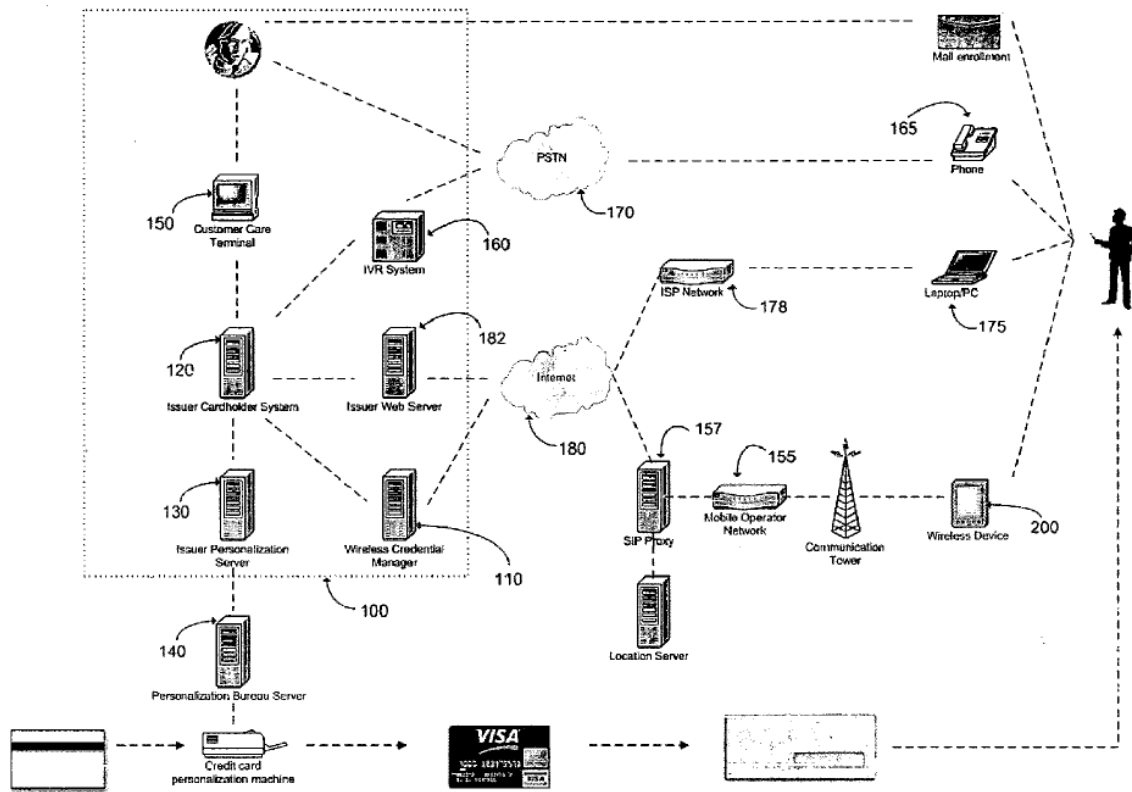


FIG. 1

Dua, Fig. 1.

