UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.,

Petitioner,

v.

TELCOM VENTURES LLC.,

Patent Owner.

U.S. Patent No. 9,462,411

"Mobile device mode enablement responsive to a proximity criterion"

DECLARATION OF KEVIN ALMEROTH, PH.D., IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 9,462,411

TABLE OF CONTENTS

LIST OF EXHIBITS

Ex.	Description
EX1001	U.S. Patent No. 9,462,411 ("'411 patent")
EX1002	Declaration of Kevin Almeroth, Ph.D.
EX1003	Exhibit Intentionally Omitted
EX1004	Curriculum Vitae of Dr. Kevin Almeroth, Including List of Recent Expert Witness Engagements of Dr. Kevin Almeroth
EX1005	Prosecution History for U.S. Pat. No. 9,462,411
EX1006	Prosecution History for U.S. Pat. No. 9,832,708
EX1007	Prosecution History for U.S. Pat. No. 10,219,199
EX1008	Prosecution History for U.S. Pat. No. 10,660,015
EX1009	Prosecution History for U.S. Pat. No. 10,674,432
EX1010	Prosecution History for U.S. Pat. No. 11,304,118
EX1011	Prosecution History for U.S. Pat. No. 11,770,756
EX1012	Prosecution History for U.S. Pat. Appl. Pub. No. 2023/0403631
EX1013	Prosecution History for U.S. Pat. No. 11,924,743
EX1014	Prosecution History for U.S. Pat. No. 11,937,172
EX1015	Prosecution History for U.S. Pat. No. 12,028,793
EX1016	Patent Owner's District Court Infringement Chart for '411 Patent
EX1017	U.S. Pub. No. 2009/0069049 ("Jain")
EX1018	U.S. Pub. No. 2006/0165060 ("Dua")
EX1019	U.S. Pub. No. 2010/0082481

EX1020	U.S. Pub. No. 2010/0082490
EX1021	U.S. Pub. No. 2009/0307140
EX1022	"Product Overview", Vivotech (Jun. 27, 2007), https://web.archive.org/web/20070627155330/ http://www.vivotech.com/products/vivo_pay/index.asp
EX1023	"Kyocera Wireless Mobile Phones Excel in Cellular South WirelessWallet Consumer Trial", Kyocera (Oct. 18, 2007), https://americas.kyocera.com/press-releases/press-releases_201503201874.htm
EX1024	U.S. Pub. No. 2005/0137977
EX1025	U.S. Pub. No. 2001/0026632
EX1026	NTT DoCoMo FOMA F900iC Basic Manual
EX1027	Jain et al., "An Identity-Authentication System" (Sep. 1997)
EX1028	U.S. Patent No. 6,957,339
EX1029	Jin et al., "Biohashing: two factor authentication featuring fingerprint data and tokenised random number" (Apr. 27, 2004)
EX1030	Bhargav-Spantzel, "Privacy Preserving Multi-Factor Authentication with Biometrics" (2006)
EX1031	"About NFC Technology", NFC Forum (Jun. 15, 2006), https://web.archive.org/web/20060615050709/http://www.nfc-forum.org/aboutnfc/about_nfc_technology/
EX1032	Erik Rolf & Viktor Nilsson, "Near Field Communication (NFC) for Mobile Phones" (Aug. 2006)
EX1033	Wall Street Journal, Vivotech (Aug. 12, 2005), https://web.archive.org/web/20060915080521if_/http://www.vivotech.com:80/newsroom/coverage/Videos/Wall_Street_Journal/Wall_Street_Journal.wmv

EX1034	Near Field Communication - Interface and Protocol (NFCIP-1), Standard ECMA-340 (December 2002)
EX1035	NFC Forum News Conference, NFC Forum (June 5, 2006)
EX1036	Dean A. Gratton, "Developing Practical Wireless Applications", Elsevier Digital Press (2007)
EX1037	Jacki Katzman, "NFC Forum Unveils Technology Architecture and Announces Initial Specifications and Mandatory Tag Format Support", NFC Forum, at 3 (June 5, 2006)
EX1038	Exhibit Intentionally Omitted
EX1039	U.S. Pub. No. 2010/0082445
EX1040	Exhibit Intentionally Omitted
EX1041	Exhibit Intentionally Omitted
EX1042	"iPhone Premieres This Friday Night at Apple Retail Stores", Apple (Jun. 28, 2007), https://www.apple.com/newsroom/2007/06/28iPhone-Premieres-This-Friday-Night-at-Apple-Retail-Stores/
EX1043	Exhibit Intentionally Omitted
EX1044	Exhibit Intentionally Omitted
EX1045	Exhibit Intentionally Omitted
EX1046	Exhibit Intentionally Omitted
EX1047	Near Field Communication - Interface and Protocol (NFCIP-1), Standard ECMA-340 (2nd Edition, December 2004)

I, Dr. Kevin Almeroth, declare as follows:

I. Introduction

1. I have been retained by Quinn Emanuel Urquhart & Sullivan, LLP on behalf of the Petitioner Samsung Electronics Co., Ltd. ("Petitioner") as an independent expert in this *inter partes* review (this "Proceeding") before the Patent Trial and Appeal Board of the United States Patent and Trademark Office (the "Board") to review claims 1-4 ("the challenged claims") of U.S. Patent No. 9,462,411 ("the '411 patent"). I have been asked by the Petitioner to assist in evaluating the claims and the disclosure of the '411 patent.

A. Qualifications

2. EX1004 is a true and correct copy of my current CV, which describes my education, patents and publications, employment and research history, and professional activities and awards.

1. Educational Background

3. I hold three degrees from the Georgia Institute of Technology: (1) a Bachelor of Science degree in Information and Computer Science (with minors in Economics, Technical Communication, and American Literature) earned in June 1992; (2) a Master of Science degree in Computer Science (with specialization in Networking and Systems) earned in June 1994; and (3) a Doctor of Philosophy (Ph.D.) degree in Computer Science (Dissertation Title: Networking and System

Support for the Efficient, Scalable Delivery of Services in Interactive Multimedia System, minor in Telecommunications Public Policy) earned in June 1997. I have taken a wide variety of courses as demonstrated by my minor. My undergraduate degree also included a number of courses more typical of a degree in electrical engineering, including digital logic, signal processing, and telecommunications theory.

2. Career

4. I am a Professor Emeritus in the Department of Computer Science at the University of California, Santa Barbara (UCSB). While active at UCSB, I held faculty appointments and was a founding member of the Computer Engineering (CE) Program, Media Arts and Technology (MAT) Program, and the Technology Management Program (TMP). I was the Associate Director of the Center for Information Technology and Society (CITS) from 1999 to 2012. I have been a faculty member at UCSB since July 1997.

5. One of the major concentrations of my research has been the delivery of multimedia content and data between computing devices, including various network architectures. In my research, I have studied large-scale content delivery systems, and the use of servers located in a variety of geographic locations to provide scalable delivery to hundreds or thousands of users simultaneously. I have also studied smaller-scale content delivery systems in which content is exchanged

between individual computers and portable devices. My work has emphasized the exchange of content more efficiently across computer networks, including the scalable delivery of content to many users, mobile computing, satellite networking, delivering content to mobile devices, and network support for data delivery in wireless networks.

6. In 1992, the initial focus of my research was on the provision of interactive functions (*e.g.*, VCR-style functions like pause, rewind, and fast-forward) for near video-on-demand systems in cable systems; in particular, how to aggregate requests for movies at a cable head-end and then how to satisfy a multitude of requests using one audio/video stream broadcast to multiple receivers simultaneously. This research has continually evolved and resulted in the development of techniques to scalably deliver on-demand content, including audio, video, web documents, and other types of data, through the Internet and over other types of networks, including over cable systems, broadband telephone lines, and satellite links.

7. An important component of my research has been investigating the challenges of communicating multimedia content, including video, between computers and across networks including the Internet. I have worked on a variety of research problems and used a number of systems that were developed to deliver multimedia content to users. One content-delivery method I have researched is the

one-to-many communication facility called "multicast," first deployed as the Multicast Backbone, a virtual overlay network supporting one-to-many communication. Multicast is one technique that can be used on the Internet to provide streaming media support for complex applications like video-on-demand, distance learning, distributed collaboration, distributed games, and large-scale wireless communication. The delivery of media through multicast often involves using Internet infrastructure, devices and protocols, including protocols for routing and TCP/IP.

8. Starting in 1997, I worked on a project to integrate the streaming media capabilities of the Internet together with the interactivity of the web. I developed a project called the Interactive Multimedia Jukebox (IMJ). Users would visit a web page and select content to view. The content would then be scheduled on one of a number of channels, including delivery to students in Georgia Tech dorms delivered via the campus cable plant. The content of each channel was delivered using multicast communication.

9. More recently, I have also studied issues concerning how users choose content, especially when considering the price of that content. My research has examined how dynamic content pricing can be used to control system load. By raising prices when systems start to become overloaded (*i.e.*, when all available resources are fully utilized) and reducing prices when system capacity is readily

available, users' capacity to pay as well as their willingness can be used as factors in stabilizing the response time of a system. This capability is particularly useful in systems where content is downloaded or streamed on-demand to users.

10. Protecting networks, including their operation and content, has been an underlying theme of my research almost since the beginning of my research career. Starting in 2000, I have been involved in several projects that specifically address security, network protection, and firewalls. After significant background work, a team on which I was a member successfully submitted a $4.3M grant proposal to the Army Research Office (ARO) at the Department of Defense to propose and develop a high-speed intrusion detection system. Key aspects of the system included associating streams of packets and analyzing them for viruses and other malware. Once the grant was awarded, we spent several years developing and meeting the milestones of the project. A number of my students worked on related projects and published papers on topics ranging from intrusion detection to developing advanced techniques to be incorporated into firewalls. I have also used firewalls, including their associated malware detection features, in developing techniques for the classroom to ensure that students are not distracted by online content.

11. Recent work ties some of the various threads of my past research together. I have investigated content delivery in online social networks and proposed reputation management systems in large-scale social networks and

marketplaces. On the content delivery side, I have looked at issues of caching and cache placement, especially when content being shared and the cache has geographical relevance. We were able to show that effective caching strategies can greatly improve performance and reduce deployment costs. Our work on reputation systems showed that reputations have economic value, and as such, creates a motivation to manipulate reputations. In response, we developed a variety of solutions to protect the integrity of reputations in online social networks. The techniques we developed for content delivery and reputation management were particularly relevant in peer-to-peer communication.

12. My involvement in the research community extends to leadership positions for several academic journals and conferences. I am the co-chair of the Steering Committee for the ACM Network and System Support for Digital Audio and Video (NOSSDAV) workshop and on the Steering Committees for the International Conference on Network Protocols (ICNP), ACM Sigcomm Workshop on Challenged Networks (CHANTS), and IEEE Global Internet (GI) Symposium. I have served or am serving on the Editorial Boards of IEEE/ACM Transactions on Networking, IEEE Transactions on Mobile Computing, IEEE Network, ACM Computers in Entertainment, AACE Journal of Interactive Learning Research (JILR), and ACM Computer Communications Review. I have co-chaired a number of conferences and workshops including the IEEE International Conference on

Network Protocols (ICNP), IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), International Conference on Communication Systems and Networks (COMSNETS), IFIP/IEEE International Conference on Management of Multimedia Networks and Services (MMNS), the International Workshop On Wireless Network Measurement (WiNMee), ACM Sigcomm Workshop on Challenged Networks (CHANTS), the Network Group Communication (NGC) workshop, and the Global Internet Symposium, and I have served on the program committees for numerous conferences.

13. Furthermore, in the courses I taught at UCSB, a significant portion of my curriculum covered aspects of the Internet and network communication including the physical and data link layers of the Open System Interconnect (OSI) protocol stack, and standardized protocols for communicating across a variety of physical media such as cable systems, telephone lines, wireless, and high-speed Local Area Networks (LANs). The courses I have taught also cover most major topics in Internet communication, including data communication, multimedia encoding, and mobile application design. My research and courses have covered a range of physical infrastructures for delivering content over networks, including cable, Integrated Services Digital Network (ISDN), Ethernet, Asynchronous Transfer Mode (ATM), fiber, and Digital Subscriber Line (DSL). For a complete list of courses I have taught, see my curriculum vitae (EX1004).

14. I co-founded a technology company called Santa Barbara Labs that was working under a sub-contract from the U.S. Air Force to develop very accurate emulation systems for the military's next generation internetwork. Santa Barbara Labs' focus was in developing an emulation platform to test the performance characteristics of the network architecture in the variety of environments in which it was expected to operate, and, in particular, for network services including IPv6, multicast, Quality of Service (QoS), satellite-based communication, and security. Applications for this emulation program included communication of a variety of multimedia-based services, including video conferencing and video-on-demand.

15. In addition to having co-founded a technology company myself, I have worked for, consulted with, and collaborated with companies for nearly 30 years. These companies range from well-established companies to start-ups and include IBM, Hitachi Telecom, Turner Broadcasting System (TBS), Bell South, Digital Fountain, RealNetworks, Intel Research, Cisco Systems, and Lockheed Martin.

16. Additional details about my employment history, fields of expertise, and publications are further included in my CV (EX1004).

3. Other Relevant Qualifications

17. I am a Member of the Association of Computing Machinery (ACM) and a Fellow of the Institute of Electrical and Electronics Engineers (IEEE).

18. As an important component of my research program, I have been involved in the development of academic research into available technology in the market place. One aspect of this work is my involvement in the Internet Engineering Task Force (IETF). The IETF is a large and open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. I have been involved in various IETF groups including many content delivery-related working groups like the Audio Video Transport (AVT) group, the MBone Deployment (MBONED) group, Source Specific Multicast (SSM) group, the Inter-Domain Multicast Routing (IDMR) group, the Reliable Multicast Transport (RMT) group, the Protocol Independent Multicast (PIM) group, etc. I have also served as a member of the Multicast Directorate (MADDOGS), which oversaw the standardization of all things related to multicast in the IETF. Finally, I was the Chair of the Internet2 Multicast Working Group for seven years.

19. I am an author or co-author of approximately 200 technical papers, published software systems, IETF Internet Drafts and IETF Request for Comments (RFCs). A complete list of my publications is in my CV (EX1004).

20. I have been awarded numerous teaching awards, including Computer Science Outstanding Faculty Member (1997-98, 1998-99, 1999-2000, 2004-06,

UCSB Spotlight on Excellence Award (2000-01), and UCSB Academic Senate Distinguished Teaching Award (2006-07).

B. Previous Expert Witness Testimony

21. The list of recent matters in which I have testified can be found in EX1004.

C. Preparation for this Declaration

22. In forming my opinions, I have considered the ’411 patent specification, including the Abstract, the figures, and the claim language itself, as would have been understood by a person of ordinary skill in the art as of the priority date of the ’411 patent (a “POSITA”). My understanding of “POSITA” and “priority date” are set forth below. I have also reviewed the file history of the ’411 patent, the Exhibits that are listed in the list of Exhibits, and any other material cited in this declaration.

23. In forming my opinions, I have relied on my personal knowledge and professional experience, and on the documents and information referenced in this declaration.

24. This declaration explains, based on facts and information available to me to date, the subject matter and opinions related to this Proceeding. As such, I am prepared to provide expert testimony regarding opinions formed resulting from my

analysis of the issues considered in this declaration if asked about those issues by the Board or by the private parties' attorneys.

25. Additionally, I may discuss my own work, teachings, and knowledge of the state of the art in the relevant time period. I may rely on handbooks, textbooks, technical literature, and the like to demonstrate the state of the art in the relevant period and the evolution of relevant technologies.

26. Throughout this declaration, I refer to specific pages of the '411 patent and other documents. The citations are intended to be exemplary and are not intended to convey that the citations are the only source of evidence to support the propositions for which they are cited.

27. I am being compensated for my time spent on this matter at a rate of $850 per hour, and my compensation is in no way contingent upon the outcome of this matter or on the opinions I offer. All of the opinions expressed in this declaration are my own.

II. Legal Understanding

28. In this section, I describe my understanding of certain legal standards that I have relied upon in forming my opinions set forth in this declaration. I have been informed of these legal standards by Petitioner's attorneys. I am not an attorney and I have not thoroughly researched the law on patent invalidity. I am relying only on instructions from Petitioner's attorneys for these legal standards.

A. Claim Construction

29. I have been instructed by counsel that claim construction is a matter of law for the arbiter of law to decide. I understand that in an *inter partes* review, claims are construed using the same claim construction standard that would be used to construe the claim in a civil action.

30. I understand that a patent may include two types of claims, independent claims and dependent claims. An independent claim stands alone and includes only the limitations it recites. A dependent claim can depend on an independent claim or another dependent claim. I understand that a dependent claim includes all the limitations that it recites in addition to the limitations recited in the claim from which it depends.

B. Anticipation

31. I understand that a patent claim is anticipated when a single piece of prior art describes every element of the claimed invention, either expressly or inherently, arranged in the same way as in the claim. For inherent anticipation to be found, it is required that the missing descriptive material is necessarily present in the prior art. I understand that, for the purpose of an *inter partes* review, prior art that anticipates a claim can include both patents and printed publications from anywhere in the world.

C. Obviousness

32. I understand that a patent claim is unpatentable and invalid if the subject matter of the claim as a whole would have been obvious to a POSITA as of the time of the invention at issue. My understanding of a POSITA is set forth below. I understand that the following factors must be evaluated to determine whether the claimed subject matter is obvious: (1) the scope and content of the prior art; (2) the difference or differences, if any, between each claim of the patent and the prior art; and (3) the level of ordinary skill in the art at the time the patent was filed. Unlike anticipation, which allows consideration of only one item of prior art, I understand that obviousness may be shown by considering more than one item of prior art. Moreover, I have been informed and I understand that the so-called objective indicia of non-obviousness, also known as "secondary considerations," are also to be considered when assessing obviousness. These include: (1) commercial success; (2) long-felt but unresolved needs; (3) copying of the invention by others in the field; (4) initial expressions of disbelief by experts in the field; (5) failure of others to solve the problem that the inventor solved; and (6) unexpected results. I also understand that evidence of objective indicia of non-obviousness must be commensurate in scope with the claimed subject matter.

III. The '411 Patent

33. The '411 patent is titled "Mobile device mode enablement responsive to a proximity criterion."

34. The '411 patent lists inventors Peter D. Karabinis and Rajendra Singh and issued October 4, 2016.

A. Priority Date

35. The '411 patent claims priority to U.S. Patent Application No. 12/264,711, filed on November 4, 2008.

B. Specification

36. The specification assumes familiarity with a "wireless communications device" such as "a wireless terminal, a wireless/mobile phone, a Personal Digital Assistant (PDA), a smart phone, a multi-media device including Global Positioning System (GPS) capability, etc." EX1001 at 2:60-64; *id*. at 1:35-50. It further relies on long-established, generic concepts of computer systems such as "authorization" (5:26-28 et seq.), "sensors" capable of detecting, inter alia, physiological input (mentioned only at 5:65-6:9), "short-range communications" (mentioned in the specification only at 8:14-19 and 8:41-50), "air interface[s]" (6:36-52 et seq., with a recitation of then-existing interfaces at 7:3-13), and "communications service[s]" (8:64-66 et seq.). For example, the specification acknowledges that the "adaptivity and mobility aspects of wireless communications" were already "important in

people's lives" at the time of alleged invention. EX1001 at 1:15-16. It also assumes, in the "Background of the Invention" section, that mobile phones could act as digital wallets. EX1001 at 1:24-27. The specification does not disclose or purport to disclose new or improved means of sensing (including physiological/biometric sensing) or proximity detection.

37. At the heart of the disclosure is a mobile wireless device (element 14 in Figure 1) that "may be configured to enable one or more modes/functions" of itself or of another device "responsive to a proximity criterion having been satisfied." EX1001 at 2:60-3:2. The proximity criterion is a measure of how close the wireless device (or the second device) is to an "entity" such as a person, product for sale, or POS terminal. EX1001 at 3:3-17, 3:31-39. For example, the device may determine proximity using well knowns means such as detecting a low-power or short range signal radiated from a (third) device (element 16 in Figure 1) that is part of or associated with the entity. *See* EX1001 at 3:17-21, 3:40-67.