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

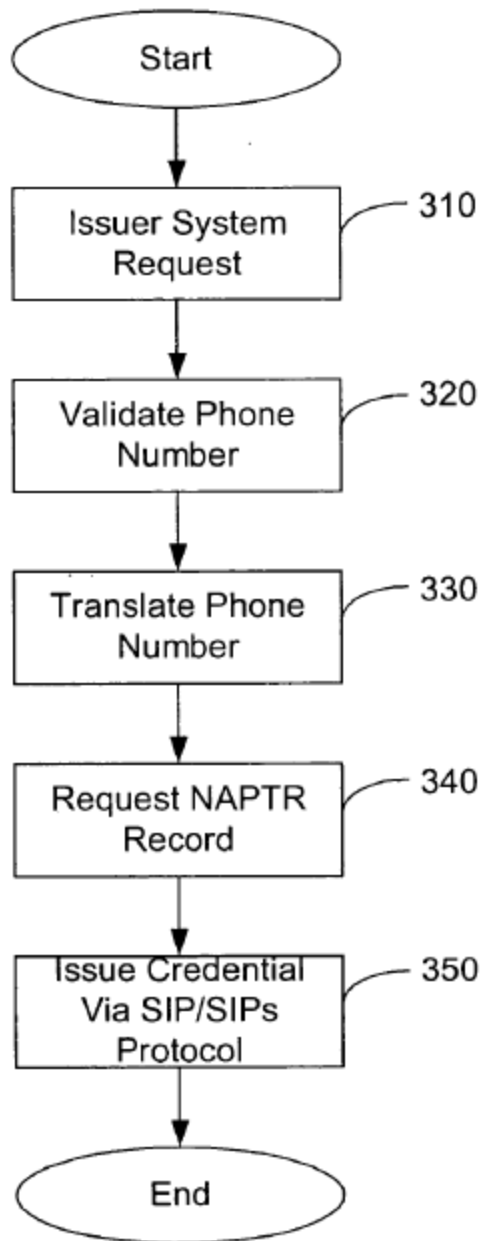


FIG. 2

Dua, Fig. 2.

82. 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].

83. 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].

84. 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 '432 PATENT WOULD NOT HAVE BEEN OBVIOUS

A. Petitioner's Ground 1 Fails Because the Claims Would Not Have Been Obvious in View of Jain

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

86. 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 and Would Not Have Rendered Obvious “a method of operating a smartphone in performing a plurality of financial transactions.”

87. Claim 1 requires “a method of operating a smartphone in performing a plurality of financial transactions.” Claim 10 similarly requires “a smartphone that is configured to perform operations associated with a plurality of financial transactions.” The preambles of these independent claims are limiting because they disclose the smartphone recited in subsequent claim limitations. All dependent claims of the ’432 Patent depend from these independent claims, and therefore, all claims of the ’432 Patent require a “smartphone.”

88. It is this claimed smartphone which performs all of the claim limitations to include transmitting by the smartphone first data to a first device, receiving by the smartphone second data from the first device, and performing a first transaction of the plurality of financial transactions. ’432 Patent, cls. 1, 10.

89. The '432 Patent contemplates a smartphone or “wireless communication device” that is itself capable of both a first and second communications mode. *Id.* at 3:9-18; 7:18-28. Similarly, it is the “mobile subscriber device 14” of the '432 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 9:25-34. The '432 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 ¶118 (pointing to the receipt of an activation code *of the mobile device* as the claimed “receiving by the smartphone *second data* from the first device responsive to said transmitting by the smartphone the first data, the second data relating to the plurality of financial transactions to be conducted and differing from the first data”) (emphasis added); Ex. 1002 ¶129 (pointing to the the *transaction card* 112, which “may execute transactions with POS device 114 using short-range signals such as NFC (e.g., ISO 18092/ECMA 340), . . . Bluetooth, . . . proximity signals, and/or other signals compatible with retail payment terminals” as the claimed “detecting by the smartphone that a proximity condition is satisfied between the smartphone and a first entity, wherein the first entity is distinct from the first device”).

90. Whenever the '432 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.

'432 Patent, 10:40-50.

91. Thus, whenever the '432 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.

92. Dr. Almeroth first argues that Jain discloses both the “smartphone.” Ex. 1002 ¶98. Dr. Almeroth argues that Jain discloses the “smartphone” and “method of operating a smartphone” because Jain “interfaces mobile device 110 (e.g., ‘a smartphone’ (¶[0018])) with a transaction card 112 that convert[s] the mobile device 110 to a contactless payment device loaded with a financial vehicle (FV) that may be, for example, a credit card, a debit card, a gift card and/or other retail payment product (¶[0029]).” Ex. 1002 ¶100. I disagree. Jain does not disclose and would not have rendered obvious “a method of operating a smartphone in performing a

plurality of financial transactions” of claim 1 nor the “smartphone that is configured to perform operations associated with a plurality of financial transactions” of claim 10 because Jain does not disclose a single device, i.e., a smartphone, with the claimed functionality as required by the claims.

93. 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 smartphone second data from the first device responsive to said transmitting by the smartphone the first data, the second data relating to the plurality of financial transactions to be conducted and differing from the first data,” Dr. Almeroth identifies: “[i]n response to the step 924 request, mobile device 110 (*smartphone*) receives an activation code (*second data*) from the financial institution (*first device*). The received activation code is checked against a stored activation code (retrieved at step 922).” Ex. 1002 ¶118 (emphasis in original). Later, Dr. Almeroth references paragraph [0023] of Jain with regard to “performing a first transaction . . .” *Id.* ¶¶128-129. However, this paragraph of Jain relates solely to the transaction card—“[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].