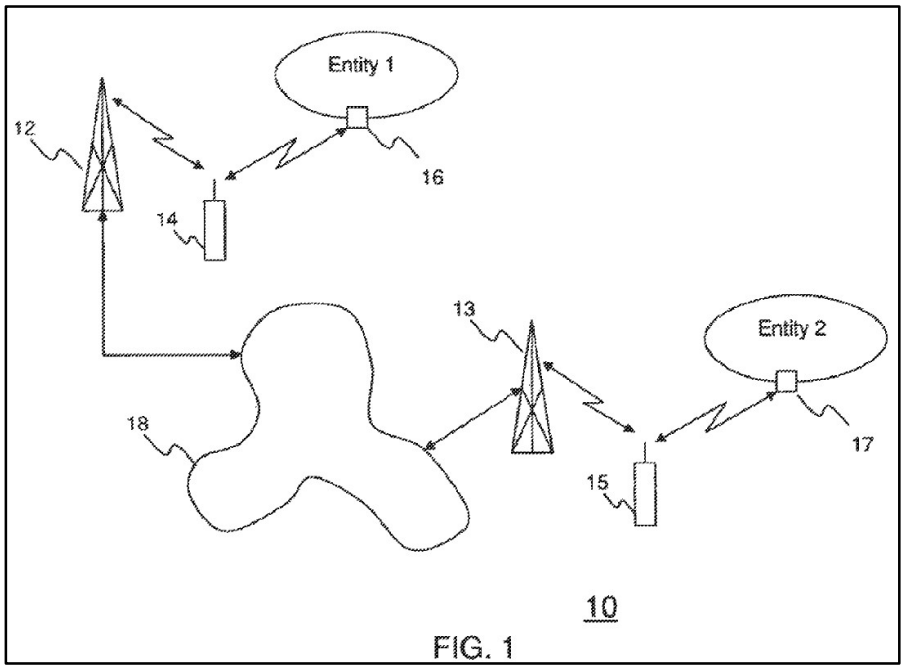


FIG. 1

C. Prosecution History

1. '411 Patent File History

38. The '411 Patent was filed as U.S. Patent Application No. 12/264,711 on November 4, 2008 and issued October 4, 2016.

39. Throughout prosecution, the Examiner rejected the claims of the '411 patent nine times, primarily on obviousness grounds. EX1005 at 74, 127, 197, 240, 295, 330, 382, 420, 453. Accordingly, Applicant amended the claims substantially, including a final Examiner's Amendment for allowance. EX1005 at 108, 166, 220, 266, 316, 351, 407, 434, 498. The breadth of the claims caused many of these rejections and amendments. EX1005 at 410 ("The Examiner also indicated that our response should make it clear where support for any claim amendments are found, and how these claim amendments distinguish over the cited art, as the claims are

broad. The undersigned indicated that the claims are broad, but that their filing date of November 4, 2008 is quite early relative to the claimed invention.").

40. For claim 1's sensing of physiological data, Applicant argued to distinguish prior art where the relevant fingerprint sensor was not "smartphone-based." EX1005 at 484. Further, Applicant distinguished the prior art because the cited prior art, US 2007/0197261 ("Humbel") indicated that "the combination of NFC transceiver plus biometric finger sensor did not yet exist in a mobile phone at the time of filing of Humbel." EX1005 at 483.

41. For the sequencing of limitations in claim 1, Applicant conceded in an amendment that "the 'detecting' has been moved after the 'sensing' in the claim in order to provide proper antecedent basis for the 'living organism,' and to also indicate that the 'detecting' and the 'sensing' can occur in either order and/or simultaneously." EX1005 at 435.

42. Applicant argued throughout several amendments that claim 1's "selectively communicating … responsive to the proximity criterion and a value of the physiological data … and refraining …" distinguished it from prior art. EX1005 at 225, 272, 274, 322, 354, 356, 357, 411, 437. Within these amendments, Applicant exchanged "preferentially" for "selectively." EX1005 at 407. Further, Applicant argued to distinguish this limitation from prior art where there "is no refraining ... because communications using both air interfaces takes place." EX1005 at 356; *see*

also EX1005 at 355 ("both air interfaces would come into play simultaneously"). Additionally, Applicant argued to distinguish prior art where the communication "selections are based purely on which mode is enabled, but neither mode is selected preferentially, and neither mode is avoided, based on any criteria other than the selected mode." EX1005 at 357.

2. '708 Patent File History

43. U.S. Patent Application No. 15/251,882 was filed August 30, 2016, and issued on November 28, 2017, as U.S. Patent No. 9,832,708 ("'708 patent"). It is a continuation of above-discussed U.S. Patent Appl. No. 12/264,711, which issued as U.S. Patent No. 9,462,411.

44. The Examiner rejected the claims for double patenting over the '411 patent and obviousness. EX1006 at 59, 60. In response, Applicant conceded that "[a] smartphone that concurrently performs the recitations (i) and (iii) of independent Claims 1 and 5 may function as a mobile wallet or a 'digital wallet.'" At 110. Applicant argued to distinguish Claims 1 and 5 based from the cited prior art because "a mutually exclusive selection in Gallagher of either (a) the licensed wireless communications session 106 or (b) the JCS access interface 110 does not disclose or suggest the concurrent performance recited in independent Claims 1 and 5." EX1006 at 111.

45. Regarding "enabling," Applicant argued to distinguish prior art where "merely enabling detection of entry of the mobile terminal into the zone of coverage of the localization point does not disclose or suggest enabling a function of the mobile terminal." EX1006 at 117.

46. Applicant further argued to distinguish the cited prior art based on the limitation that "the entity is not involved in providing the communications service." EX1006 at 113. Specifically, the prior art taught "two alternative paths for accessing the voice and data network," which the Applicant argued "provides the opposite of the 'the entity is not involved in providing the communications service' that is received via the second air interface." EX1006 at 113.

3. '199 Patent File History

47. U.S. Patent Application No. 15/800,885 was filed November 1, 2017 and issued on February 26, 2019 as U.S. Patent No. 10,219,199 ("'199 patent"). It is a continuation of above-discussed U.S. Patent Application No. 15/251,882, which issued as U.S. Patent No. 9,832,708.

48. The Examiner required an election by Applicant for a group of the claims, and Applicant elected "Claims 1-8, drawn to a smartphone to provide information an entity using a first air interface, and a second air interface." EX1007 at 70, 88. Additionally, the Examiner rejected for double patenting "[c]laims 1, 4 are rejected on the ground of non-statutory obviousness-type double patenting as

being unpatentable over claims 1, 11, 16, 18 of Patent No. 9,832,708." EX1007 at 108. Applicant responded with a terminal disclaimer. EX1007 at 157. Finally, the Examiner rejected claims of the '199 patent as obvious. EX1007 at 110.

49. For the "proximity condition," Applicant argued to distinguish the prior art because the particular device detecting "would do so using its (a) server rather than its (b) wireless client … therefore [it] does not disclose or suggest detecting by a smartphone that a proximity condition is satisfied between the smartphone and an entity." EX1007 at 184-85.

50. Applicant also argued to distinguish the "wirelessly providing by the smartphone information to the entity" because the prior art "discusses that its server sends 'a set of parameters for use in accessing a second wireless access point using the second air interface' … [it] does not disclose or suggest that its set of parameters includes a physiological parameter." EX1007 at 185.

51. Applicant argued that prior art disclosing "CDMA (which stands for Code Division Multiple Access) ... does not disclose or suggest that 'the second air interface is based upon an Orthogonal Frequency Division Multiplexed (OFDM) and/or Orthogonal Frequency Division Multiple Access (OFDMA) protocol." EX1007 at 185-86.

4. '015 Patent File History (Unasserted)

52. U.S. Patent Application No. 16/012,513 was filed June 19, 2018, and issued as U.S. Patent No. 10,660,015 ("'015 patent", not asserted) on May 19, 2020. It is a division of above-described U.S. Patent Application No. 15/800,885, which issued as U.S. Patent No. 10,219,199.

53. The Examiner rejected the claims as obvious four times. EX1008 at 67, 117, 157, 207. Applicant amended the claims and the Examiner provided an amendment before allowance. EX1008 at 101, 191, 254.

54. Specifically, the Examiner rejected claims 1, 4-9, and 11-15 "as being unpatentable over Dua (US 2006/0165060), hereinafter 'Dua,' in view of Todd et al. (US 8,091,780), hereinafter 'Todd,' further in view of Garberg et al (US 6,944,981), hereinafter 'Garberg.'" EX1008 at 207. The Applicant responded to the rejection on account of Dua by authorizing, during an interview, an Examiner amendment to the claims with "shopping cart" language. EX1008 at 253-57.

5. '432 Patent File History

55. U.S. Patent Application No. 16/251,834 was filed January 18, 2019, and issued June 2, 2020, as U.S. Patent No. 10,674,432 ("'432 patent"). It is a continuation of above-discussed U.S. Patent Application No. 15/800,885, which issued as U.S. Patent No. 10,219,199.

56. The Examiner rejected the pending claims 1-8 for double patenting "over claims 1, 6, 8-10, 16, 18-19 of Patent No. 10,219,199." EX1009 at 71. Applicant submitted a terminal disclaimer for the '199 patent. EX1009 at 262.

57. Additionally, the Examiner rejected the claims as obvious. EX1009 at 72, 169. Applicant substantially amended the claims in response. EX1009 at 154, 242. Specifically, the Examiner rejected all of the pending claims "under 35 U.S.C. 103 as being unpatentable over Dua (US 2006/0165060), hereinafter 'Dua', in view of Creamer et al (US 2004/0143550), hereinafter 'Creamer.'" EX1009 at 169. The Applicant amended claims 1 and 5, attempting to avoid Dua with the limitation of "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." EX1009 at 275-276.

6. '118 Patent File History (Unasserted)

58. U.S. Patent Application No. 15/929,609 was filed May 12, 2020, and issued as unasserted U.S. Patent No. 11,304,118 ("'118 patent") on April 12, 2022. It is a continuation of above-discussed U.S. Patent Application No. 16/012,513, which issued as (unasserted) U.S. Patent No. 10,660,015.

59. The Examiner rejected Claims 1, 6-8, 16, 18, and 23-24 for double patenting "over claims 1-2, 5, 9-10, 12, 16, of Patent No. 10,660,015." EX1010 at 64. Applicant submitted a terminal disclaimer for the '015 patent. EX1010 at 209.

60. The Examiner rejected the claims as obvious twice. EX1010 at 66, 138. First, Applicant amended the claims to "identify one or more products removed from the one or more product carrying regions based on information from the one or more sensors." EX1010 at 128. Second, Applicant amended claim 1 to include "wherein the system is configured to verify an identify of an individual in connection with the transaction based on sensing a physiological parameter." EX1010 at 206.

7. '756 Patent File History

61. U.S. Patent Application No. 17/653,748 was filed March 7, 2022, and issued as U.S. Patent No. 11,770,756 ("'756 patent") on September 26, 2023. It is a continuation of above-discussed U.S. Patent Application No 15/929,609 filed May 12, 2020, which issued as (unasserted) U.S. Patent No. 11,304,118.

62. The Examiner rejected the pending claims 1, 9, 16, 22 for double patenting "over claims 1, 7, 17 of Patent No. 11,304,118." EX1011 at 105. Applicant submitted a terminal disclaimer for the '118 patent. At 148. The Examiner rejected the claims as obvious. EX1011 at 106.

63. First, Applicant argued that the prior art failed to "teach anything relating to 'disabling a function of the device.' In fact, a global word search of Abell does NOT return anything relating to 'disabling.'" EX1011 at 136.

64. Second, Applicant argued that the prior art failed to teach "physiological parameter satisfy[ing] any criterion" because it "simply senses and transmits the sensed value without teaching any examination (or comparison) thereof with anything else in order to determine whether or not that which is sensed satisfies any criterion." EX1011 at 136-37.

65. Finally, Applicant made what it characterized as "non substantive" amendments to claim 1. EX1011 at 158, 164.

8. U.S. Patent Application Publication No. 2023/0403631 (pending)

66. Currently pending U.S. Patent Application No. 18/450,517 was filed August 16, 2023, and published as U.S. Patent Application Publication No. 2023/0403631 on December 14, 2023. It is a continuation of above-discussed U.S. Patent Application No. 17/653,748, which issued as U.S. Patent No. 11,770,756.

67. The Examiner rejected the pending claims 1 and 9 for double patenting "1, 11, 14 of Patent No. 11,770,756." EX1012 at 230. Applicant submitted a terminal disclaimer for the '756 patent. EX1012 at 251. The Examiner rejected the claims as

obvious two times. EX1012 at 232, 259. The Applicant amended the claims and responded to the final office action rejection. EX1012 at 251, 274.

68. In arguing an amendment, Applicant equated "physiological state" to "physiological parameter." EX1012 at 252 ("Applicant respectfully asserts that one of ordinary skill in the art to which this invention belongs would interpret 'sensing a parameter' that is a 'physiological state' to mean that the parameter that is sensed is a 'physiological parameter'"). "Stated differently, a parameter that is associated with a living entity is another way of saying a 'physiological parameter.'" EX1012 at 253.

9. '172 Patent File History

69. U.S. Patent Application No. 18/523,863 was filed November 29, 2023, and issued on March 19, 2024, as U.S. Patent No. 11,937,172 ("'172 patent"). It is a division of U.S. Patent Application No. 18/489,517, filed on October 18, 2023; which is a continuation of U.S. Patent Application No. 18/450,517, filed on August 16, 2023; which is a continuation of U.S. Patent Application No. 17/653,748, filed on March 7, 2022, and issued as U.S. Patent No. 11,770,756 on September 26, 2023; which is a continuation of U.S. Patent Application No. 15/929,609, filed on May 12, 2020, and issued as U.S. Patent No. 11,304,118 on April 12, 2022; which is a continuation of U.S. Patent Application No. 16/012,513, filed on June 19, 2018, and issued as U.S. Patent No. 10,660,015 on May 19, 2020; which is a division of U.S.

Patent Application No. 15/800,885, filed November 1, 2017, and issued on February 26, 2019, as U.S. Patent No. 10,219,199; which is a continuation of U.S. Patent Application No. 15/251,882, filed August 30, 2016, and issued as U.S. Patent No. 9,832,708 on November 28, 2017; which is a continuation of U.S. Patent Application No. 12/264,711, filed on November 4, 2008, and issued as U.S. Patent No. 9,462,411 on October 4, 2016.

70. The Examiner allowed the claims of the ’172 patent without any rejections. The Examiner noted on allowance that the closest prior art of record (U.S. Patent Application Publication No. 2009/0058637) failed to teach or suggest claims 1 and 9’s limitations “receiving by the smartphone second data from the first device, comprising the authorization…” EX1014 at 348-49.

10. ’793 Patent File History

71. U.S. Patent Application No. 18/539,020 was filed December 13, 2023, and issued as U.S. Patent No. 12,028,793 (“’793 patent”) on July 2, 2024. It is a continuation of above-described pending U.S. Patent Application No. 18/450,517.

72. The Examiner rejected the pending claims 1-11 for double patenting “over claims 1-5, 9-13, 16-18, 22-24, 26 and 27 of U.S. Patent No. 11,770,756.” EX1015 at 243. Applicant submitted a terminal disclaimer for the ’756 patent. EX1015 at 189. This is the first application in the family not examined by the original examiner.

D. Level of Ordinary Skill in the Art

73. I understand that a person of ordinary skill in the art ("POSITA") is a hypothetical person who is presumed to be aware of all pertinent art, thinks along conventional wisdom in the art, and is a person of ordinary creativity—not an automaton. In deciding the level of ordinary skill, I understand that the following factors may be considered:

- The levels of education and experience of persons working in the field;
- The types of problems encountered in the field; and
- The sophistication of the technology.

74. I understand that the asserted claims of the asserted patents must be evaluated from the perspective of a POSITA. In my opinion, the relevant art for this patent relates to smartphones authenticating users and transmitting data (*e.g.*, to perform financial transactions), *i.e.*, applications for secure wireless communications. I understand that the relevant point in time for determining the qualifications of a person of ordinary skill in the state-of-the-art is the time of the alleged invention, which I assume to be the earliest effective filing date for the patent. Here, I understand that the earliest alleged priority date is November 4, 2008.

75. In my opinion, a person of ordinary skill in the art at the time of the '411 patent ("POSITA") 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. This level of skill is approximate, and more experience would compensate for less formal education, and vice versa.

76. I meet these criteria now and met them at the time of the alleged invention. I have applied this level of skill in my analysis. My opinions would not change if a slightly higher or lower level of ordinary skill applied.

E. Claim Construction

77. I have been instructed by Petitioner to perform my technical analysis of the disclosures of the prior art by applying the plain and ordinary meaning of all claim terms. I have not been asked to opine on the correctness of any claim constructions.

78. I reserve the right to provide additional opinions concerning claim construction or the application of certain claim constructions to the prior art, as appropriate, and to respond to any particular claim construction-related argument advanced by PO and/or its expert.

79. As described in more detail in the remainder of this declaration, the prior art discloses or renders obvious the challenged claims under any reasonable potential claim interpretation.

F. Challenged Claims

80. I understand that claims 1-4 are at issue in Petitioner's petition for *inter partes* review. They are reproduced below for reference.

Claim	Limitation
1[pre]	A method comprising:
1[a]	sensing by a smartphone, using a smartphone-based sensor, physiological data associated with a living organism;
1[b]	detecting that a proximity criterion is satisfied between the smartphone and an entity, wherein the entity is not the living organism;
1[c]	selectively communicating by the smartphone using a first air interface of a plurality of air interfaces with which the smartphone is capable of communicating, responsive to the proximity criterion having been detected as being satisfied and responsive to a value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor;
1[d]	refraining from communicating by the smartphone using the first air interface absent said value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor satisfying a criterion, even though the proximity criterion is detected as being satisfied;
1[e]	selectively sending information by the smartphone to one or more other devices and receiving information by the smartphone from the one or more other devices responsive to said value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor satisfying the criterion; and
1[f]	communicating by the smartphone using a second air interface of the plurality of air interfaces with which the smartphone is capable of communicating that differs from the first air interface.

Claim	Limitation
2[pre]	The method according to claim 1, wherein said detecting that a proximity criterion is satisfied between the smartphone and an entity comprises:
2[a]	detecting that a proximity criterion of less than 10 meters in distance is satisfied between the smartphone and the entity;
2[b]	wherein the detecting is performed by the smartphone, by a device that is associated with the entity, by a system that is associated with the smartphone, or a combination thereof.
3[pre]	A smartphone comprising:
3[a]	a processor that is configured to control the smartphone to perform operations comprising:
3[b]	sensing, using a smartphone-based sensor, physiological data associated with a living organism;
3[c]	detecting that a proximity criterion is satisfied between the smartphone and an entity, wherein the entity is not the living organism;
3[d]	selectively communicating using a first air interface of a plurality of air interfaces with which the smartphone is capable of communicating, responsive to the proximity criterion having been detected as being satisfied and responsive to a value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor;
3[e]	refraining from communicating using the first air interface absent said value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor satisfying a criterion, even though the proximity criterion is detected as being satisfied;
3[f]	selectively sending information to one or more other devices and receiving information from the one or more other devices responsive to said value of the physiological data associated with a living

Claim	Limitation
	organism that was sensed by the smartphone using the smartphone-based sensor satisfying the criterion; and
3[g]	communicating using a second air interface of the plurality of air interfaces with which the smartphone is capable of communicating that differs from the first air interface.
4[pre]	The smartphone according to claim 3, wherein said detecting that a proximity criterion is satisfied between the smartphone and an entity comprises:
4[a]	detecting that a proximity criterion of less than 10 meters in distance is satisfied between the smartphone and the entity.

IV. State of the Art

81. As the ’411 patent recognizes, even before the patent’s priority date, mobile phones could communicate using a variety of wireless protocols and frequencies that were well known at the time of alleged invention in late 2008. EX1001 at 1:35-61. The market for mobile phones capable of cellular network communications had been well-established since the 1990s, with the Nokia 3210 released in 1999 eventually selling over 160 million units. Manufacturers added other standardized wireless communication technology to mobile phones by the early 2000s. The first IEEE standard for Wi-Fi (802.11) was published in 1997, and by 2005 phones with both cellular and Wi-Fi communication capabilities, such as the 2005 Samsung SCH-i730, were common. So too were phones with Bluetooth capabilities, such as the Nokia 6310 and, again, the Samsung SCH-i730.

82. Near Field Communications (NFC), which allows for short-range wireless communication using RFID technology (more specifically, magnetic field induction), facilitating communication between devices in close proximity, was also common at that time. Examples of mobile phones with integrated NFC capabilities include the 2004 Fujitsu F900ic, the 2004 Nokia 3220 NFC Shell, and the 2007 Nokia 6131 NFC.

83. Manufacturers quickly began exploring applications to leverage devices that had both cellular capabilities and these secondary communication capabilities. One of those applications was mobile payment. Mobile payment technology was commercially deployed as early as 2004 in Japan with NTT Docomo's support of the Sony FeliCa chip for mobile phones coupled with Osaifu-Keitai ("Wallet Mobile") software. This technology was also deployed in the United States, with mobile phone and payment companies teaming up to conduct pilot programs of their own mobile payment software, including a 2006 pilot by Nokia and MasterCard, a 2007 pilot program by Motorola and Discover, a 2007 pilot by Kyocera and MasterCard, and companies such as ViVOtech releasing full mobile payment solutions. *See* EX1022:

See also screenshot from EX1033:

84. As mobile phones (which were evolving into smartphones) were increasingly used for sensitive activities (*e.g.*, financial transactions) and to store sensitive user data (*e.g.*, payment account information), mobile phone security received industry attention. One security mechanism that gained popularity in the early 2000s was biometric authentication. By the early 2000s, fingerprint scanners were routinely integrated into mobile phones, such as the 2000 SAGEM MC 959, the 2003 Fujitsu F505i, the 2004 Pantech GI100, and the 2007 Toshiba G500 and G900. For example, the 2007 Kyocera and MasterCard trial used mobile phones with

fingerprint scanners and required biometric authentication. EX1023 (describing Kyocera trial of "mobile payment technology" from ViVOtech with "biometric security, with fingerprint scanners from Atrua Technologies for transactional security on the test handsets").