94. Dr. Almeroth further argues that the Jain “transaction card 112 is part of mobile device 110 (i.e., smartphone).” Ex. 1002 ¶100 (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 transaction card is “part” of the mobile device. 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. According to 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.

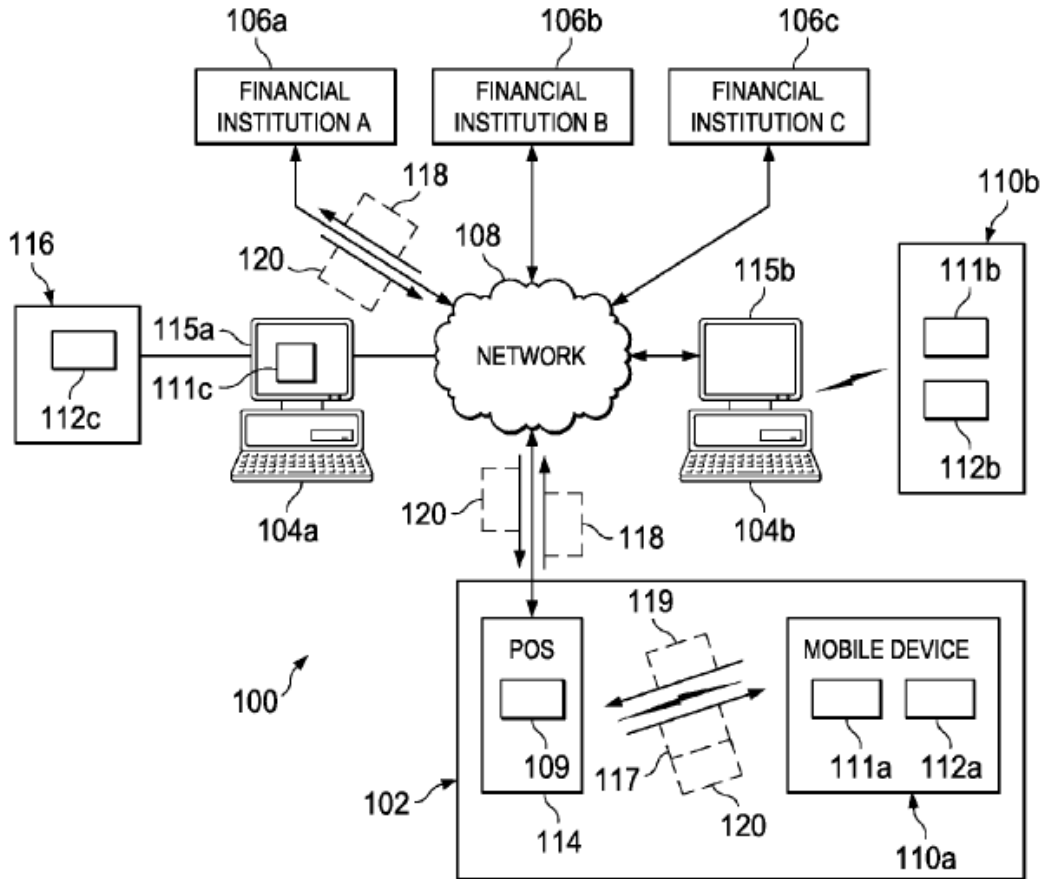


FIG. 1

95. 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 an 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.”

96. Dr. Almeroth argues that a POSITA would have understood that the Jain transaction card “can be a non-removable part of the smartphone” because the transaction card can be “software, hardware, and/or firmware” and the “mobile device 110 does not require additional hardware, software, and/or firmware.” Ex. 1002, ¶101 (citing Jain ¶[0023]). I disagree.

97. As an initial matter, Dr. Almeroth is incorrect that Jain’s transaction card “**can be** ‘software, hardware, and/or firmware.’” Ex. 1002 ¶101 (quoting Jain ¶[0023] (emphasis added)). Rather, instead of describing what the card **can be**, Jain states that the “transaction card 112 **can include** any software, hardware, and/or firmware.” Jain ¶[0023] (emphasis added). Additionally, 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 functionalities, such as NFC. *See* Jain ¶[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). 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.