V. Grounds

Ground	Basis	Reference	Claims
1	§103	Jain (U.S. Pat. Appl. Pub. No. 2009/0069049)	1-4
2	§103	Dua (U.S. Pat. Appl. Pub. No. 2006/0165060)	1-4

A. Ground 1: Jain (EX1017)

1. Background

85. Jain is the March 12, 2009, publication of U.S. Patent Application No. 12/205,807, which was filed on September 5, 2008, claims priority to provisional application No. 60/971,813 filed on September 12, 2007, and is assigned to Device Fidelity, Inc. EX1017. Jain is prior art to the '411 patent under at least pre-AIA 35 U.S.C. § 102(e). Jain was not considered by the Examiner during prosecution of the '411 patent.

86. Jain describes systems and methods for interfacing intelligent transaction cards with mobile devices, such as smartphones with a Graphical User Interface (GUI), to wirelessly execute financial transactions with retail point-of-sale

(POS) terminals. *See* Jain ¶¶[0005], [0018]. The transaction card works together with a smartphone to provide a user with the ability to wirelessly execute transactions with financial institutions and point-of-sale (POS) retail terminals to enable users to use the smartphone for mobile payments. *See* Jain ¶[0019]. Jain describes various examples of how the transaction card interfaces with the smartphone to provide end-to-end transactions, with reference to Figure 1, shown below:

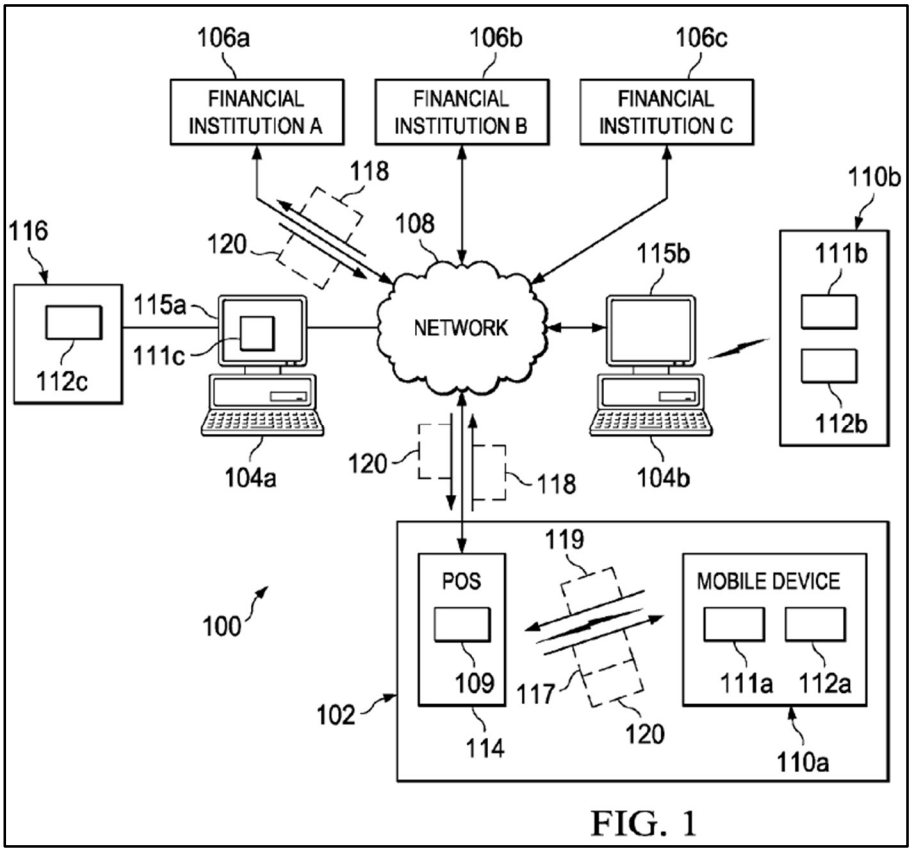
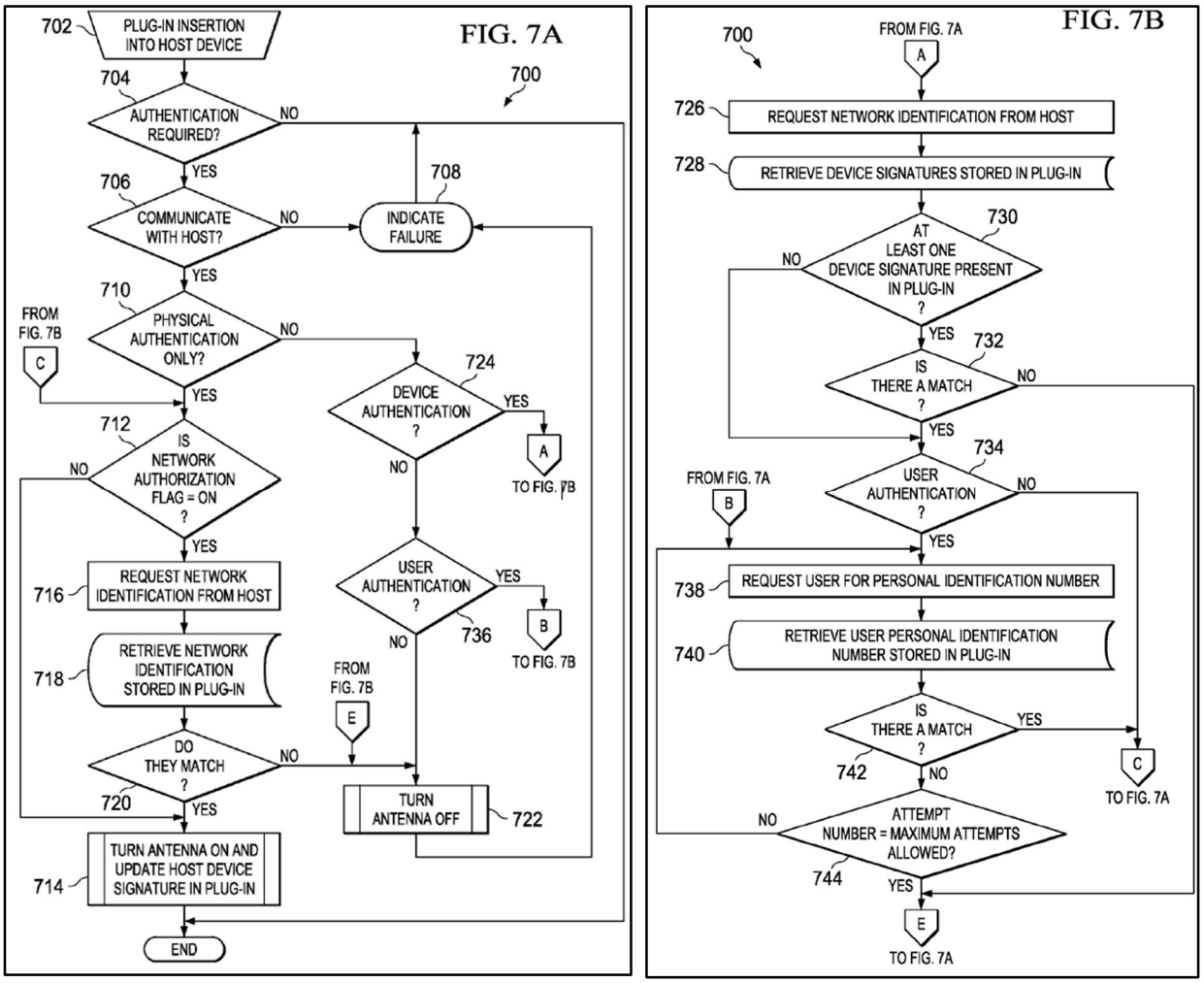


FIG. 1

87. Figure 1 shows a customer's mobile device 110a with transaction card 112a and GUI 111a wirelessly executing transactions with a nearby POS device 114.

See Jain ¶[0019]. The POS device 114 transmits transaction request 117 to the transaction card 112 of mobile device 110 requesting a transaction response 119 that identifies information associated with a payment account including account number, transaction amount, user credentials, and/or other information. Jain ¶[0027]. The mobile device transaction response 119 generates a transaction authorization request 118 that is transmitted to the financial institution 106 (shown as either 106a, 106b, or 106c) to authorize the payment transaction. Jain ¶[0027]. The financial institution transmits authorization response 120 to the POS device 114, which in turn transmits it to the mobile device's transaction card 112, and may include, for example, a payment transaction receipt presentable to the user through the mobile device's GUI 111. Jain ¶[0027]. The exchange between the mobile device's transaction card 112 and POS device 14 uses short range signals such as near-field communication (NFC), Bluetooth, or Radio Frequency Identifier (RFID) and other signals compatible with retail payment terminals. Jain ¶[0023].

88. The transaction card 112 of the mobile device may first need to be authenticated with the mobile host device as part of an "automatically bootstrapping" operation. Fig. 7A and 7B illustrate those procedures, such as in response to detecting that the transaction card has been inserted into the mobile host device. Jain ¶[0072].



Jain at Fig. 7B. Once the transaction card 112 is detected by the mobile device 110 at step 702, the mobile host device begins the authentication process. The mobile device requests the user to be authenticated at step 738 using information such as biometric information (*e.g.*, fingerprint) or requests that the user enter a PIN through the GUI. Jain ¶[0075]. The mobile device next authenticates the user with the financial institution and updates the mobile host device signature, thereby allowing the transaction card 112 to integrate with mobile device 110. Jain ¶[0075]. If this

bootstrapping operation is unsuccessful, then transaction card 112 return to its state prior to being inserted into mobile device 110. Jain ¶[0065].

89. After a transaction card has been authenticated, Jain discloses a separate process to activate the transaction card. This activation enables the financial institution to transmit information, such as authorization response 120, directly to the mobile device 110 via a cellular network. Jain ¶[0019]. Figure 9 illustrates an example for activating the transaction card using GUI 111 of the mobile device 110. Jain ¶[0081].

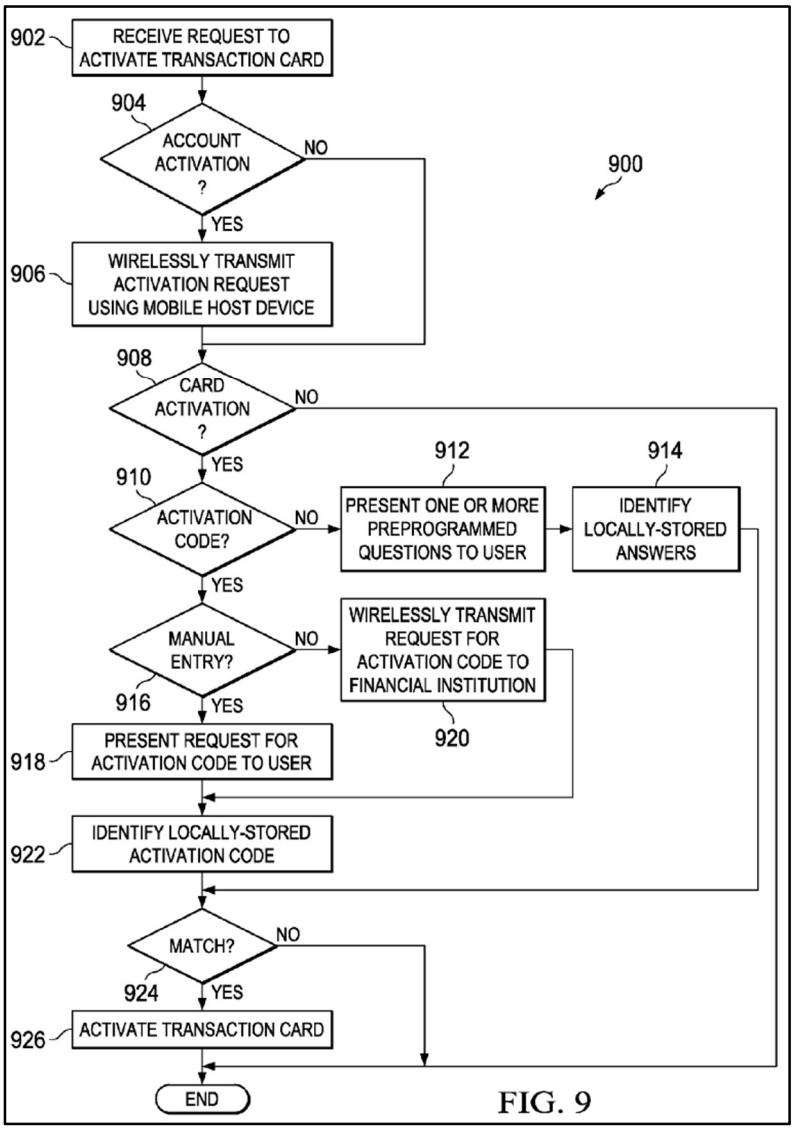


FIG. 9

90. To activate the transaction card, the mobile device wirelessly communicates with the financial institution using cellular radio to transmit an activation request at step 906 and activates the transaction card at step 926 in response to a user entering a matching activation code or PIN through the GUI 111. Jain at [0081], FIG. 9.

91. Thus, in my opinion and as further explained below, Jain discloses every one of the purportedly novel steps of the '411 patent's claimed method and smartphone, which roughly consist of: (1) sensing physiological data associated with a living organism (*e.g.*, a user of the smartphone); (2) detecting if the smartphone is in the proximity of some other entity that is not the living organism (*e.g.*, a "store" or "check-out counter in a store"); (3) selectively communicating information to another device (*e.g.*, a payment terminal) if both of the foregoing criterion are met while also refraining from communicating if they are not; and (4) also communicating over a separate "air interface" (*e.g.*, cellular or Wi-Fi)

2. Analysis

(a) Claim 1

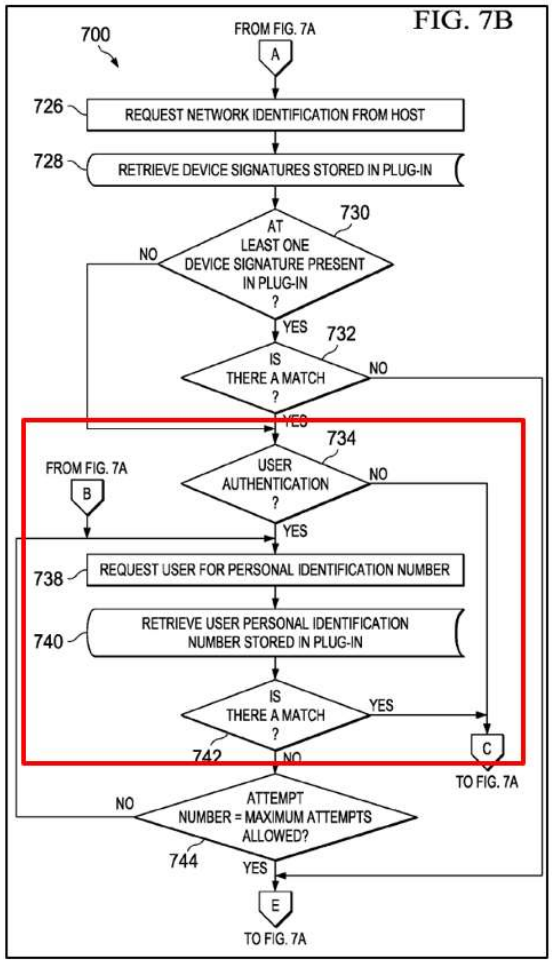
(i) 1[pre]: A method comprising:

92. In my opinion, Jain discloses this limitation. Jain describes a method comprising the steps in the remaining limitations of claim 1 as I explain in my further opinions below. *See also* Jain at Abstract ("The present disclosure is directed to a system ***and method*** for interfacing transaction cards with mobile devices. In some implementations, ***a method*** includes . . . .").

(ii) 1[a]: sensing by a smartphone, using a smartphone-based sensor, physiological data associated with a living organism;

93. In my opinion, Jain discloses this limitation in at least two instances.

94. First, Jain discloses an authentication process for "automatically bootstrapping" transaction card 112 to mobile device 110. Part of that authentication process includes authenticating a user using a PIN number or biometrics (*e.g.*, fingerprint). *See* Jain ¶¶[0072], [0075], FIG. 7B at steps 734-742:



95. Indeed, Jain discloses user authentication—whether by PIN or biometric—throughout its disclosure. Jain ¶[0065] ("the CPU 408 may execute one or more authentication processes prior to activating the intelligent card 400 and/or antenna 402 as illustrated in FIG. 7"), ¶[0066] (describing authentication), ¶[0070]

(describing adding "user authentication" through "self-select[ed] PIN authentication to prevent unauthorized use"), Table 1 ("The user can also optionally select a PIN (change Antenna availability to user authentication)").

96. In my opinion, the PIN inputted by the user constitutes ***sensing physiological data associated with a living organism***. To ***sens***[***e***] the PIN, the smartphone's touch screen or keypad constitutes ***a smartphone-based sensor*** to ***sens***[***e***] the PIN. A POSITA would understand a touch screen or keypad as sensing touch of a living organism, such as through a capacitive touch screen. *See also* EX1042. To the extent the touch has to be specific to a particular living organism (*e.g.*, a particular user), Jain validates the PIN and, as such, determines the physiological data (sequence of touches of the touchscreen) are associated with a specific user. Specifically, at step 738, the smartphone receives as user input a PIN via the smartphone's touch screen or keypad of GUI 111. Jain ¶¶[0022], [0075]. At step 740, the smartphone also retrieves a locally stored PIN. Jain ¶[0075]. Then, at step 742 ("is there a match?"), the smartphone determines whether the user-inputted PIN matches the locally-stored PIN. Jain ¶[0075], FIG. 7B.

97. In addition, Jain discloses that rather than "entering a PIN," "the user may be authenticated using … biometric information (*e.g.*, fingerprint)." Jain ¶[0075]. In this case, in my opinion, the biometric information, such as a fingerprint, provided by the user constitutes the ***physiological data associated with a living***

organism. The smartphone's biometric sensors, such as a fingerprint scanner, constitutes the ***smartphone-based sensor*** that ***sens***[***es***] the fingerprint.

98. And to the extent the fingerprint has to be specific to a particular living organism (*e.g.*, a particular user), Jain validates and authenticates the fingerprint. Specifically, for the previous discussion of Jain's steps 738, 740, and 742, the PIN can be substituted with biometric information, such as a fingerprint, and checked against a stored fingerprint for a specific user.

99. Thus, Jain discloses performing steps 738, 740, and 742, where step 738 includes sensing "biometric information" using a biometric sensor, step 740 includes retrieving locally stored biometric information, and step 742 includes determining if the sensed biometric information matches the stored biometric information. Jain ¶[0075].

100. Further confirming that this limitation is met, Patent Owner alleges in its infringement contentions in the district court litigation that the use of biometric verification is itself sufficient to show ***sensing by a smartphone, using a smartphone-based sensor, physiological data associated with a living organism***. EX1016 at 7-12.

101. It is also my opinion that, at a minimum, it would be obvious to implement Jain's teaching of "authentication using … biometric information" in this manner. Not unlike using a PIN, the purpose of biometric authentication is to ensure

biometric information of a current user matches the biometric information of the rightful owner of the device. So, the biometric information of the current user must be compared against the biometric information of the rightful owner.

102. Implementing biometric authentication on a smartphone can require obtaining the biometric information of the rightful owner, storing that information, and then using that biometric information to compare against the biometric information provided by the current user. Obtaining biometric information can be done during a setup or calibration phase. *See, e.g.*, EX1026 at 196. During the setup or calibration phase, the smartphone uses embedded sensors, such as fingerprint scanners, to scan the rightful owner's biometric information. *See, e.g.*, EX1026 at 28-29, 196. This information can be stored locally on the smartphone, and used later to compare against the biometric information of users. *See, e.g.*, EX1026 at 196; EX1024 ¶¶[0009], [0025]; EX1025 ¶¶[0044], [0086]-[0092]. Comparing, for user authentication, means that the stored and sensed biometric information are sufficiently correlated such that there is adequate confidence that the current user is the device's owner. *See, e.g.*, EX1027 at 1370-73. Specifically, for fingerprint comparisons, comparing means finding a set of features, landmarks, or minutiae in the current user's fingerprint that match with those found in the rightful owner's fingerprint, where the amount pass a certain threshold. *See, e.g.*, EX1027 at 1370-

73. Otherwise, without performing this comparison, biometric information authentication would not serve its central purpose.

103. This type of implementation was well known to a POSITA, as indicated by the numerous prior art references describing it. *See, e.g.*, EX1026 at 196; EX1024 ¶¶[0009], [0025]; EX1025 ¶¶[0044], [0086]-[0092]; EX1021 ¶¶[0040]-[0042]. For instance, U.S. Pub. No. 2005/0137977 discloses a payment device "recording a biometric profile or template of an authorized individual in it." EX1024 ¶[0009]. The biometric profile or template is later used for authentication by comparing scanned biometric data with the locally stored biometric data of an authorized individual. EX1024 ¶¶[0009], [0025]. "The biometric reader incorporated in the payment device … acquire[s] biometric measurements of a person who is attempting to use the payment device to make a proximity payment. These field biometric measurements are internally compared with the previously recorded biometric profile of the authorized individual." EX1024 ¶[0009]. Similarly, EX1025 also discloses a portable telephone receiving biometric data and comparing that biometric data to locally stored biometric data of an authorized individual. EX1025 ¶¶[0044], [0086]-[0092].

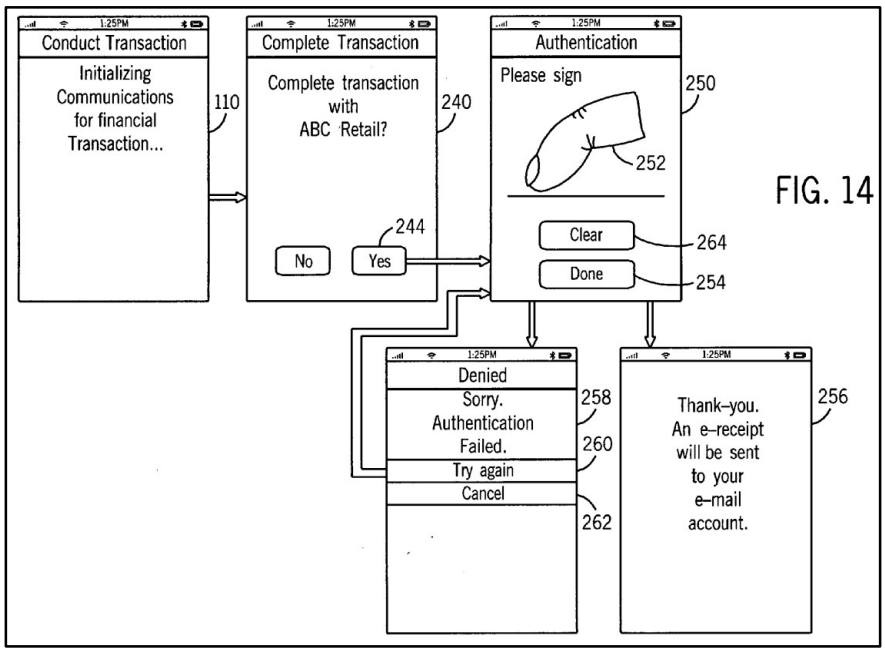
104. Second, Jain also discloses sensing physiological data associated with a living organism for each individual transaction after transaction card 112 has been bootstrapped onto and is a part of mobile device 110. For example, Jain discloses

that during payment, the merchant terminal may "prompt the user to authorize a transaction such as by entering a PIN." Jain ¶[0029]. Authorization via a PIN involves, or at least obviously involves, the process of Jain paragraph [0075] discussed above in connection with bootstrapping. At a minimum, a POSITA would find that ***sensing*** touch on a touchscreen and, more specifically, a user-entered PIN and determining if that PIN matches a previously-stored PIN to be the simplest, most natural, and thus obvious way of implementing PIN authorization, since it does not require communication with any other devices and allows the POSITA to reuse aspects of the software that implements the user authentication of Fig. 7.

105. This is as opposed to incorporating PIN authorization on the POS device. Incorporating PIN authorization on the POS device would require additional functionality on a separate device with a different manufacturer. The user would have to interact with a separate device, limiting its role as the one-stop shop for credit card management and transaction execution. This reduces the speed of transaction execution. Requiring a separate physical interaction with third-party device, where sensitive data is provided, also increases the security risk. Restricting authorization to the mobile device and prior to each transaction is common in prior art references.

106. For instance, EX1020 discloses completing a transaction, providing a signature on the mobile device, and authenticating the signature by comparing it

"with a signature that has been previously stored for authentication purposes." EX1020 ¶¶[0083]-[0084]; *see also* EX1020 FIG. 4:



Further, the signature to be authenticated could be a "biometric signature such as a fingerprint[] … ." EX1020 ¶[0088].

107. Similarly, EX1021 discloses biometric authentication prior to initiating a transaction. EX1021 ¶[0052]. "Selecting 'Payment' may prompt a payment application 155 on the mobile device 100 to check the biometric sensor 160 for biometric input." EX1021 ¶[0052].

108. Also, in my opinion, Jain discloses replacing the transaction-based PIN authentication with biometrics (see ¶[0075]), but to the extent PO argues otherwise, it would at least have been obvious for a POSITA to authorize the transaction with user biometrics instead of the disclosed PIN. Requiring biometric authentication

before authorizing individual transactions was well known in the art. EX1020 ¶¶[0083]-[0084], [0088], FIG. 14 ("[T]he authentication screen 290 provides a menu 291 that lists various ways for authenticating a transaction … including biometric signatures such as fingerprints and retinal scans, for instance."); EX1021 ¶[0052] ("Selecting 'Payment' may prompt a payment application 155 on the mobile device 100 to check the biometric sensor 160 for biometric input."). This is not unlike my prior analysis with respect to bootstrapping, where Jain contemplates using biometrics (*e.g.*, fingerprints) for its authorization process. Jain ¶[0075], Figure 7. That software and hardware can be reused here for individual transactions without further complicating the system or incurring any costs. Moreover, Jain recognizes biometrics as a good alternative to PINs. Jain ¶[0075].

109. In my opinion, a POSITA would also recognize the advantages of biometrics over PINs. Biometrics cannot be forgotten and has less risk of being obtained by a bad actor, such as through phishing. And unlike the short numerical PIN codes, which could be guessed or memorized and are otherwise a weak password, biometric information allows for comparison across numerous values, which is more akin to a longer, variable password—strengthening security by increasing the likelihood of correct authentication. Authorizing individual transactions through biometrics improves security.

110. In addition, a POSITA would further understand that two-factor authentication—PIN and biometric authentication—could be warranted here to provide additional security. A POSITA would also be familiar with two-factor authentication and would know how to perform both PIN and biometric authentication. *See, e.g.*, EX1028 Abstract; EX1029 Abstract; EX1030 Abstract. The PIN authentication could be followed by the biometric authentication or vice versa. A POSITA would recognize the extreme sensitivity of financial information and transactions, and be motivated to incorporate heightened security measures.

(iii) 1[b]: detecting that a proximity criterion is satisfied between the smartphone and an entity, wherein the entity is not the living organism;

111. In my opinion, Jain discloses this limitation. Jain discloses executing transactions with a nearby merchant and its POS device using short range signals, such as near-field communication (NFC) or "proximity signals." *See* Jain ¶[0023]. In other words, executing transactions are responsive to ***detecting that a proximity criterion is satisfied between the smartphone and an entity, wherein the entity is not the living organism***. Specifically, the smartphone (mobile device 110 having transaction card 112) first "wirelessly receive[s] a request from the POS device 114 to execute a transaction and/or provide a response." Jain ¶[0023]. The smartphone then activates a "reader mode" of the transaction card "[i]n the event that the mobile device 110 is proximate (*e.g.*, 10 cm or less) a transmitting terminal" to the POS—

detecting that a proximity criterion is satisfied—and prompts the user though the GUI of the smartphone for authorization to proceed with the transaction. Jain ¶[0030]. Once the user authorizes the transaction, such as by clicking "an OK button on a screen" of the smartphone, the payment proceeds. Jain ¶[0030].

112. Through this process, the mobile device 110 having transaction card 112 detects that it is proximate the merchant by proximity with the merchant's POS device 114. At a minimum, Jain renders ***detecting that a proximity criterion is satisfied between the smartphone and an entity*** obvious.

113. A POSITA would understand that NFC protocols use discovery techniques where a POS device would periodically broadcast its presence, and once detected, a smartphone would request a connection. EX1034 at 11-12; *see also* EX1036 at 220. Short-range NFC signal communications are thus dependent on the proximity between the two devices communicating. EX1037 at 3; EX1035 at 4, 36.

114. A POSITA would also understand NFC and other short range wireless communication protocols require satisfying a proximity condition because such wireless communication protocols are only effective within a short range. The communication signals between the device and terminal must be strong enough to engage in communication with that protocol. The strength of the signal is dependent on distance between device and terminal, where signal strength increasingly attenuates as the distance gets greater.

115. Without reaching a certain signal strength or otherwise satisfying a ***proximity condition***, both devices are sending unnecessary communication signals guaranteed to be lost. This wastes time and processing. Especially for communications executing financial transactions, either device indiscriminately transmitting sensitive financial information without ensuring communication to the correct device is a security risk. Either device is sending communications that will likely to subject to errors, like packet loss, due to transmission past an effective range, increasing the risk of miscommunication. And devices trying to read wireless communications with weak signal strength are also likely to misinterpret noise or other small unintended wireless signals as communications.

116. Implementing NFC to determine whether a proximity condition is satisfied and communicating based on that condition's satisfaction, were well-known to a POSITA. For example, EX1020 discloses using NFC to limit the range at which communication may take place. EX1020 ¶¶[0041] ("In certain embodiments, the communication may occur within a range of approximately 2 to 4 cm. The close range communication with the NFC device 44 may take place via magnetic field induction, allowing the NFC device 44 to communicate with other NFC devices or to retrieve information from tags having radio frequency identification (RFID) circuitry."), [0063] ("The device 10 may be configured to communicate with the transaction terminal 120 using a short range wireless

communication protocol, when positioned over the box 124. … In some embodiments, the wireless communication device 126 may be a near field communication (NFC) device and the device 10 may be configured to initiate NFC communications with the terminal 120."). Further, EX1020 discloses using other wireless signals to determine proximity. EX1020 ¶[0073] ("The [identifying information] may be used by the device 10 to indicate that the device is located within communication range of the hot spot 169."). This makes common sense. Where a particular wireless signal is restricted to a particular distance (*e.g.*, "2 to 4 cm" or "10 cm or less" for NFC (Jain ¶[0030]; EX1020 ¶[0041].)), a device receives messages at a certain signal strength and generally without errors when the transmitting device is within that distance. Thus, signal strength and received messages can be used to determine proximity. Receiving a weak signal and receiving incoherent messages—messages picking up errors from wireless transit—indicate that the transmitter is outside the effective range.

117. As such, it would have been obvious for a POSITA to configure Jain's smartphone to first detect that it is proximate to a POS device prior to attempting short-range signal communication to reduce wasted time, wasted power, security risks, and miscommunication in transmission and reception.

118. Thus, for Jain's smartphone to communicate with the POS device using NFC, the smartphone has ***detected that a proximity criterion is satisfied*** (*e.g.*, the

device is within a range of "10 cm or less" to the POS device, *see* Jain ¶[0030]) by receiving and decoding a short-range NFC signal from the POS device.

119. Jain also discloses an "active-reader mode" activated by proximity between the mobile device 110 and a POS device, and that "this mode can require special NFC hardware." Jain ¶[0030]. This means that the mobile device 110 having transaction card 112 communicates with POS device 114 via NFC only by first detecting it is proximate the POS device ("10 cm or less"). This, too, is an express disclosure of ***detecting that a proximity criterion is satisfied between the smartphone and an entity***.

120. Also, Jain teaches that its NFC "wireless connection" is based on "ISO 18092/ECMA 340" standards. Jain ¶¶[0023], [0051], [0018].

121. ECMA 340 is a well-known communications standard that defined NFC communication. EX1047 is a true and correct copy of the 2nd edition of the ECMA 340 Interface and Protocol Standard for NFC ("ECMA-340"), which was publicly available and known to a POSITA as of its release in December 2004, and which was not updated again until June 2013. *See* https://ecma-international.org/publications-and-standards/standards/ecma-340/. This version was also published as the "ISO 18092." *Id*. In addition, the disclosures of ECMA-340 discussed below are found in both the 1st edition (released December 2002) and the 2nd edition. *See* EX1034 (December 2002 first edition).

122. ECMA 340 explains that an NFC "transaction" requires an "initialization" (described in ECMA-340 §11) and then a "data exchange" (described in §12). EX1047 at §4.26, §10, Figure 5. ECMA-340 specifies two devices ("Initiator" and "Target") and two communication modes ("Passive" and "Active"). EX1047 §1, §4.1, §4.7, §4.17, §4.23, §7.

123. Regardless of whether Jain's POS device or mobile device is the "Initiator" or "Target," or what communication mode they use: every combination results in Jain's mobile device (***smartphone***) detecting a ***proximity criterion is satisfied*** and then establishing a short-range link used for subsequent communications. Specifically, in both modes, an "Initiator" device "shall activate its RF field" and a "Target" device then "shall be activated by the RF field of the Initiator." EX1047 §10. Then, the "Initiator" sends one or more commands (e.g., ALL_REQ, SENS_REQ, and/or ATR_REQ) and receives one or more responses (e.g., SENS_RES and/or ATR_RES). EX1047 §§11.2.1.16-.17, §11.2.1.23, §11.3.2, §§12.2-.3, Figures 13, 24-25.

124. In even more detail, in Passive mode, an activated Target enters the SENSE state. EX1047 §11.2.1.8, §11.2.1.9. The "Initiator" then sends commands "to probe the field for Targets" (EX1047 § 11.2.1.16), receives a SENS-RES response from a Target in the SENSE state (EX1047 §11.2.1.17), and then selects that Target "for further communication" (EX1047 §11.2.1.23, Figure 13). *See also*

EX1047 §12.2 and Figure 24. In Active mode, after the Target is activated by the RF field of the Initiator, it receives an ATR_REQ message from the Initiator, generates its own RF field, and uses that field to send an ATR_RES message to the Initiator. EX1047 §11.3.2. In response to that message, the Initiator sends a DEP_REQ "to start the data exchange protocol." EX1047 §11.3.2. *See also* EX1047 §12.3 and Figure 25.

125. Thus, regardless of what mode is used and which of Jain's devices is the Initiator or Target, the Target device detects a sufficiently strong field from the Initiator (***proximity criterion is satisfied***), and the Initiator device detects that a Target is within its field by receiving a response to a command from the Target (***proximity criterion is satisfied***). This exchange of commands and responses results in selection of a particular "Target" and attributes/parameters for further communication with the same, thereby establishing a short-range link. EX1047 §7, §§11.2.1.24-25, §12, §12.1, Figures 22, 24-25. After this link is established, the Initiator and the Target communicate using ECMA-340's data exchange protocol. EX1047 Figures 5, 23, and 24. This includes transmission of Jain's transaction request 117, transaction response 119, and authorization response 120.

126. In my opinion, a POSITA reading Jain would have known the above. For example, Jain teaches that its NFC communication is based on the "ISO 18092/ECMA 340" standards. Jain ¶[0023]. *See also* Jain ¶[0018], ¶[0051]. But at a

minimum, it would have been obvious to implement Jain's NFC communications in this manner, because that is the exchange taught by the NFC standard cited in Jain and because a POSITA would be motivated to implement the standard rather than define a proprietary approach to simplify design, to allow for use of commercially available NFC hardware and software, to minimize the need for trial and error, and to maximize interoperability with standard-compliant reader/POS systems and mobile devices.

127. The Patent Owner agrees with this mapping. In its infringement contentions in the district court litigation, Patent Owner also asserts use of short range communications—specifically, use of NFC—is sufficient to establish ***detecting that a proximity criterion is satisfied between the smartphone and an entity, wherein the entity is not the living organism***. *See* Exhibit 1016 at 12-15.

(iv) 1[c]: selectively communicating by the smartphone using a first air interface of a plurality of air interfaces with which the smartphone is capable of communicating, responsive to the proximity criterion having been detected as being satisfied and responsive to a value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor;

128. In my opinion, Jain discloses this limitation. Jain discloses ***a plurality of air interfaces with which the smartphone is capable of communicating***, including: (1) a first air interface for short-range communications (such as for

contactless transactions) with POS device 114; and (2) a second air interface for cellular and other communications with a cellular network, for example. *See* Jain ¶¶[0021], [0023], [0027], [0030], [0041]-[0044], [0046]-[0048], and Fig. 2.

129. Jain's first air interface may utilize "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." Jain ¶[0022]; *see also* Jain ¶[0030] (recognizing need for "special NFC hardware").

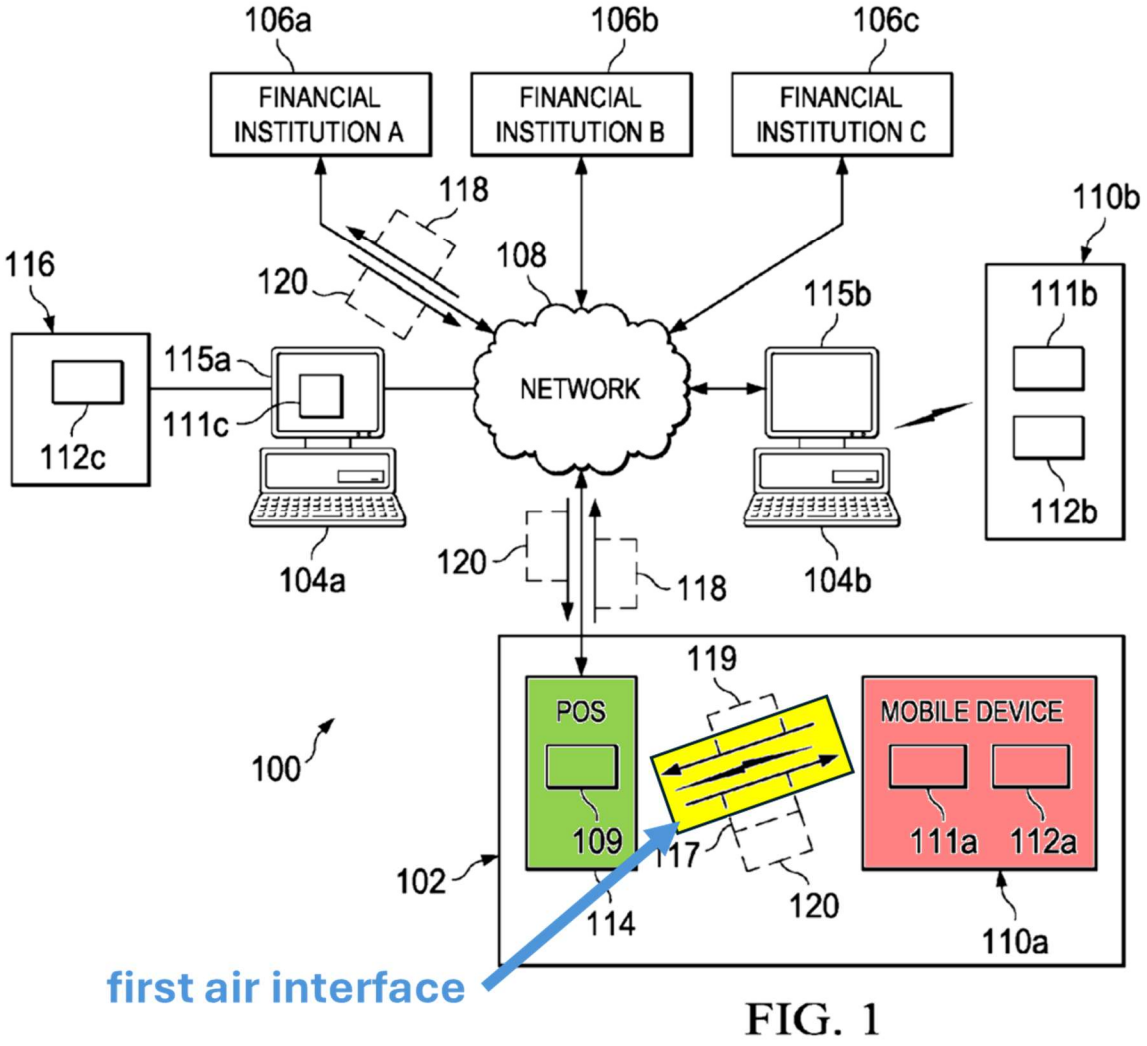


FIG. 1

130. Separately, Jain's second air interface (together, with the first air interface, ***a plurality of air interfaces with which the smartphone is capable of communicating***) may be with a radio access network that provides access to the cellular network (and its associated infrastructure, including base station 210, macrocell 208, base station controller 212, etc.) using "Advanced Mobile Phone Service (AMPS), GSM standards, Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), IS-54 (TDMA), General Packet Radio Service

(GPRS), Enhanced Data Rates for Global Evolution (EDGE), or proprietary radio interfaces." Jain ¶¶[0043], [0044].