98. Dr. Almeroth also argues that “[i]ntegrating transaction card 112 improves the simplicity and efficiency of the design.” Ex. 1002 ¶102. As an example, Dr. Almeroth points to the “translation or communication step between transaction card 112 and mobile device 110” as ***no longer needed*** after integrating the transaction card and the mobile device. *Id.* But Jain emphasizes, as a stated ***benefit*** of Jain’s disclosure, 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.* ¶[0035] (“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. Jain, ¶[0023]. Finally, Jain confirms that the “financial institutions 106 may assign **one or more** mobile host devices 110 to **a** transaction card 112. . . .” Jain, ¶[0041] (emphasis added). 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.

99. Next, Dr. Almeroth alleges that the integration of the mobile device and the transaction card would have been obvious because “[r]emovability of the transaction card **is also not always beneficial**.” Ex. 1002, ¶105 (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. *See 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, Jain implements security to guard against lost transaction cards, such as by way of a PIN. Jain ¶¶[0072], [0075]. Under Dr. Almeroth's theory, the inadvertent loss of a transaction card is simply replaced by the inadvertent loss of a smartphone, which provides no added benefit.

100. Therefore, Jain fails to disclose or render obvious “a method of operating a smartphone in performing a plurality of financial transactions” of independent claim 1, nor the “smartphone” of independent claim 10.

2. Jain Does Not Disclose and Would Not Have Rendered Obvious “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”

101. Claim 1 requires “***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” Claims 2 through 9 depend from claim 1, and thus also include this limitation. Claim 10 requires: “while the mode is enabled, transmitting first data to a first device as a precursor to performing the plurality of financial

transactions.” Claims 11 through 17 depend from claim 10, and thus also include this limitation.

102. Dr. Almeroth argues that Jain discloses this limitation. Ex. 1002 ¶116. I disagree.

a. Turning on the Transaction Card’s Antenna is not the Claimed “Enabling a Mode to Communicate”

103. Under limitations 1[b] and 10[b], the claimed “transmitting” occurs “*while* the mode is enabled.” See ’432 Patent, Cls. 1, 10 (emphasis added). In order to satisfy this requirement with respect to the mode to communicate being enabled, Dr. Almeroth points to method 700 and asserts that “step 714: ‘turn antenna on and update host device signature in plug-in’” is the claimed “enabling a mode to communicate.” Ex. 1002 ¶113 (citing Jain ¶¶[0072]-[0075] and Fig. 7A). That is, Dr. Almeroth equates enabling the antenna of the transaction card (*see, e.g.*, Figure 7, step 714) with the claimed “enabling a mode to communicate” and, thus, requires that the antenna of the transaction card be enabled throughout the “transmitting” step of the claims.

104. But turning on the antenna via step 714 of method 700 cannot be the claimed “enabling a mode to communicate,” and Dr. Almeroth fails to address how this mode to communicate relates to requesting an authorization as is required by the claims. As stated above, Method 700 relates to connecting or bootstrapping the transaction card to the mobile device and is unrelated to any request for authorization

(Petitioner asserts that the request for authorization happens in a different method). Limitation 1[b] requires the smartphone to “transmit[] by the smartphone first data to a first device, the first data relating to a plurality of financial transactions to be conducted” *while* the mode to communicate is enabled. Instead of a request for authorization, once the transaction card’s antenna is turned on by step 714 of method 700, Jain’s bootstrapped system of the mobile device and the transaction card is ready to perform financial transactions. *See* Jain ¶[0073] (“As for the example, the transaction card 112 *may activate the antenna for wireless transactions . . .*”) (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). Step 714 is unrelated to any request for authorization. Accordingly, step 714 of method 700 does not disclose “enabling a mode to communicate by the smartphone information requesting an authorization.” *See* ’432 Patent, Cls. 1, 10. No other steps are required or follow Jain’s enablement of the antenna of the transaction card.

b. Petitioner Lacks a Sufficient Motivation to Combine Elements of Method 700 and Method 900

105. Again, using Dr. Almeroth’s own mapping (e.g., enabling the mode is turning on the transaction card’s antenna via step 714), the claimed “transmitting” step must occur while the antenna of the transaction card is turned on. But when alleging that Jain performs the claimed “transmitting” step, Dr. Almeroth points to

a different method altogether, method 900 and Figure 9. Ex. 1002 ¶117. Dr. Almeroth alleges that Jain’s *mobile device* (not the transaction card) performs the steps of Figure 9 after a user is authenticated and the antenna of the transaction card is turned on. *Id.* I disagree.