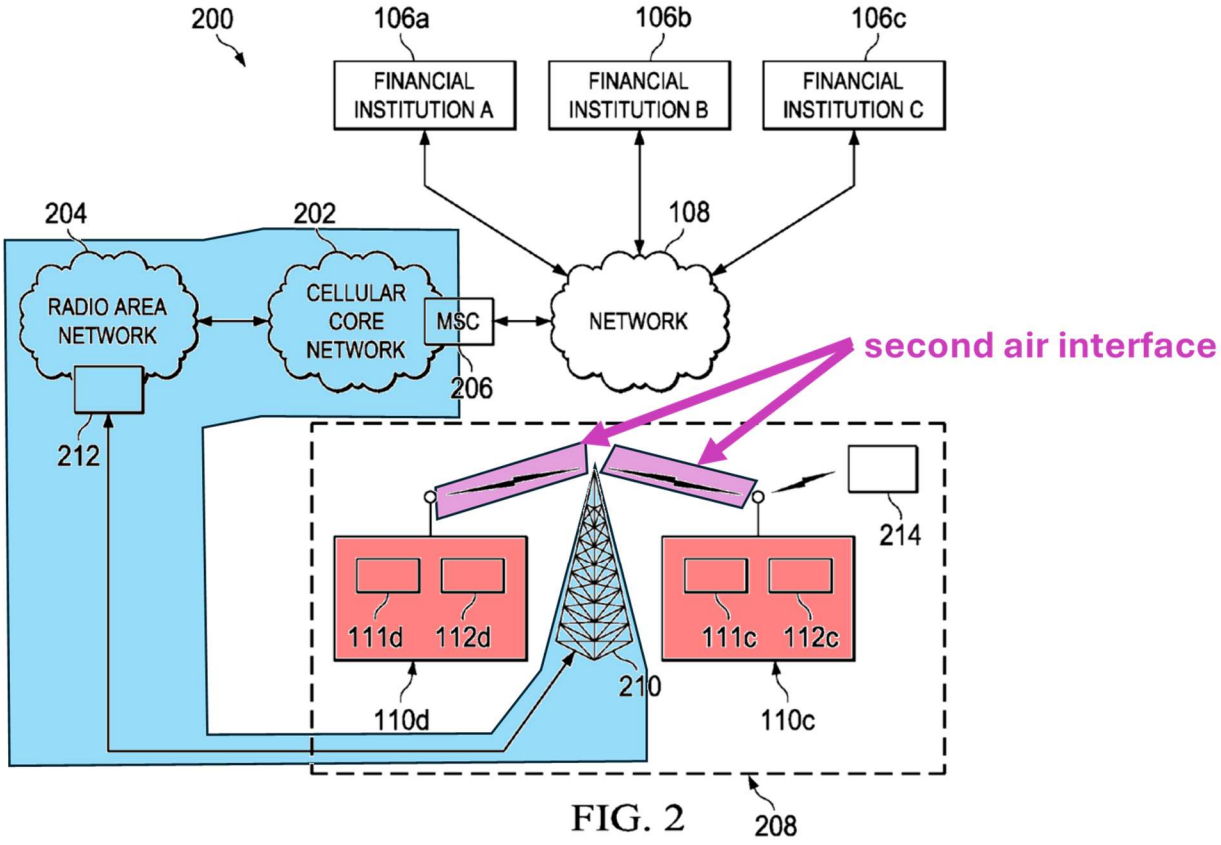


FIG. 2

131. Patent Owner also alleges in its district court infringement contentions that a cellular smartphone capable of conducting transactions over NFC meets the ***plurality of air interfaces with which the smartphone is capable of communicating***. Exhibit 1016 at 14-20.

132. In my opinion, Jain also discloses the smartphone ***selectively communicating*** over the first air interface responsive to and based on satisfying the proximity criterion and the value of physiological data that was sensed.

133. With respect to selectively communicating responsive to the proximity criterion, I explained above with respect to limitation 1[b] that mobile device 110 only engages in contactless payments with POS device 114 when it detects proximity with the merchant and its POS device 114, such as by being proximate the POS device by "10 cm or less." Jain ¶¶[0023], [0029], [0030]. For example, Jain illustrates this point in Fig. 1 by showing mobile device 110a selectively communicating with POS device 114 via transaction request 117, transaction responses 119, and authorization response 120, responsive to proximity with the POS device, as both are inside store 102 (Jain ¶[0019]. Mobile device 110b is not inside store 102 and is, thus, not proximate POS device 114 and therefore does not communicate with POS device 114:

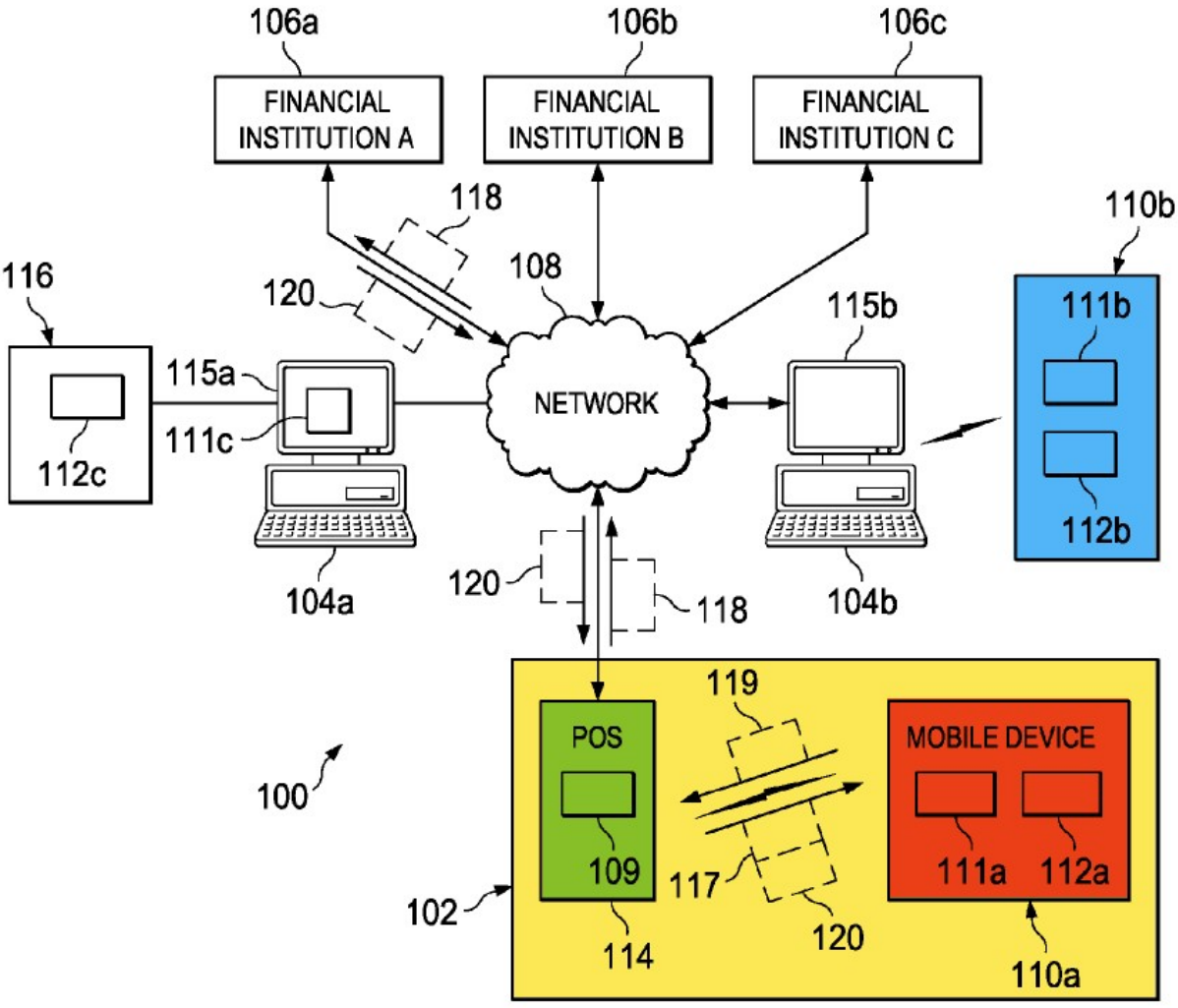


FIG. 1

134. With respect to selectively communicating responsive to the value of physiological data that was sensed, I explained above with respect to limitation 1[a] that mobile device 110 engages in contactless payments with POS device 114 only after having authenticated its user in response to a sensed PIN or biometric (*e.g.*, fingerprint). Jain ¶¶[0022]-[0025], [0029], [0065], [0066], [0072], [0075], Table 1, Fig. 7B at steps 734-742.

135. Jain's mobile device 110 having transaction card 112 therefore selectively communicates with POS device 114 over NFC or other short-range communication medium responsive to both the proximity criterion being met and the value of physiological data sensed (***selectively communicating by the smartphone using a first air interface of a plurality of air interfaces with which the smartphone is capable of communicating . . .***). The POS device 114 can then initiate the remaining steps of completing the financial transaction. Jain ¶¶[0036] ("In illustrated implementation, the POS 114 can wirelessly receive encrypted transaction information [*e.g.*, routing number, account number, transaction amount, credit-card number, etc.] from the transaction card 112 and electronically send the information to one or more of the financial institutions 106 for authorization."); *see also* Jain ¶¶[0028] ("The GUI 109 may present a series of screens or displays to the user to, for example, accept a transaction and enter security information such as a PIN."), [0029] (" a merchant terminal may detect the presence of a host device with the transaction card 112 and prompt the user to authorize a transaction such as by entering a PIN")

136. Patent Owner also alleges in its district court infringement contentions that using a smartphone to conduct a financial transaction via NFC after having authenticated the user and bringing the phone proximate a payment terminal meets the ***selectively communicating by the smartphone using a first air interface of a***

plurality of air interfaces with which the smartphone is capable of communicating, responsive to the proximity criterion having been detected as being satisfied and responsive to a value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor. Exhibit 1016 at 15-16.

(v) 1[d]: refraining from communicating by the smartphone using the first air interface absent said value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor satisfying a criterion, even though the proximity criterion is detected as being satisfied;

137. In my opinion, Jain discloses this limitation. As I explained in my opinions with respect to limitations 1[a] and 1[c], mobile device 110 does not communicate with POS device 114 unless its user has been authenticated—first as part of initial bootstrapping but also for each individual transaction. And the user is authenticated by entry of a PIN on the mobile device touch screen or through biometric/fingerprint scan. Without user authentication, NFC transactions cannot occur.

138. Accordingly, Jain teaches that its mobile device 110 having transaction card 112 refrains from communicating using the first air interface (*e.g.*, for NFC transactions) absent said value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor

satisfying a criterion (e.g., entered PIN matching authorized PIN, or scanned fingerprint matching a stored fingerprint). *See* Jain ¶¶[0022]-[0025], [0028], [0029], [0065], [0066], [0072], [0075], Table 1, Fig. 7B at steps 734-742.

139. Jain further teaches the refraining limitation through its disclosure of selectively disabling its NFC antenna if the user enters an incorrect PIN—or in the case of biometrics, a POSITA would understand the same would apply to entering an incorrect biometric (e.g., where the fingerprint scanned does not match an authorized fingerprint). For example, Jain Figs. 7A and 7B teach an authentication loop in which a user may be asked to enter their PIN (steps 734 and 736) when a transaction card is first inserted into the mobile device (step 702) and the antenna is turned off (step 722) if the number of attempts to enter the correct PIN exceeds some threshold (steps 738-744) and thus the device refrains from communicating using the transaction card. *See* Jain ¶[0024] ("In some implementations, the transaction card 112 may selectively switch the antenna between an on and off state in response to one or more events. The one or more events may include . . . detection of incorrect PIN entered by the user . . . [and] [i]n some implementations, the transaction card 112 may request user identification such as a PIN, a user ID and password combination, biometric signature, and/or others."), ¶[0061] (disclosing "antenna control function 320 [that] may activate/deactivate the antenna 322 [which 'may be a short range wireless antenna'] in response to, for example, successful

authentication"), ¶[0066] ("In case of a successful [PIN] match, the antenna 402 may be activated."), Table 1 ("The user can also optionally select a PIN (change Antenna availability to user authentication)")

140. I've annotated Figs. 7A and 7B, below, to help illustrate this sequence. Specifically, when a user inserts transaction card 112 into mobile device 110 (step 702—plug-in insertion into host device), a series of authentication decision steps may ultimately lead to User Authentication 736 and 734, which lead to several steps that sense physiological data and determine if it satisfies a criterion (steps 738-744). If user authentication fails (wrong PIN or fingerprint), then the NFC antenna turns off at step 722:

FIG. 7A

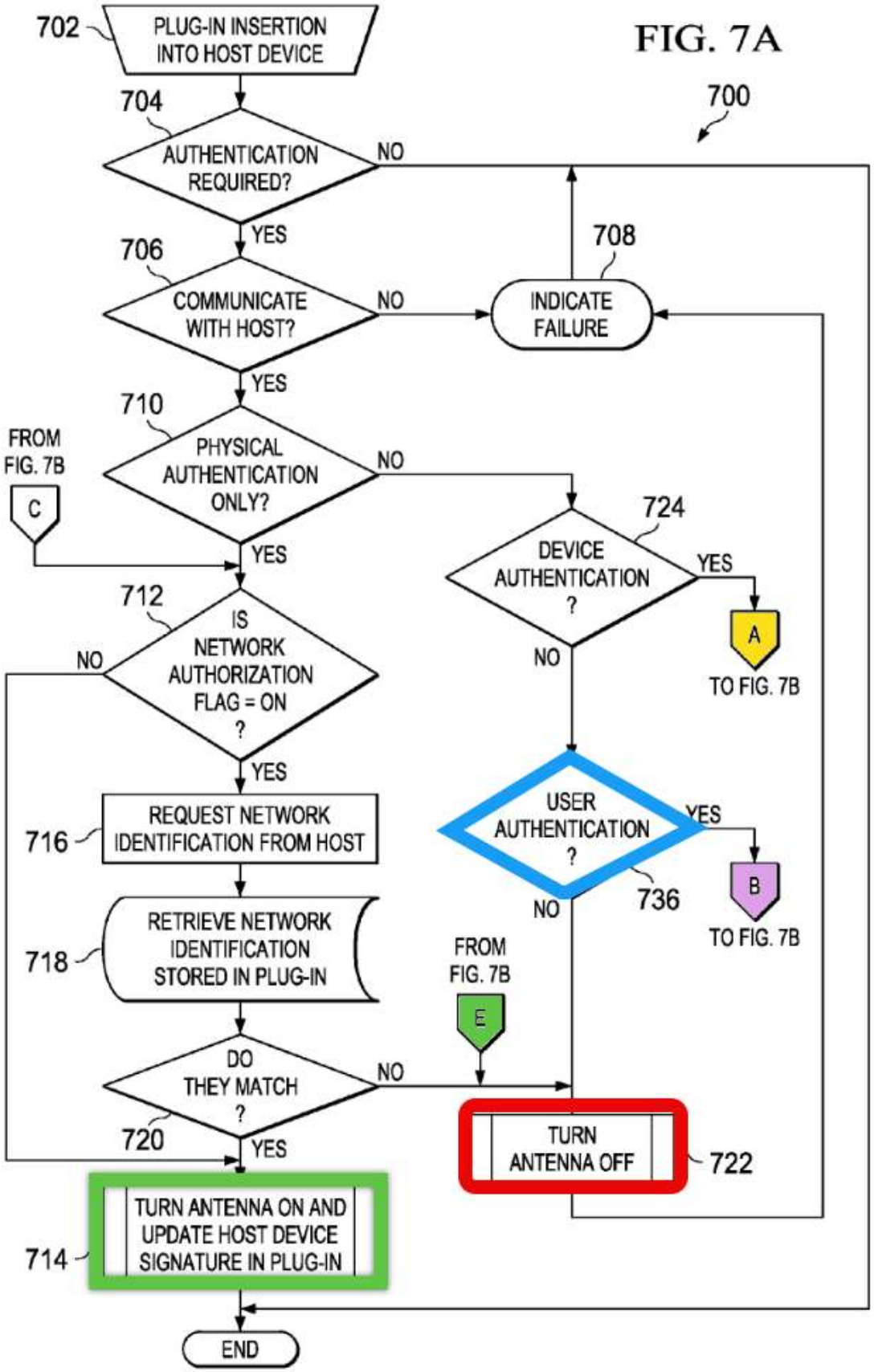
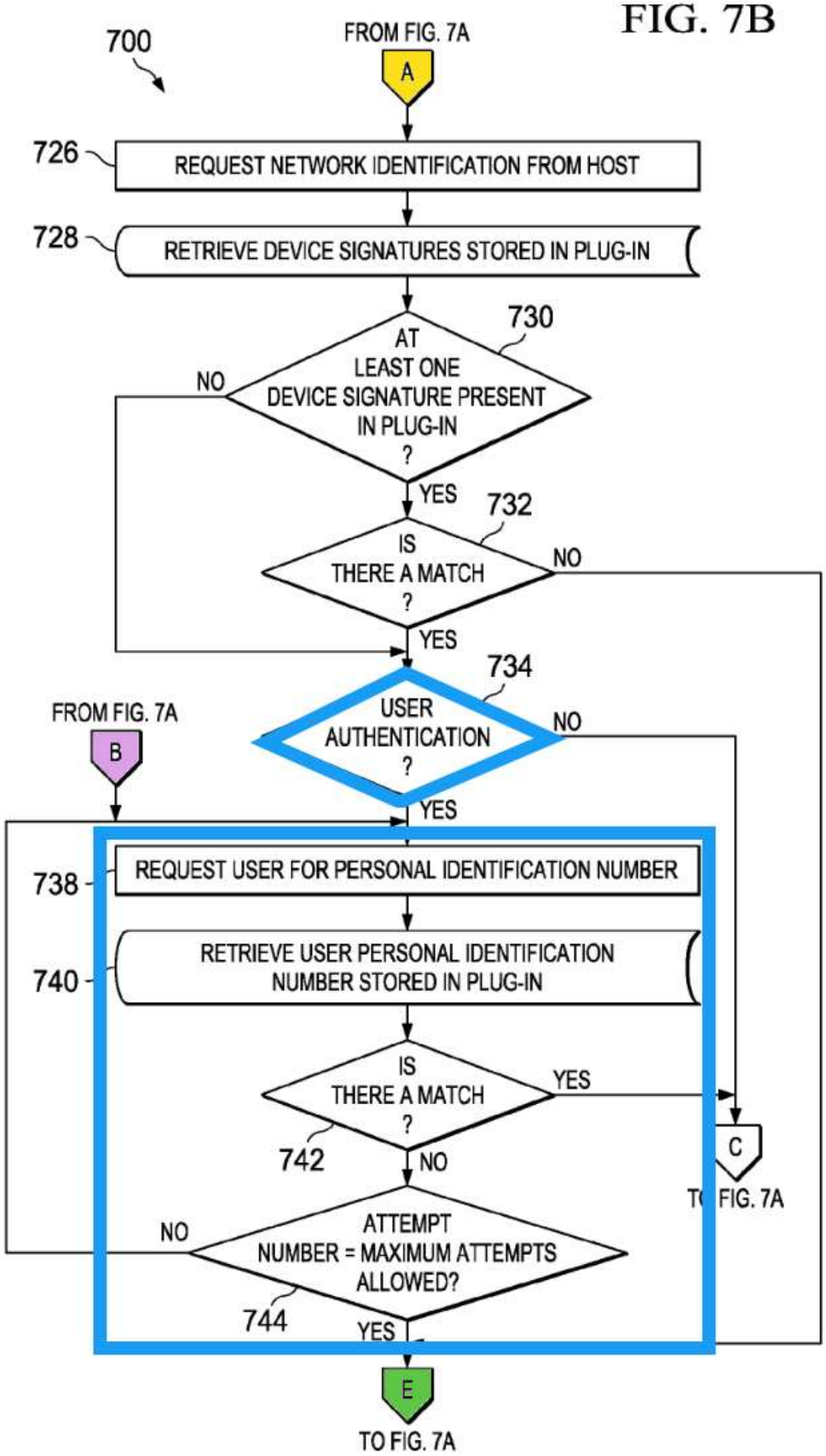

700
702
PLUG-IN INSERTION INTO HOST DEVICE
704
AUTHENTICATION REQUIRED?
NO
YES
706
COMMUNICATE WITH HOST?
NO
YES
708
INDICATE FAILURE
710
PHYSICAL AUTHENTICATION ONLY?
NO
YES
FROM FIG. 7B
C
712
IS NETWORK AUTHORIZATION FLAG = ON ?
NO
YES
716
REQUEST NETWORK IDENTIFICATION FROM HOST
718
RETRIEVE NETWORK IDENTIFICATION STORED IN PLUG-IN
720
DO THEY MATCH ?
NO
YES
714
TURN ANTENNA ON AND UPDATE HOST DEVICE SIGNATURE IN PLUG-IN
END
724
DEVICE AUTHENTICATION ?
YES
NO
A
TO FIG. 7B
736
USER AUTHENTICATION ?
YES
NO
B
TO FIG. 7B
FROM FIG. 7B
E
TURN ANTENNA OFF
722

FIG. 7B


700
FROM FIG. 7A
A
726
REQUEST NETWORK IDENTIFICATION FROM HOST
728
RETRIEVE DEVICE SIGNATURES STORED IN PLUG-IN
730
AT LEAST ONE DEVICE SIGNATURE PRESENT IN PLUG-IN ?
NO
YES
732
IS THERE A MATCH ?
NO
YES
734
USER AUTHENTICATION ?
NO
YES
FROM FIG. 7A
B
738
REQUEST USER FOR PERSONAL IDENTIFICATION NUMBER
740
RETRIEVE USER PERSONAL IDENTIFICATION NUMBER STORED IN PLUG-IN
IS THERE A MATCH ?
YES
742
NO
C
TO FIG. 7A
ATTEMPT NUMBER = MAXIMUM ATTEMPTS ALLOWED?
NO
744
YES
E
TO FIG. 7A

141. Jain also discloses fraud control mechanisms whereby transaction card 112 disables transactional communications (*e.g.*, "execute a command to block . . . the transaction card 112") if it detects "an operational violation" such as the transaction card 112 being moved from an authorized mobile device 110 to a different mobile device 110. Jain ¶[0026]. A POSITA would understand that a failed user authentication qualifies as an operational violation or at least would have been obvious to include as a violation, particularly since Jain already recognizes that "detection of incorrect PIN entered by the user" qualifies as a violation that triggers disabling use of the transaction card antenna. Jain ¶¶[0024], [0061], [0065], [0066].

142. Accordingly, a POSITA would understand that Jain's mobile device 110 having transaction card 112 will turn the NFC antenna off or otherwise disable transactional communications absent the value of a correct PIN (or biometric) being sensed and, thus, refrains from communicating with POS device 114 under such circumstance even though the proximity criterion may be satisfied.

143. As further evidence that Jain discloses limitation 1[d], Patent Owner alleges in its district court infringement contentions that this limitation is met just by requiring a smartphone to authenticate its user via biometrics before it is allowed to conduct a financial transaction via NFC, even though the phone may be proximate a payment terminal—precisely what is taught in Jain. EX1016 at 20-22.

(vi) 1[e]: selectively sending information by the smartphone to one or more other devices and receiving information by the smartphone from the one or more other devices responsive to said value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor satisfying the criterion; and

144. In my opinion, Jain discloses this limitation. As I explained above with respect to limitations 1[a] and 1[c], Jain discloses that mobile device 110 communicates with POS device 114 (***one or more other devices***) by sending transaction responses 119 (***selectively sending information by the smartphone to one or more other devices***) and receiving authorization responses 120 (***receiving information by the smartphone from the one or more other devices***) responsive to a user's authentication via PIN or biometric (***responsive to said value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor satisfying the criterion***). *See* Jain ¶¶[0022]-[0025], [0029], [0065], [0066], [0072], [0075], Table 1, Fig. 7B at steps 734-742.

145. For example, responsive to user authentication (through initial bootstrapping and for each transaction), "transaction card 112 may transmit one or more transaction responses 119 identifying information associated with a payment account" to POS device 114. Jain ¶[0027]. POS device 114 may then use said

information to "transmit a request 118 to authorize a transaction to the financial institution 106." *Id*. Financial institution 106 may then authorize the transaction and "transmit an authorization response 120" to POS device 114, which "may transmit the response 120 to the to the transaction card 112" where "[t]he transaction response 120 may include, for example, a receipt presentable to the user through the GUI 111 a." *Id*. All these transmissions to and from mobile device 110 having transaction card 112 (***the smartphone***) are ***selective*** communications at least because they are responsive to the user authentication via PIN/biometric (*i.e.*, they are not sent absent authentication).

146. The transmissions are further selective because they are specific to the device to which they are sent. In other words, the transmissions are sent to a specific POS device 114 in response to a transaction request 117 received specifically from that POS device. Jain ¶[0027].

147. For example, Jain discloses mobile device 110 having transaction card 112 may be instructed "to transmit data using its wireless connection with, for example, ***the POS 114***"—not some other device. Jain ¶¶[0054], [0057] (describing selective communications directed to POS device 114, including encrypted data). Jain also discloses encrypting the communications between the two devices, which further shows that they are selective communications between two specific devices—not any other devices: "[i]n addition, the data may be encrypted by the

transaction card 112 prior to transmission using, for example, keys and encryption capability stored within the security module." *Id*. and ¶[0025] (identifying public and private key encryption schemes supported by transaction card 112), ¶[0036] ("the POS 114 can wirelessly receive encrypted transaction information from the transaction card 112"). A POSITA would understand encrypted communications with a specific POS device 114 prevents other devices from accessing the transaction information and is, thus, a selective communication to a specific device (the device having the correct decryption key).

148. Moreover, in my opinion the "selectively" language in this limitation modifies the "sending information" portion of the overall phrase and not "receiving information." Nevertheless, even if Patent Owner argues that "selectively" also requires ***selectively*** "receiving information" in addition to "selectively sending," then in my opinion Jain also discloses that for all the same reasons that sending data to POS device 114 is selective. Specifically, receiving authorization response 120 only occurs in an authenticated transaction and is only received from POS device 114. In other words, mobile device 110 does not receive data from other devices with which it is not engaged in a transaction while it is conducting a transaction with POS device 114.

149. Moreover, Patent Owner alleges in its district court infringement contentions that using a smartphone to submit a financial transaction to a POS

terminal and receive a confirmation from the POS terminal responsive to user authentication (via "a fingerprint, facial recognition, or iris") meets limitation 1[e]—that is precisely what is disclosed in Jain. EX1016 at 22-26.

(vii) 1[f]: communicating by the smartphone using a second air interface of the plurality of air interfaces with which the smartphone is capable of communicating that differs from the first air interface.

150. In my opinion, Jain discloses this limitation. As I explained above with respect to limitation 1[c], mobile device 114 has a plurality of wireless interfaces, including a second air interface with a radio access network that provides access to a cellular network and its associated infrastructure, such as base station 210, microcell 208, and base station controller 212 (***communicating by the smartphone using a second air interface of the plurality of air interfaces with which the smartphone is capable of communicating***), all of which are separate from the NFC interface used for short-range communications (***that differs from the first air interface***). Jain ¶¶[0043], [0044]; see also Jain ¶[0046] (disclosing that mobile device 110 wirelessly communicates with a financial institution "using the cellular core network 202" separate from any NFC communication with a POS terminal, since "the financial institutions 106 may transmit information to the transaction card 112 ***without requiring a POS terminal being proximate to the card 112***").

151. I've illustrated this in annotated Fig. 2, below, to show the second air interface and associated network infrastructure accessed via that interface:

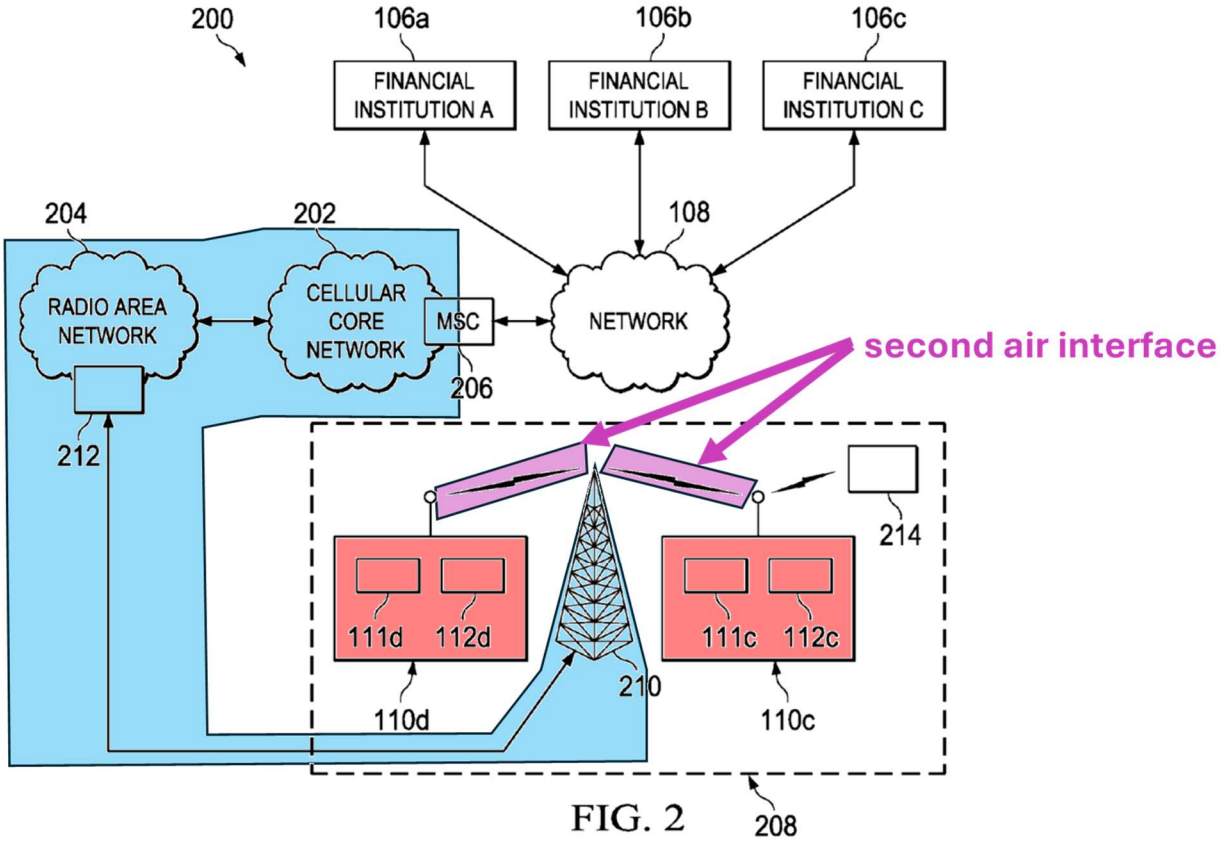


FIG. 2

152. Additionally, Patent Owner alleges in its district court infringement contentions that a smartphone that can communicate over a cellular data network in addition to NFC meets limitation 1[f]—precisely what is disclosed in Jain. EX1016 at 26-27.

(b) Claim 2

(i) 2[pre]: The method according to claim 1, wherein said detecting that a proximity criterion is satisfied between the smartphone and an entity comprises:

153. In my opinion, Jain discloses this limitation for the same reasons as I explained above for limitation 1[b].

(ii) 2[a]: detecting that a proximity criterion of less than 10 meters in distance is satisfied between the smartphone and the entity;

154. In my opinion, Jain discloses this limitation. Specifically, Jain discloses that the short-range communication occurs at a range of "10 cm or less" (Jain ¶[0030]) or between 10 cm and 50 cm (Jain ¶[0045]). Thus, when Jain detects the proximity criterion is met at those ranges, as I explained above with respect to limitation 1[b], Jain is ***detecting that a proximity criterion of less than 10 meters in distance is satisfied between the smartphone and the entity***. Also, that range is consistent with what a POSITA knows about NFC: it has an effective range of about 10 cm. EX1032 §8. Moreover, a POSITA would understand the short-range communications disclosed in Jain occur over distances shorter than 10 meters, as they include contactless payment transactions between a user and a POS terminal. It would make no sense to conduct such transactions at a distance greater than 10m, as a POSITA would understand any such communication between devices that are more than 10m apart would no longer be considered a "short-range" communication. Nor would many, if not all, of the short-range air interfaces disclosed by Jain be capable of even communicating over a range greater than 10m.

(iii) 2[b]: wherein the detecting is performed by the smartphone, by a device that is associated with the entity, by a system that is associated with the smartphone, or a combination thereof.

155. In my opinion, Jain discloses this limitation. As I explained above for limitation 1[b], the detecting is performed by the smartphone, by a device that is associated with the entity, by a system that is associated with the smartphone, or a combination thereof. Specifically, either mobile device 110 with transaction card 112 detects proximity, POS device 114 detects proximity, or a combination of the two through exchange of communications at short range.

156. Moreover, in the language of the ECMA-340 NFC standard, which I discussed above, one of those devices is the Initiator and the other is the Target. Either way, both the Target and the Initiator detect that a proximity criterion is satisfied.

(c) Claim 3

(i) 3[pre], 3[a]

157. As I explained in my opinions above, Jain discloses a smartphone having a processor that is configured to and does control the smartphone to perform the claimed process steps and capabilities.

158. Jain expressly discloses its mobile device 110 may be a smartphone with a processor. *E.g.*, Jain at ¶[0021] ("As 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.").

(ii) 3[b] – 3[g]

159. The remaining limitations of claim 3 are substantively identical to claim 1 and merely remove the references in claim 1 to claim steps being performed "by a smartphone," as claim 3 separately recites the smartphone in 3[pre]/3[a]. Accordingly, Jain discloses a smartphone with a processor that implements the claimed capabilities for the same reasons provided above with respect to claim 1, where my opinions with respect to limitations 1[a]-1[f] map directly to limitations 3[b]-[g], which are therefore disclosed by Jain for the same reasons as 1[a]-1[f], respectively.

(d) Claim 4

160. Claim 4 is substantively identical to claim 2, limitations 2[pre] and 2[a]. Accordingly, my opinions relating to Jain's disclosure of limitations 2[pre] and 2[a] map directly to limitations 4[pre] and 4[a], which are therefore disclosed by Jain for the same reasons as 2[pre] and 2[a], respectively.

B. Ground 2: Dua (EX1018)

1. Background

161. Dua is the July 27, 2006, publication of U.S. Patent Application No. 11/040,847, which was filed on January 21, 2005, and is assigned to Samsung Electronics Co., Ltd. EX1018. Dua is prior art to the '411 Patent under at least pre-AIA 35 U.S.C. § 102(b), as it was published more than one year before the filing date of the '411 patent.

162. Dua is titled "Method and apparatus for managing credentials through a wireless network." It describes systems and methods for (1) credit card issuers to "control[] and distribut[e] credentials" to a wireless device (*e.g.*, "mobile telephone") and (2) "us[ing] the [wireless] device to conduct [an] authorized [financial] transaction via … a short range wireless link with a point-of-sale terminal." Dua Abstract.

163. The distribution and management of credentials on a wireless device is done by the issuer's wireless credential manager. The network for this system is partially shown in Figure 1 below:

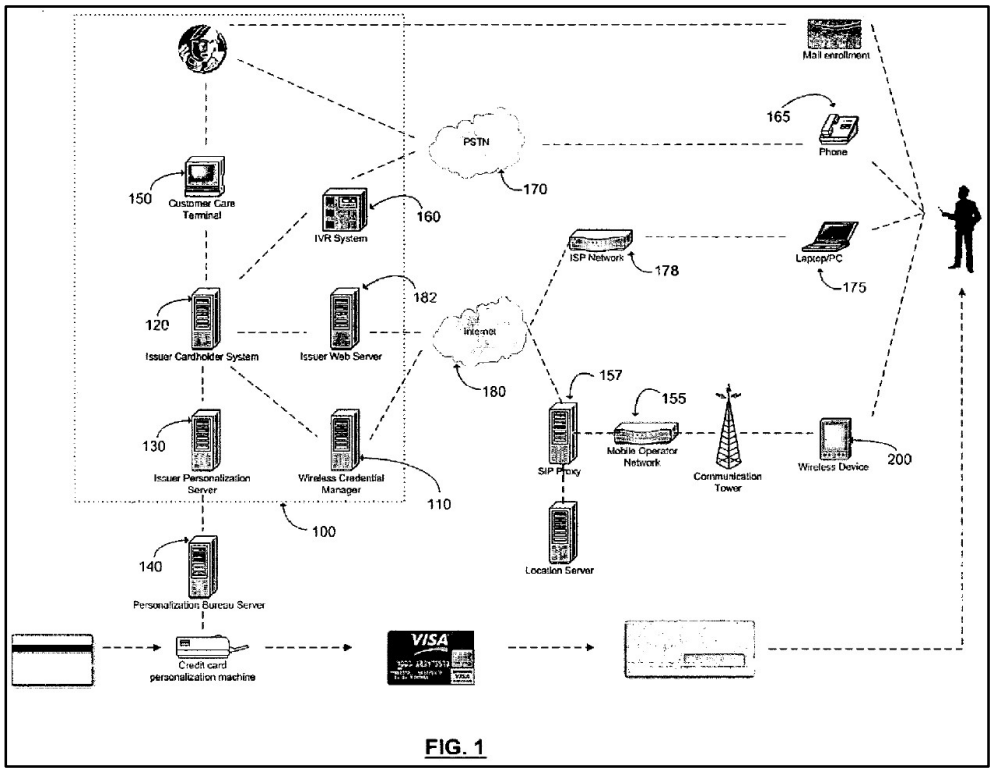


FIG. 1

164. Figure 1 shows a network by which a wireless credential manager "WCM 110 [can] … issu[e], cancel[], and manag[e] eletronic credentials [to] wireless device[]" 200. Dua ¶[0046]. An issuer can issue a physical credit card to a user, and the user "may also request a digital card for use with [a] wallet application on … [a] wireless device 200." Dua ¶[0055]. After the "issuer's system validat[es] the user's identity in real-time," such as by the user sending a "special code or PIN mailed to the user," the "WCM … will transmit the credential to the wallet application." Dua ¶[0180]. The wallet application can store credentials on the wireless device or, for greater security, in an external wallet storage service accessible by the wallet application. Dua ¶¶[0041], [0287]-[0288], [0491]-[0492].

165. Communication channels between the wallet application and the issuer's wireless credential manager or the external wallet storage service are set up through Session Initiation Protocol ("SIP") communications. An example of the wallet application engaging in SIP communications is shown in Figures 3 and 4:

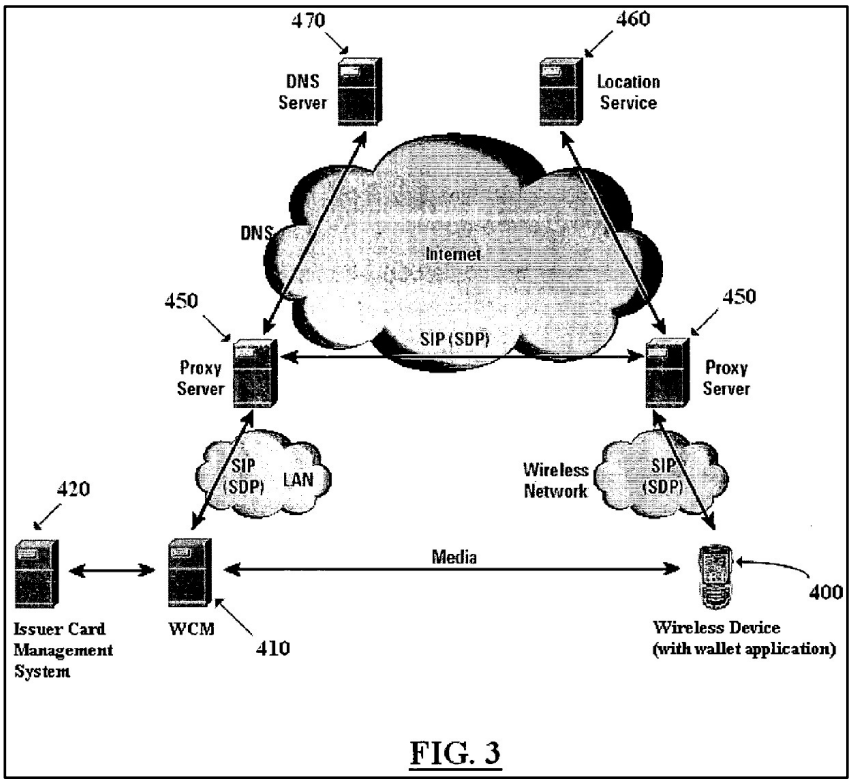

470
DNS Server
460
Location Service
DNS
Internet
450
SIP (SDP)
450
Proxy Server
Proxy Server
SIP (SDP) LAN
Wireless Network
SIP (SDP)
420
Media
400
Issuer Card Management System
WCM
410
Wireless Device (with wallet application)

FIG. 3

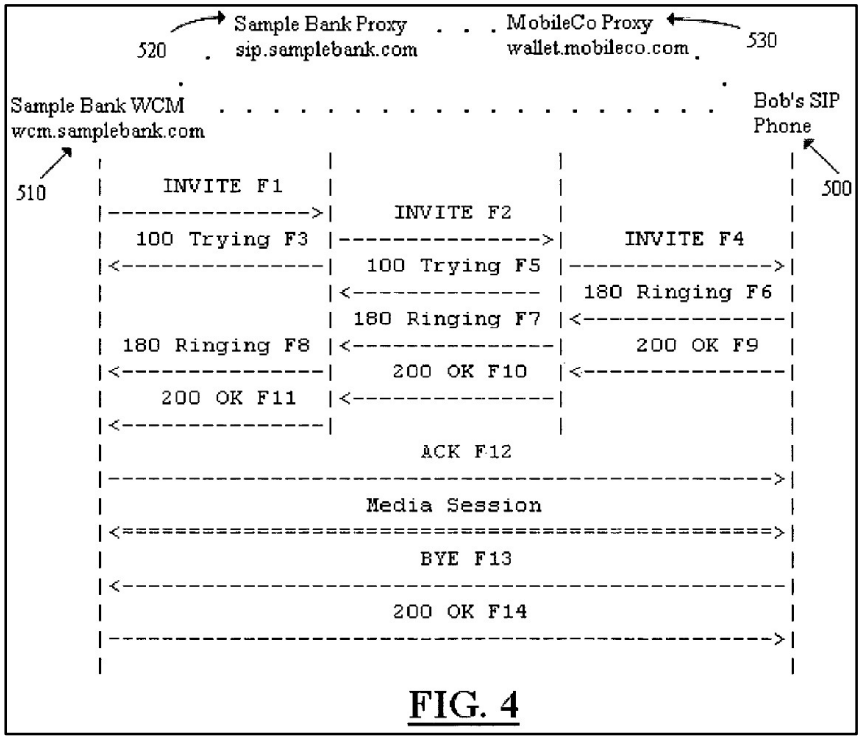

Sample Bank Proxy
sip.samplebank.com
520
MobileCo Proxy
wallet.mobileco.com
530
Sample Bank WCM
wcm.samplebank.com
Bob's SIP Phone
510
500
INVITE F1
INVITE F2
INVITE F4
100 Trying F3
100 Trying F5
180 Ringing F6
180 Ringing F7
180 Ringing F8
200 OK F9
200 OK F10
200 OK F11
ACK F12
Media Session
BYE F13
200 OK F14

FIG. 4

166. The wallet application allows the user to access and use credentials for financial transactions. Dua ¶[0041]. For security, opening the wallet application to view and transmit credentials can require user authentication, such as through PIN entry, fingerprint scanning, or other biometrics. Dua ¶¶[0366], [0414], [0534]-[0535]. If the credentials are stored on an external wallet storage service, user authentication is still required to open the wallet application, but the wallet application subsequently uses a "username/password" established between the external storage and wallet application "to automatically access the storage area." Dua ¶[0492], [0495].