106. It is my opinion that method 900 is unrelated to method 700 and uses the antenna on the mobile device, *not* the antenna on the transaction card as in Figure 7. See Jain ¶[0063] (“As illustrated, the intelligent card 400 includes *an antenna 402*”) (emphasis added); see also *id.* ¶[0081] (“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); see also *id.* (“If the activation code is not manually entered by the user, then at step 920, the transaction card wirelessly transmits a request for the activation code *using the cellular radio technology of the host device.*”) (emphasis added). Turning on the transaction card’s antenna by the process of method 700 does not impact the execution of method 900.

107. Dr. Almeroth cites no disclosure suggesting that method 900 will occur following method 700 or while the transaction card’s antenna is enabled as a result of method 700. Jain likewise does not support Dr. Almeroth’s unsupported interpretation. Indeed, 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]. A POSITA would have understood that Method 900 pertains to activating a previously inactive card or account.

108. Dr. Almeroth does not explain why a POSITA would have been motivated to combine methods 700 and 900 and, in my opinion, a POSITA would not have combined them given that they relate to different hardware and unrelated processes. 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 “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” in limitation 1[b] and 10[b].

3. *Jain Does Not Disclose and Would Not Have Rendered Obvious “enabling a mode to communicate by the smartphone information requesting an authorization” and “receiving by the smartphone second data from the first device responsive to said transmitting by the smartphone the first data”*

109. Claim 1 requires “enabling a mode to communicate by the smartphone information requesting an authorization.” Claim 10 similarly requires “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.” Petitioner and Dr. Almeroth treat these limitations as substantively identical. Pet. at 44-45. Claims 2 through 9 depend from claim 1, and thus also include this limitation. Claims 11 through 17 depend from claim 10, and thus also include this limitation. Dr. Almeroth argues that Jain discloses this limitation. *E.g.*, Ex. 1002 ¶118. I disagree.

110. 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 ¶¶115 (explaining that requesting an authorization is explained in limitations 1[b] and 1[c]), 119. 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 asserts that “the request sent by the smartphone to a financial institution—devices in an enterprise that authorize transactions through the network by accepting data from clients and returning appropriate responses (Jain ¶¶[0038]-[0039])—constitutes ***requesting an authorization.***” Ex. 1002 ¶122 (emphasis in original).

111. But Dr. Almeroth fails to explain how this requested activation code can be the claimed “second data” that is received after “requesting an authorization” 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, which occurs at step 920. *See id.* ¶[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.”). Jain relies on the transaction card itself to perform the authentication. *See id.* (“If the locally stored information matches the provided information at decisional step 924, then at step 926, the transaction card is activated.”). 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).

112. 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 the activation code sent by the financial institution cannot be the claimed “second data.”

113. Next, Dr. Almeroth argues that a POSITA would “understand that Jain’s request for activation code to the financial institution (step 920) is a request for authorization.” Ex. 1002 ¶124. 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.” Ex. 1002 ¶124 (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].

114. 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.*

115. 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 ¶125 (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.

116. Dr. Almeroth fails to establish that Jain discloses or would have rendered obvious “enabling a mode to communicate by the smartphone information

requesting an authorization” in independent claim 1 or “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” of independent claim 10.

4. Jain Does Not Disclose and Would Not Have Rendered Obvious “detecting by the smartphone that a proximity condition is satisfied.”

117. Claims 1 and 10 require “detecting by the smartphone that a proximity condition is satisfied between the smartphone and a first entity.” Claims 2 through 9 depend from claim 1, and thus also include this limitation. Claims 11 through 17 depend from claim 9, and thus also include this limitation.