167. Opening the wallet application to view and transmit credentials can also be done through a wallet button and/or reader key. Dua ¶[0370], [0392]-[0393]. The wallet button can "launch[] the wallet application" and "enable RF communications" for transmitting credentials. Dua ¶¶[0383]-[0384]. An example of the wallet button on the wireless device is shown in Figures 6(a) and 6(b) below.

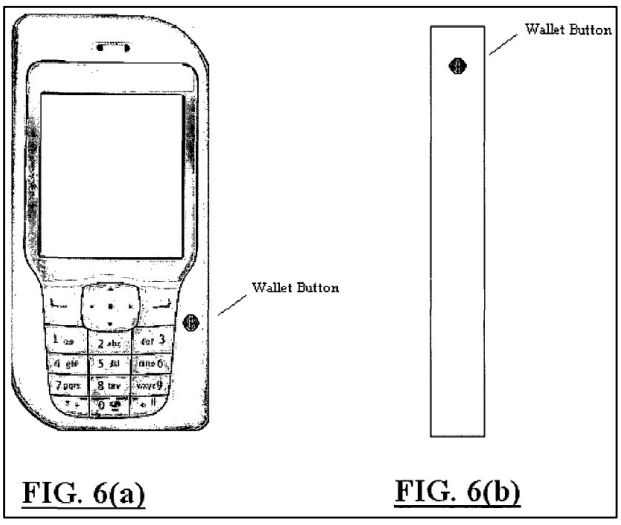


FIG. 6(a) FIG. 6(b)

168. A reader key is a code constantly "transmitted from [a point-of-sale] reader." Dua ¶[0353]. When the wireless device is sufficiently close to the reader, the wireless device can detect the reader key. Dua ¶[0353]. When it does, if the wallet application has credentials registered with that reader key (and subject to any required user authentication), the wallet application automatically opens, selects a credential for a financial transaction, and transmits the credential. Dua ¶¶[0353]-[0354].

2. Analysis

(a) Claim 1

(i) 1[pre]

169. In my opinion, Dua discloses this limitation. Dua describes a method with steps matching the remaining limitations of claim 1 as provided in my opinions below. Dua at Abstract ("A novel system and methodology for conducting financial and other transactions using a wireless device. . . . Credentials are ultimately supplied

to a handheld device such as a mobile telephone via a wireless network. The user holding the credential may then use the handheld device to conduct the authorized transaction or set of transactions via, for example, a short range wireless link with a point-of-sale terminal."), ¶¶[0041], [0312]-[0313], [0333].

170. Indeed, Dua discloses a wireless device—a smartphone. Dua Abstract, FIGS. 3, 5, 6(a)-8. The wireless device includes a "handheld device, such as a mobile telephone," "capable of wirelessly connecting to the internet" and phone applications like a "wallet application." Dua Abstract, ¶¶[0041], [0049], [0050], [0051], [0287]-[0288], FIGS. 3, 5, 6(a)-8. The wallet application can "conduct[] financial … transactions," and thus performs methods associated with executing financial transactions. Dua Abstract, ¶¶[0041], [0312]-[0313], [0333].

(ii) 1[a]

171. In my opinion, Dua discloses this limitation. Dua discloses using its wireless device (***smartphone***) to sense a user's fingerprint (***sensing . . . physiological data associated with a living organism***) with the "wireless device's embedded biometric technologies," which involves biometric sensors (***using a smartphone-based sensor***). Dua ¶¶[0366], [0414], [0534] (also disclosing other types of user physiological data that may be sensed, including "iris, voiceprints, facial recognition, and hand geometry"). While a PIN can also be used (similar to Jain, above), Dua's wallet application can scan for "fingerprint[s] in lieu of a PIN code to

authenticate a user." Dua ¶¶[0366], [0414], [0534]. And the scanned fingerprint can also be used to decrypt wallet application data, such as credit card credentials needed to conduct financial transactions. Dua ¶¶[0050], [0366], [0399], [0429].

172. In addition to fingerprint and other biometric sensing, Dua also discloses using PINs to secure its wallet application and data contained in the electronic wallet. For example, Dua discloses using PIN-entry to open the wallet application for the wallet application to be issued a credit card. Issuing a credit card to the wallet application requires the wallet application to first be opened. *See* Dua ¶¶[0128]-[0129], [0178], [0180], [0250]. And the "default security setting in the wallet application is that PIN-entry is required before the wallet application can be 'opened,'" or otherwise "allow the user access to the application," including to receive an issued a credit card. Dua ¶¶[0366], [0429]. In other words, after passing PIN-entry to open the wallet application, the wallet application can be issued a credit card.

173. To the extent Patent Owner argues that Dua does not expressly mention PIN-entry to open the wallet application prior to card issuance, that would be incorrect, but in any event it is my opinion that such a function would at least be obvious to a POSITA. Using the wallet application requires authentication because "[d]ata in the wallet application is encrypted and protected with a special wallet PIN code … ." Dua ¶¶[0366], [0429]. Making significant changes in the wallet

application, such as "access[ing] stored credentials and chang[ing] any application settings or preferences" requires user authentication. Dua ¶[0366]. Such significant changes includes adding a new credit card. A wallet application can hold multiple credit cards, amongst other confidential information. Dua ¶¶[0041], [0055], [0287]-[0288], [0334]. When the wallet application is opened, such as for credit card issuance, the wallet application allows the user to navigate and view the stored credentials. Dua ¶¶[0324]-[0332], [0334], [0366], [0378]. A similar security risk is that credit card issuance requires the wallet application to connect with, and accept data from, a remote server—usually a WCM. Dua ¶¶[0038], [0179]-[0180], Figs. 3-4. But without requiring PIN-entry to open the wallet for credit card issuance, anyone could allow the wallet application to connect and accept data from an unknown remote server under the pretext of credit card issuance. To ensure security of the wallet application, a POSITA would retain Dua's "default" PIN-entry user authentication when opening the wallet application for credit card use. *See* Dua ¶[0366].

174. Further, it was well known to a POSITA that sensitive functionalities should be protected behind authentication or verification process. EX1019 ¶[0167], FIGS. 10A-B. For instance, U.S. Pub. No. 2010/0082481 discloses and locking a payment application and a functionality labeled "Transactions Mode" behind a PIN code. EX1019 ¶[0167], FIGS. 10A-B.

175. Additionally, a feature within a payment application to add an account or credit cards was well known to a POSITA. *See, e.g.*, EX1019 ¶¶[0136]-[0140], FIGS. 5A-B; EX1039 ¶[0117] ("The user then may be required to enter a personal identification number, a password, a security number, or the like in order to authenticate the user and add the payment option to the device 10."); EX1021 ¶[0047] ("payment credentials (account number, credit card number, etc.) are first unlocked, such as with a thumbprint or other biometric technique, to enable a pre-loaded payment application (step 605)"). And in my opinion, a POSITA would be motivated to incorporate an add-account feature within Dua's PIN-entry-protected wallet application. For instance, EX1019 discloses an add-account feature in its payment app for the iPhone, where a user can open and use the payment app to add an account, such as a credit card, to the app. EX1019 ¶¶[0136]-[0140], FIGS. 5A, 5B. To add an account, a user adds credit card information, and issuers "verif[y] … [the] credit card information" and "confirm the identi[t]y of the user by transmitting one or more verification codes" in order to ensure a valid credit card is sent to the correct user. EX1019 ¶[0143]-[0146], FIGS. 5A, 5B.

176. Indeed, even accessing Dua's wallet application may require entry of and sensing a PIN or biometric because, as disclosed by Dua, "[t]he data stored inside the wireless device is encrypted and protected with the wallet PIN code (or other biometric security information), which is used to allow the user access to the

application." Dua ¶[0429]. Thus, Dua discloses its users cannot even access the wallet application without the wireless device first sensing the appropriate PIN or biometric. And securing access to the wallet application makes sense to a POSITA, as the application can hold credit card and other sensitive, confidential information. Dua ¶¶[0041], [0055], [0287]-[0288], [0334]. The wallet application allows the user to navigate, view, and select the stored credentials for transmission and thus needs to be protected. Dua ¶¶[0324]-[0332], [0334], [0366], [0378], [0384]. Again, in my opinion Dua discloses that protection in the form of PIN or biometric entry.

177. Dua discloses that PIN-entry requires the wireless device receiving a PIN code after being typed in a PIN-entry or text-entry field by a keyboard or touchscreen keyboard—***sensing by a smartphone, using a smartphone-based sensor, physiological data associated with a living organism***. Dua ¶¶[0366], [0384], [0395], FIGS. 1, 3, 6(a), 8, 9. A POSITA would understand a touch screen or keypad as sensing touch, such as through a capacitive touch screen. *See also* EX1042. The entered PIN code validates the user's identity. For instance, a valid PIN code decrypts the wallet application's data or, as also understood by a POSITA, matches a valid PIN code stored on the wallet application. Dua ¶¶[0050], [0366], [0399], [0429].

178. And as I explained above, Dua also discloses replacing PIN codes with fingerprints or other biometric data. The "wireless device's embedded biometric

technologies," which involves biometric sensors, will scan for fingerprints—***sensing by a smartphone, using a smartphone-based sensor, physiological data associated with a living organism***. Dua ¶¶[0366], [0414]. Dua contemplates using other biometric data biometric data, such as "iris, voiceprints, facial recognition, and hand geometry." Dua ¶[0534]. Using biometric data, like a "fingerprint[,] in lieu of a PIN code to authenticate a user to the wallet application" requires comparing the scanned biometric data with valid biometric data stored on the wireless device or, as also disclosed by Dua, decrypting the wallet application's data with the scanned biometric data. Dua ¶¶[0050], [0366], [0399], [0429].

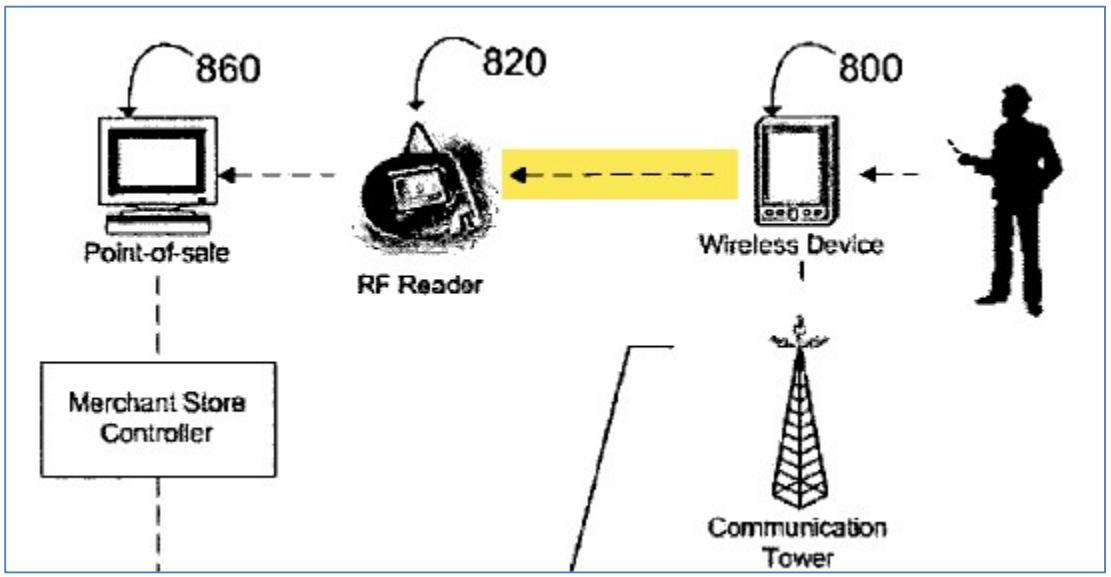
179. Further confirming my opinion that this limitation is disclosed by Dua, Patent Owner alleges in its district court infringement contentions that using biometrics to authenticate a user meets limitation 1[a]—which is precisely what Dua discloses. EX1016 at 7-12.

(iii) 1[b]

180. In my opinion, Dua discloses this limitation. Specifically, Dua discloses facilitating transactions and other communications between its wireless device and a merchant POS reader/terminal "via, for example, a short range wireless link . . . ." Dua ¶[0026]. This short-range link between wireless device and POS reader is disclosed throughout Dua. *E.g.*, Abstract ("The user holding the credential may then use the handheld device to conduct the authorized transaction or set of

transactions via, for example, ***a short range wireless link*** with a point-of-sale terminal."), ¶[0041] ("Wireless device 200 also preferably has an integrated ***short-range communication capability*** for transmitting confidential information and exchanging other data between the wallet application and ***an external reader that is in proximity to the wireless device***").

181. For example, I've annotated a portion of Figure 8, below, to highlight the short-range link between Dua's wireless device 800 (***the smartphone***) and an RF reader 820 of a merchant POS terminal 860 (***an entity, wherein the entity is not the living organism***) in yellow:



182. As is clearly shown and disclosed in Dua, the short-range proximity criterion that must be met in Dua is between a user's (***living organism***) wireless device 800 (***smartphone***) and an RF reader 820 of a merchant point-of-sale (POS) terminal 860 (***an entity, wherein the entity is not the living organism***). *See also*

Dua ¶[0405] ("point of sale terminal 860, via RF reader 820 can be used to capture and transmit an electronic credential from a wireless device").

183. Dua's financial transactions cannot occur unless the consumer wireless device is "in close proximity to a reader device" such that it can communicate and engage in a "proximity transaction." Dua ¶[0315]. Dua discloses that, "[f]or example, 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*.; *see also* ¶¶[0321], [0355], [0371]. Dua also discloses the RFID chip can be an NFC chip—thus disclosing NFC transactions. *Id*. ¶[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.").

184. A POSITA would understand that short-range RFID links, including in particular the NFC communication link disclosed by Dua, are established responsive to detecting that a proximity criterion is satisfied between the smartphone and an entity (the POS reader/terminal). Specifically, Dua's RFID and NFC communications would only be effective if there is an underlying signal of sufficient signal strength detected by the two entities (the smartphone and the POS reader/terminal) such that they can establish a communications link and engage in communications associated with the financial transaction. *E.g.*, EX1035 at 4, 36;

EX1037 at 3. As I explained above with respect to limitation 1[b] in the context of Jain, which also discloses short-range, NFC communications, the signal strength between devices correlates to proximity and rapidly deteriorates as the distance between them increases. That is why RFID and NFC transactions are known to have a range of only about 3 meters and 10 centimeters, respectively.

185. Accordingly, receipt of a short-range RFID or NFC signal (by either Dua's wireless device or POS reader) corresponds to and teaches detecting that a proximity criterion has been satisfied between the smartphone and an entity—the entity being, for example, the retail store of a merchant that houses the POS device with which a user's wireless device communications as part of a transaction.

186. Dua also discloses additional embodiments that further disclose the detection of proximity between a smartphone and POS reader.

187. For example, Dua discloses that "the device is not placed in proximity of the reader" for a set time (*e.g.*, "30 seconds"), the wallet application on the wireless device "will disable RF communication and the application may shutdown or go into its normal dormant state." Dua ¶¶[0383], [0384]. This requires the device (***smartphone***) to detect whether it is proximate to the reader of the merchant's POS terminal (***entity***), otherwise it would not know to shut down RF communication.

188. In another example, Dua discloses that a consumer may 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." Dua ¶[0321]. The devices may then "exchange encryption keys via RF in order to establish a secure Bluetooth connection." *Id*. This teaches limitation 1[b] because the RFID reader would not know to send a command specifically to a specific user's wireless device that is in proximity with the RFID reader unless the RFID reader has detected said proximity with the wireless device. And consistent with my opinions above, the two devices would not be able to exchange encryption keys via RF unless and until they have detected one another's presence in terms of proximity. Indeed, Dua discloses the RFID reader directing "a command to ***the wallet application*** [of a user in proximity]"—it does not disclose indiscriminately broadcasting the command. Such directing of a command to a specific device would not be possible without first detecting proximity with the device.

189. Again, Dua teaches that its short-range communications protocol may be NFC. Dua ¶[0016]. ECMA-340 explains that an NFC "transaction" requires an "initialization" (described in §11 of the standard) and then a "data exchange" (described in §12 of the standard). *See supra* ¶122; EX1047 §4.26, §10, Figure 5. The standard specifies two devices ("Initiator" and "Target") and two communication modes ("Passive" and "Active"). EX1047 §1, §4.1, §4.7, §4.17, §4.23, §7.

190. Regardless of whether Dua's POS device or mobile device is the "Initiator" or "Target," or what communication mode they use: every combination results in Dua's mobile device (***smartphone***) detecting a ***proximity criterion is satisfied*** and then establishing a short-range link that is used for subsequent communications. Specifically, in both modes, an "Initiator" device "shall activate its RF field" and a "Target" device then "shall be activated by the RF field of the Initiator." EX1047 §10. Then, the "Initiator" sends one or more commands (e.g., ALL_REQ, SENS_REQ, and/or ATR_REQ) and receives one or more responses (e.g., SENS_RES and/or ATR_RES). EX1047 §§11.2.1.16-.17, §11.2.1.23, §11.3.2, §§12.2-.3, Figures 13, 24-25. *See supra* ¶¶123-124.

191. Thus, regardless of what mode is used and which of Dua's devices is the Initiator or Target, the Target device detects a sufficiently strong field from the Initiator (***proximity criterion is satisfied***), and the Initiator device detects that a Target is within its field by receiving a response to a command from the Target (***proximity criterion is satisfied***). This exchange of commands and responses results in selection of a particular "Target" and attributes/parameters for further communication with the same, thereby establishing a short-range link. EX1047 §7, §§11.2.1.24-25, §12, §12.1, Figures 22, 24-25. After this link is established, the Initiator and the Target communicate using ECMA-340's data exchange protocol. EX1047 Figures 5, 23, and 24. This includes transmission of Dua's credential data.

192. At a minimum, it would have been obvious to implement Dua's NFC communications this way. Dua tells a POSITA to look to "ISO/IEC 14443" RF proximity standard (Dua ¶[0013]), which would motivate a POSITA to also look to the standard for NFC. And a POSITA would have been motivated to implement the standard for at least the reasons I set forth above, in paragraph 126.

193. These embodiments are further evidence of limitation 1[b] and are consistent with a POSITA's understanding that the wireless device (***smartphone***) must detect it is proximate the reader of a merchant POS terminal (***entity***), or *vice versa*, before communicating, because the short-range link between the wireless device and reader/POS terminal requires proximity.

194. Moreover, Patent Owner alleges in its district court infringement contentions that the use of NFC to conduct financial transactions with a POS terminal meets limitation 1[b]—which is precisely what is disclosed in Dua. EX1016 at 12-15.

195. To the extent Patent Owner argues that this limitation is not disclosed by Dua, that would be incorrect, but in any event it is my opinion that, at a minimum, it would have been obvious to a POSITA to have Dua's smartphone detect proximity to a POS device of a merchant (or *vice versa*) before attempting to engage in transactions or other communications. Specifically, to ensure communications are successful and not wasted signaling (which wastes battery life—a particularly

important problem faced by mobile devices at the time of the '411 patent), and further to avoid the security risk of indiscriminately transmitting sensitive financial information over the air (which was also of particular concern with wireless transactions), there must first be a determination that Dua's smartphone is near the merchant and the merchant POS before attempting a payment transaction.