118. Dr. Almeroth argues that Jain discloses this limitation. Ex. 1002 ¶128. I disagree.

119. In support of his position, Dr. Almeroth first misquotes Jain. Dr. Almeroth alleges that “[t]he *mobile device* first ‘wirelessly receive[s] a request from the POS device 114 to execute a transaction and/or . . . provide a response.’” Jain ¶[0023].” Ex. 1002 ¶[129] (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* (not the mobile device) as capable of “execut[ing] transactions with the POS

device 114 using short range signals such as NFC.” Jain ¶[0023]. 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 “detecting” step must be performed by the smartphone 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 “detecting by the smartphone that a proximity condition is satisfied.” *See supra* Section XII.A.1.

120. Next, Dr. Almeroth argues that Jain renders this limitation obvious. Ex. 1002 ¶138. 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. *See* Jain ¶[0023]. Therefore, Jain fails to disclose or render obvious “detecting by the smartphone that a proximity condition is satisfied” in independent claims 1 and 10.

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

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

122. 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 and Would Not Have Rendered Obvious “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.”

123. Claim 1 requires “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.” Claim 10 similarly requires “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.” Petitioner and Dr. Almeroth treat these limitations as substantively identical. Pet. at 76. Claims 2 through 9 depend from claim 1, and thus also include this limitation. Claims 11 through 17 depend from claim 10, and thus also include this limitation.

124. Dr. Almeroth argues that Dua discloses this limitation under either a “Card-Issuing Theory” or an “External-Storage-Authentication Theory.” Ex. 1002 ¶213. I disagree.

a. Dua’s “Card-Issuing” Theory Fails

125. According to Dr. Almeroth, Dua’s Card-Issuing Theory states that “[a]fter matching PIN code or fingerprint is sensed, the wallet application is opened in order to be issued a credit card. The wallet application then establishes Session Initiation Protocol (“SIP”) communication session between the wireless device and

the issuer's wireless credential manager ("WCM") (*enabling a mode to communicate*).” Ex. 1002 ¶225 (citing Dua ¶¶[0046], [0104], [0128], [0178]) (emphasis in original). Dr. Almeroth points to the establishing of the SIP session as the claimed “enabling a mode to communicate.” *Id.* I disagree.

126. In rendering his opinion, Dr. Almeroth ignores that the “enabling a mode to communicate information requesting an authorization” must be “*responsive to* at least one physiological parameter having been sensed by at least one sensor of the smartphone.” 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). It is my opinion that a POSITA would have understood that communications in Dua rely on an authentication whereas a PIN is only used for transactions

127. To overcome this deficiency, Dr. Almeroth alleges that there is a relationship between opening the wallet application “requires a PIN code or alternatively, fingerprints” and the establishment of SIP communications. *See* Ex.

1002 ¶¶214-216. 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], [0366].

128. In fact, Dua does not even require the wallet to be opened prior to SIP communications. *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.”); Dua ¶[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.”). A POSITA would have understood that a PIN would not be required because the user is authenticated via a distinct protocol. Dr. Almeroth’s citations to Dua 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] (“Further, online PIN verification also gives certain credential issuers a stronger means by which to validate a person's identity 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.”). The connection via SIP is used to exchange credentials and Dua provides no support of either opening of a wallet application or requiring a separate PIN prior to such a connection.

129. Dr. Almeroth also maps the “mode to communicate by the smartphone information requesting an authorization” in this limitation to SIP communications. Ex. 1002 ¶225. But Dua discloses that “SIP is used to invite one or more participants

to a session” and that the SIP message contains “information about what media encodings (for example, voice, video) the parties can and will use.” *See* Dua ¶[0110]; *see also id.* ¶[0093] (“SIP (Session Initiation Protocol, RFC 3261) is a text-based application protocol that allows two endpoints in the Internet to discover one another in order to exchange context information about a session they would like to share.”); *see also id.* ¶[0048] (describing a SIP handshake).

130. But SIP is just the mechanism in which two endpoints connect and is not the transport protocol in which information, such as financial credentials, are exchanged. Indeed, Dua discloses that once the context information, such as financial credentials is exchanged, “data transmission begins, ***using an appropriate transport protocol.***” Dua . ¶[0110]. (emphasis added); *see supra* Section IX.B. And Dua distinguishes SIP from other 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” that are used for data transmission or communication. *Id.* ¶[0101]. As such, SIP, which is only used for establishing the connection, cannot satisfy the claimed “mode to communicate.” *See supra* Section IX.B. Accordingly, Dua’s “Card-Issuing” Theory fails to render this limitation obvious.

b. Dua's "External-Storage-Authentication" Theory Fails

131. Dr. Almeroth states: "Retrieving the credential from external storage requires setting up a communications session between the wallet application and external storage. A 'real-time connection is initiated between the wallet application and the storage service' by 'utiliz[ing] SIP' (*enabling a mode to communicate*)" and "Through that real-time connection, the wireless device transmits a "username/password for the wallet application to automatically access the storage area." Ex. 1002 ¶229. Dr. Almeroth later states: that the "username/password" is "transmitting by the smartphone first data." Ex. 1002 ¶233. I disagree. As claimed, there is a separate "enabling" step before the authorization is requested and then received. In contrast and in Dua, to enable SIP communication between the wallet and the storage service (the alleged enabled mode to communicate), Dua requires that the "wallet application and storage service [] exchange encryption keys for secure communication." Dua, ¶[0493]. These encryption keys include the "username/password for the wallet application to automatically access the storage area" that were established during profile setup. *Id.*, ¶[0492]. The exchange of encryption keys is part of enabling SIP communications (alleged mode to communicate). But Petitioner relies on the "username/password" to be first data and not part of the "enabling a mode to communicate," which is improper because the mode to communicate must be enabled before "transmitting by the smartphone first

data.” As such, Petitioner fails to establish that Dua teaches or would have rendered obvious “first data.” Worse, “No credential data or settings are retained in memory of the wireless device after a transaction is completed” (Dua ¶[0495]) further confirming that Dua did not teach and would have rendered obvious “first data” given that first data (and second data) is related “to a *plurality* of financial transactions to be conducted.”

132. Dr. Almeroth also argues that, under Dua’s “External-Storage-Authentication” Theory, “retrieval of credentials from the external storage is only possible after (*responsive to*) sensing a PIN code or fingerprint (*physiological parameter*) as part of opening the wallet.” Ex. 1002 ¶227 (citing Dua ¶¶[0353]-[0354], [0366], [0429]) (emphasis in original). Dr. Almeroth again points to establishing a SIP session as the claimed “enabling the mode to communicate.” Ex. 1002 ¶229. Again, I disagree because the SIP session is not responsive to either of Dr. Almeroth’s proffered parameters. Dr. Almeroth relies on his arguments related to the Card Issuing Theory, i.e., that “Dua’s requirement that the user enter a PIN code or provide a fingerprint to open Dua’s wallet discloses or at least renders obvious the claimed *sensing*.” *Id.* ¶228 (emphasis in original). 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 id.* ¶[0129].

133. Therefore, Dua fails to disclose or render obvious, in either its “Card-Issuing” Theory or its “External-Storage-Authentication” Theory, “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” in independent claim 1 or “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” in independent claim 10.

2. *Dr. Almeroth fails to establish that Dua discloses detecting that a proximity criterion is satisfied.*

134. Claims 1 and 10 require “detecting by the smartphone that a proximity condition is satisfied...” Claims 2 through 9 depend from claim 1, and thus also include this limitation. Claims 11 through 17 depend from claim 10, and thus also include this limitation.

135. Dr. Almeroth asserts that Dua discloses this limitation. Ex. 1002 ¶¶236-237. I disagree.

136. Dr. Almeroth alleges that Dua “teaches that its short-range communications protocol may be NFC.” Ex. 1002 ¶237.¹ 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*

¹ Dr. Almeroth pivots to disclosures in the ECMA 340 standard for NFC (Ex. 1002 ¶¶238-242) – disclosures that are not incorporated into Dua, are not referenced in Dua, and which Dr. Almeroth never establishes would be obvious to combine with Dua. In fact, Dua never mentions ECMA.

id. ¶[0101] (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.”).

137. 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].

138. 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].

139. 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.

140. 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.

141. 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 ¶242. 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 ¶242. 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).

142. 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.

143. Because Dr. Almeroth does not show that Dua discloses the proximity condition of the ’432 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 or would have rendered obvious "detecting by the smartphone that a proximity condition is satisfied" in independent claims 1 and 10.

XIII. SUMMARY AND OTHER REMARKS

144. 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.

145. 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 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