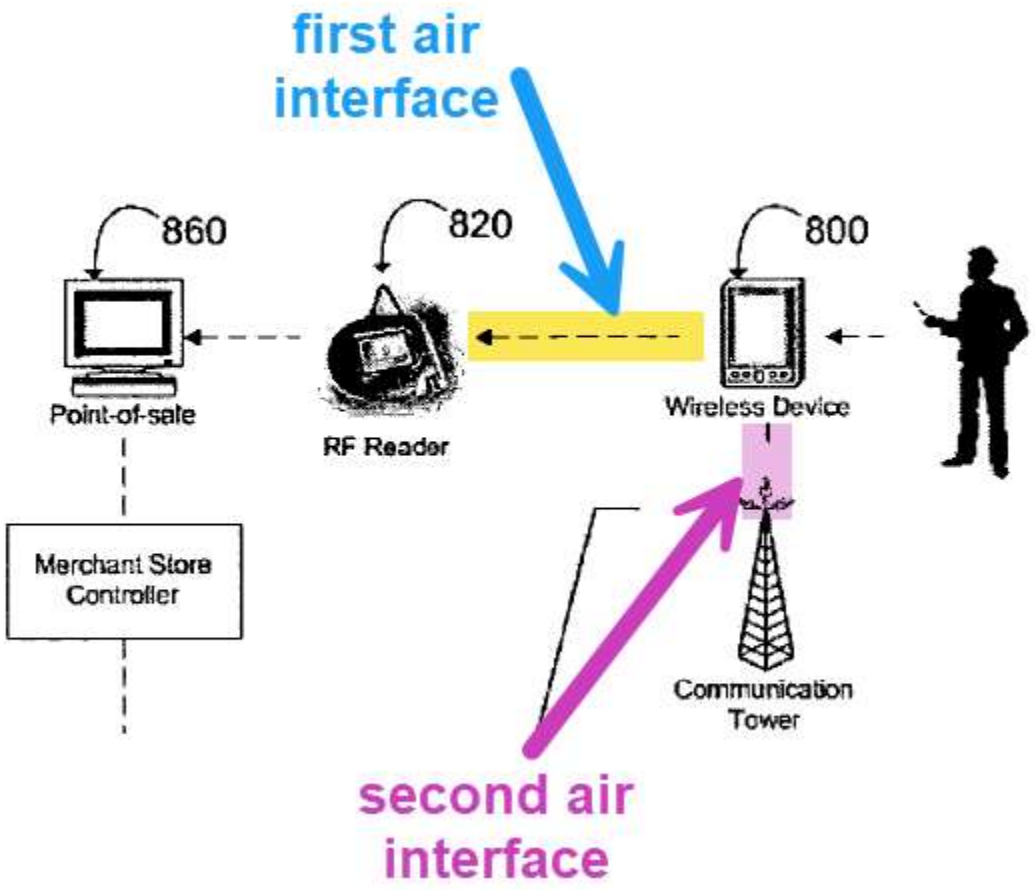
196. If proximity detection was not used, short-range communications between smartphones and POS readers would fail, cause the smartphone's battery to drain, and/or send information to unintended recipients. Indeed, proximity detection in such contexts and to avoid such problems were well-known to a POSITA at the time of the '411 patent. For example, EX1020 teaches using NFC to limit the range at which communication may take place between devices. EX1020 ¶[0041], [0063] [0041]. EX1020 further teaches using this ability to detect proximity with a Wi-Fi hotspot before connecting to it. EX1020 ¶[0073]. A POSITA would be motivated and able to use Dua's wireless device in the same manner to detect proximity with a merchant and its POS device before communicating with it at least to avoid all the problems noted above.

197. It would have also been obvious for a POSITA to use Dua's wireless device as the Target and use NFC's passive communications mode, particularly since Dua expressly discloses the use of NFC as an optional communications platform for its short-range communications. In NFC passive mode, the wireless

device detects the RF field generated by the RF reader/POS terminal when it is proximate the reader/terminal of the merchant POS entity (***detecting that a proximity criterion is satisfied between the smartphone and an entity***) and thereafter engages in further communications, such as those relating to a financial transaction. See paragraphs 120-126 and 189-192, above, where I discuss the ECMA-340 standard for NFC.

(iv) 1[c]

198. In my opinion, Dua discloses this limitation. Dua discloses ***a plurality of air interfaces with which the smartphone is capable of communicating***, including: (1) a first air interface for short-range communications (such as for contactless transactions) with RFID/NFC readers at a point of sale (*e.g.*, RF Reader 820/POS 860); and (2) a second air interface for cellular and other communications with a cellular network, for example. *See* Dua ¶¶[0015]-[0018], [0044], [0051], [0409], Fig. 1 (element 155). For example, I've annotated a portion of Fig. 8, excerpted below, to highlight the first and second air interfaces disclosed in Dua:



199. Dua's first air interface is used for "exchang[ing] data over short ranges with other wireless devices or readers" (Dua ¶¶[0015], [0018], [0041], [0383]) and can include, for example, infrared, RFID, and NFC air interfaces, among others. *Id*. ¶[0016].

200. Separately, Dua's second air interface is used for cellular communications. Dua ¶[0015]. A POSITA would understand that cell phones, including those expressly disclosed by Dua, make and receive voice calls and exchange data over a cellular network using a cellular modem that communicates

over a cellular antenna that acts as its interface with the air and allowing the over-the-air cellular communications. Indeed, Dua discloses using cellular networks, which Dua calls a "mobile operator network," for data communications. *See, e.g.*, Dua ¶¶[0044], [0051], [0409], Fig. 1 (element 155), Fig. 8 (element 880). And Figs. 1 and 8 both show the wireless device connecting to the mobile operator network via a cell tower (see above).

201. Patent Owner also alleges in its district court infringement contentions that a cellular smartphone capable of conducting transactions over NFC meets the ***plurality of air interfaces with which the smartphone is capable of communicating***. EX1016 at 14-20.

202. In my opinion, Dua also discloses the smartphone ***selectively communicating*** over the first air interface responsive to and based on satisfying the proximity criterion and the value of physiological data that was sensed.

203. With respect to selectively communicating responsive to the proximity criterion, I explained above with respect to limitation 1[b] that Dua's wireless device only engages in contactless payments with a merchant POS terminal when it detects proximity with the merchant and its POS terminal's RFID/NFC reader, such as by being proximate the RFID/NFC reader within a certain range (e.g., around 3 meters for RFID and 10 centimeters for NFC. Dua ¶¶[0315], [0321], [0352]-[0355], [0371].

204. Dua also discloses an embodiment that shuts down the wallet application and disables RF communications if proximity with the merchant POS terminal is not detected for a set time. Dua ¶¶[0383], [0384]. Thus, a POSITA would recognize that subsequent proximity-based payment transactions (and selective communications related thereto) are based on and responsive to detecting proximity with the RF reader of the merchant POS terminal for that set period of time.

205. As I also explained above with respect to limitation 1[b], Dua also discloses an embodiment in which a payment credential used for mobile transactions is issued to a user who brings "his wireless device in proximity of an RFID reader [of an issuer], which will send a command to the wallet application signifying that it is going to receive a new credential via Bluetooth" and thereafter "exchang[ing] encryption keys via RF in order to establish a secure Bluetooth connection." Dua ¶[0321]. In this embodiment, proximity between the wireless device and "an issuer's site" (the ***entity***) requires detecting proximity with the issuer's RFID reader according to transmission and receipt of the command from the reader (***detecting proximity***). In other words, the RFID reader detects proximity in order to send a command, and the wireless device detects proximity by receiving the command. The wireless device then communicates with the reader to "exchange encryption keys via RF" (***selectively communicating***)—this is a selective communication because it

is based on having detected proximity and is also directed to a specific RFID reader (it is not an indiscriminate broadcast). *Id*.

206. Moreover, subsequent wireless device transactions using the acquired credential (*e.g.*, "digital debit card") are also selective communications, as they only occur after and are thus responsive to: (1) the initial proximity detection with the credential issuer and its RFID reader; and (2) subsequent proximity detection with a merchant and its RFID reader.

207. With respect to selectively communicating responsive to the value of physiological data that was sensed, I explained above with respect to limitation 1[a] that Dua's wireless device also does not communicate with a POS terminal unless its user has been authenticated—both as part of initial credential acquisition and each individual transaction—by entry of a PIN on the wireless device touchscreen or through biometric/fingerprint scan (***responsive to a value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor***). Dua ¶¶[0366], [0384], [0395], [0414].

208. .Dua's wireless device therefore selectively communicates with RFID/NFC reader of a merchant POS terminal over RFID, NFC, or other short-range communication medium responsive to both the proximity criterion being met and the value of physiological data sensed (***selectively communicating by the***

smartphone using a first air interface of a plurality of air interfaces with which the smartphone is capable of communicating . . .).

209. Patent Owner also alleges in its district court infringement contentions that using a smartphone to conduct a financial transaction via NFC after having authenticated the user and bringing the phone proximate a payment terminal meets the ***selectively communicating by the smartphone using a first air interface of a plurality of air interfaces with which the smartphone is capable of communicating, responsive to the proximity criterion having been detected as being satisfied and responsive to a value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor***—and this is precisely what is taught by Dua. EX1016 at 15-16.

(v) 1[d]

210. In my opinion, Dua discloses this limitation. As I explained in my opinions with respect to limitations 1[a] and 1[c], Dua's wireless device does not communicate with the POS RFID reader unless the user of the wireless device has been authenticated—first as part of initial credential acquisition but also for each individual transaction with a credential. And the user is authenticated by entry of a PIN on the wireless device touchscreen or through biometric/fingerprint scan. Without user authentication, NFC transactions cannot occur. Dua ¶¶[0128]-[0129], [0178], [0180], [0250], [0366], [0384], [0395], [0414], [0534].

211. Thus, a POSITA would understand that even if Dua's wireless device is brought proximate a merchant or issuer and the merchant/issuer's corresponding POS terminal, the wireless device and wallet application will refrain from communicating with the RFID reader of the POS terminal using the first air interface unless and until the user opens the wallet application and selects a credential for transmission. In either instance (whether opening the wallet application or selecting a credential for a transaction), Dua requires the user to enter and verify their PIN or fingerprint. *E.g.*, Dua ¶[0366] ("The default security setting in the wallet application is that PIN-entry is required before the wallet application can be 'opened' and any credentials transmitted to an external device."); *cf*. ¶[0395] (disclosing embodiment in which RF communication is not enabled unless the user inputs their PIN).

212. As further evidence that Dua discloses limitation 1[d], Patent Owner alleges in its district court infringement contentions that this limitation is met just by requiring a smartphone to authenticate its user via biometrics before it is allowed to conduct a financial transaction via NFC, even though the phone may be proximate a payment terminal—precisely what is taught in Dua. EX1016 at 20-22.

(vi) 1[e]

213. In my opinion, Dua discloses this limitation. As I explained above with respect to limitations 1[a] and 1[c], Dua's wireless device (***smartphone***) communicates with issuers and merchants and their respective POS

readers/terminals (***one or more other devices***), including selectively sending and receiving information (***selectively sending information by the smartphone to one or more other devices*** and ***receiving information by the smartphone from the one or more other devices***) responsive to a user's authentication via PIN or biometric (***responsive to said value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor satisfying the criterion***).

214. For example, Dua requires a user to enter a PIN (or biometric) "before the wallet application can be 'opened' and any ***credentials transmitted to an external device***" such as a POS reader/terminal (***responsive to said value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor satisfying the criterion***). Dua ¶¶[0366], [0384]. Thus the communications are responsive to the physiological data sensed.

215. Once authenticated, the user "will be required to pre-select all the credentials he wants to ***transmit to a reader*** prior to placing his device in proximity of the reader during a transaction" and "the wallet application is ready to ***transmit the credential(s)*** via its RFID interface." Dua ¶¶[0371]-[0378]. "When the wireless device is placed in proximity to the reader, the selected credential(s) are automatically ***transmitted*** by the RFID chip in the wireless device to the reader"

(***selectively sending information by the smartphone to one or more other devices***). *Id*.; *see also* ¶[0320] ("credential data is transmitted from the wireless device to a merchant"). Thus the communications are also responsive to the detected proximity.

216. Dua's wireless device also receives information from the RFID reader of a POS terminal. Specifically, a POSITA would understand that the NFC communications associated with a financial transaction are bidirectional and, indeed, Dua expressly states that the wireless device and POS readers/terminals engage in a "***bi-directional*** exchange of data." Dua ¶[0318]. In other words, the wireless device will both send information to the POS and receive information from it.

217. For example, (1) a POS reader/terminal may send a prompt to the "wireless device for various types of preferences, questions, or other data input in sequence" (Dua ¶[0319]), (2) "during a transaction—a point-of-sale device may establish secure connectivity with the user's wireless device and poll it for a list of user-defined payment methods that the user can select from using the user-interface of the POS system" (¶[0317]), and (3) the wireless device and POS reader/terminal may "exchang[e] encryption keys via RFID" (¶[0318])—all of which teach ***receiving information by the smartphone from the one or more other devices***.

218. As further evidence that Dua discloses limitation 1[e], Dua also describes an embodiment in which a user presses a "hot button" to send a pre-selected payment method and credentials matching a particular POS reader's "reader

key" to that specific reader (this is ***selectively sending*** because the transmission is directed to a specific POS reader and is not an indiscriminate broadcast), "provided that the reader sent the key in its initial communication with the wireless device" (this shows the wireless device ***receiving*** information—*i.e.*, a reader key). Dua ¶¶[0393], [0353]. The transmission and reception of information in this embodiment is responsive to user authentication, as pressing the hot button "may prompt the user to input a PIN before RF communication can be enabled." Dua ¶[0395]. And, further, it is responsive to proximity, as the wireless device would not have received a reader key or transmitted the payment information without proximity to the POS.

219. In sum, the user pushes a button and is prompted to enter a PIN before RF communication is enabled (responsive to said value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor satisfying the criterion) after which the wireless device receives a reader key from the reader/terminal (receiving information by the smartphone from the one or more other devices) and, in response, transmits a payment method and corresponding credential for that specific reader/terminal (selectively sending information by the smartphone to one or more other devices).

220. Moreover, Patent Owner alleges in its district court infringement contentions that using a smartphone to submit a financial transaction to a POS terminal and receive a confirmation from the POS terminal responsive to user

authentication (via "a fingerprint, facial recognition, or iris") meets limitation 1[e]—that is precisely what is disclosed in Dua. EX1016 at 22-26.

(vii) 1[f]

221. In my opinion, Dua discloses this limitation. As I explained above, Dua's wireless device may be a cell phone (Dua ¶[0015]), which a POSITA would understand can make and receives voice calls and exchange data over a cellular network.

222. Dua also discloses using cellular networks for data communications. Dua refers to a cellular network as a "mobile operator network." *E.g.*, Dua ¶¶[0044], [0051], [0409]; *see also* Fig. 1 (element 155) and Fig. 8 (element 880), both of which show the wireless device connecting the mobile operator network via a cell tower. Dua thus discloses the wireless device communicating ***using a second air interface . . . that differs from the first air interface***.

223. For example, Dua discloses that its wireless device and "wallet application is designed to facilitate transactions in a proximity, personal, and remote environment using the device's short-range ***or long-range transmission capability***." Dua ¶[0333]. Thus, in addition to allowing short-range NFC-based financial transactions, the wireless device can also engage in financial transactions over the cellular network. Dua ¶[0323] ("In a remote-or online--environment, transactions

are conducted with a remote server ***over a wireless network***" and can include "online purchases," "banking," and "downloading digital content").

224. Moreover, Dua expressly distinguishes the long-range transmissions over a wireless network from short-range communications with a POS reader/terminal, thereby recognizing that the wireless device communicates over both the first and second air interfaces. *E.g.*, Dua ¶[0026] (explaining that "credentials are ultimately supplied to a handheld device such as a mobile telephone via a wireless network" and separately referring to and, thus, distinguishing "a short range wireless link with a point-of-sale (POS) terminal").

225. For example, Dua discloses a feature by which a Wireless Credential Manager (WCM) can remotely wipe the wallet application of a stolen wireless device over a mobile operator's wireless network—***not*** the first air interface. Dua ¶¶[0454], [0455] (explaining this feature requires the wireless device to "have signal to the wireless network").

226. Additionally, Patent Owner alleges in its district court infringement contentions that a smartphone that can communicate over a cellular data network in addition to NFC meets limitation 1[f]—precisely what is disclosed in Dua. EX1016 at 26-27.

(b) Claim 2

(i) 2[pre]

227. In my opinion, Dua discloses this limitation for the same reasons as I explained above for limitation 1[b].

(ii) 2[a]

228. In my opinion, Dua discloses this limitation. For example, Dua discloses that the effective range of unpowered RFID smartcards is "typically two to three inches" for unpowered cards. Dua ¶[0009]. These are the cards that are included in Dua's wireless device and that Dua's wireless device is intended to emulate. Also, that range is consistent with what a POSITA knows about NFC: that under ideal circumstances, NFC is considered to have an effective range of about 10 cm. This was recognized in other references at the time, including Jain. Jain ¶¶[0030], [0045]. *See also* EX1032 §8. Thus, Dua's detection of proximity (see my opinions with respect to limitations 1[b] and 2[a]) includes ***detecting that a proximity criterion of less than 10 meters in distance is satisfied between the smartphone and the entity***.

(iii) 2[b]

229. In my opinion, Dua discloses this limitation. As I explained above for limitation 1[b], the detecting is performed by the smartphone, by a device that is associated with the entity, by a system that is associated with the smartphone, or a

combination thereof. Specifically, either Dua's wireless device detects proximity, POS terminal with RFID/NFC reader detects proximity, or a combination of the two detect proximity through their exchange of communications at short range.

230. Moreover, in the language of the ECMA-340 NFC standard, which I discussed above, one of those devices is the Initiator and the other is the Target. Either way, both the Target and the Initiator (and thus both the wireless device and the POS terminal with a reader) detect that a proximity criterion is satisfied. See also my opinions above with respect to limitation 1[b].

(c) Claim 3

(i) 3[pre], 3[a]

231. As I explained in my opinions above, Dua discloses a smartphone having a processor that is configured to and does control the smartphone to perform the claimed process steps and capabilities. Dua Abstract, FIGS. 3, 5, 6(a)-8.

232. Dua's wireless device includes a "handheld device, such as a mobile telephone," "capable of wirelessly connecting to the internet" and phone applications like a "wallet application." Dua Abstract, ¶¶[0041], [0049], [0050], [0051], [0287]-[0288], FIGS. 3, 5, 6(a)-8. A POSITA would understand that a wireless device that can connect to the internet and that includes and can run applications such as a wallet application is a smartphone and includes one or more processors for running such applications.

(ii) 3[b] – 3[g]

233. The remaining limitations of claim 3 are substantively identical to claim 1 and merely remove the references in claim 1 to claim steps being performed "by a smartphone," as claim 3 separately recites the smartphone in 3[pre]/3[a]. Accordingly, Dua discloses a smartphone with a processor that implements the claimed capabilities for the same reasons provided above with respect to claim 1, where my opinions with respect to limitations 1[a]-1[f] map directly to limitations 3[b]-[g], which are therefore disclosed by Dua for the same reasons as 1[a]-1[f], respectively.

(d) Claim 4

234. Claim 4 is substantively identical to claim 2, limitations 2[pre] and 2[a]. Accordingly, my opinions relating to Dua's disclosure of limitations 2[pre] and 2[a] map directly to limitations 4[pre] and 4[a], which are therefore disclosed by Dua for the same reasons as 2[pre] and 2[a], respectively.

VI. Secondary Considerations of Non-Obviousness

235. I understand that so-called "secondary considerations" are legally relevant to an obviousness analysis. It is my opinion that the secondary considerations I consider here further weigh in favor of obviousness.

236. In my opinion, there is a lack of commercial success for any product practicing the '411 patent because the Patent Owner has not practiced the claimed

invention (at any point in time) and because I am not aware of any other successful commercial deployments in the United States that are proven to embody the asserted claims. Even if such evidence existed, it would not undermine the strong showing of invalidity. Moreover, any difference between the claims of the '411 patent and the prior art is minimal, and any secondary considerations would have minimal impact on the invalidity analysis.

237. In my opinion, there was no long-felt, unresolved need met by the '411 patent. It is my opinion that at the time of the alleged invention there were no technical barriers to wide-scale deployment of contactless payment with mobile devices, let alone technical barriers requiring disclosure of the alleged novelties of the '411 patent. To the extent wide-scale deployment in the United States post-dated the '411 patent, my understanding is that this was for reasons other than technical feasibility, such as industry and market barriers. Further, a vast number of contactless payment systems and trials of those systems existed before the '411 priority date. In my opinion, this indicates that many within the market observed the desirability of such systems and were concurrently working towards implementing them. In sum, I'm not aware of any of the factors for secondary considerations being present, but even if they existed, it would not impact the invalidity analysis.

VII. Conclusion

238. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

* * *

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

Respectfully submitted,

Kevin C. Almeroth, Ph.D.