

**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. 11,770,756

“Mobile Device Mode Enablement/Disablement Responsive To Sensing A  
Physiological Parameter”

---

DECLARATION OF KEVIN ALMEROOTH, PH.D., IN SUPPORT OF  
PETITION FOR *INTER PARTES* REVIEW OF  
U.S. PATENT NO. 11,770,756

**TABLE OF CONTENTS**

I.	Introduction.....	1
A.	Qualifications .....	1
1.	Educational Background.....	1
2.	Career .....	2
3.	Other Relevant Qualifications.....	8
B.	Previous Expert Witness Testimony .....	10
C.	Preparation for this Declaration .....	10
II.	Legal Understanding.....	11
A.	Claim Construction.....	12
B.	Anticipation .....	12
C.	Obviousness.....	13
III.	The '756 Patent.....	14
A.	Priority Date .....	14
B.	Specification.....	15
C.	Prosecution History .....	16
1.	Prosecution History of the '756 Patent (EX1011).....	16
2.	'172 Patent File History .....	17
3.	'411 Patent File History .....	18
4.	'708 Patent File History .....	20

IPR of U.S. Patent No. 11,770,756

Decl. of Dr. Kevin Almeroth

5.	'199 Patent File History .....	21
6.	'015 Patent File History (Unasserted) .....	22
7.	'432 Patent File History .....	23
8.	'118 Patent File History (Unasserted) .....	24
9.	U.S. Patent Application Publication No. 2023/0403631 (pending) .....	25
10.	'743 Patent File History .....	26
11.	'793 Patent File History .....	26
D.	Level of Ordinary Skill in the Art .....	27
E.	Claim Construction.....	28
F.	Challenged Claims .....	29
IV.	State of the Art.....	36
V.	Grounds.....	38
A.	<u>Ground 1: Jain (EX1017)</u> .....	39
1.	Background .....	39
2.	Analysis.....	45
B.	<u>Ground 2: Dua (EX1018)</u> .....	82
1.	Background .....	82
2.	Analysis.....	86
VI.	Secondary Considerations of Non-Obviousness .....	126
VII.	Conclusion .....	127

### LIST OF EXHIBITS

<b>Exhibit</b>	<b>Description</b>
EX1001	U.S. Patent No. 11,770,756 (“’756 Patent”)
EX1002	Declaration of Dr. 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 ’756 Patent
EX1017	U.S. Pat. Pub. No. 2009/0069049 (“Jain”)
EX1018	U.S. Pat. Pub. No. 2006/0165060 (“Dua”)
EX1019	U.S. Pat. Pub. No. 2010/0082481
EX1020	U.S. Pat. Pub. No. 2010/0082490
EX1021	U.S. Pat. Pub. No. 2009/0307140
EX1022	“Product Overview”, Vivotech (Jun. 27, 2007), <a href="https://web.archive.org/web/20070627155330/">https://web.archive.org/web/20070627155330/</a> <a href="http://www.vivotech.com/products/vivo_pay/index.asp">http://www.vivotech.com/products/vivo_pay/index.asp</a>

Exhibit	Description
EX1023	“Kyocera Wireless Mobile Phones Excel in Cellular South WirelessWallet Consumer Trial”, Kyocera (Oct. 18, 2007), <a href="https://americas.kyocera.com/press-releases/press-releases_201503201874.htm">https://americas.kyocera.com/press-releases/press-releases_201503201874.htm</a>
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), <a href="https://web.archive.org/web/20060615050709/http://www.nfc-forum.org/aboutnfc/about_nfc_technology/">https://web.archive.org/web/20060615050709/http://www.nfc-forum.org/aboutnfc/about_nfc_technology/</a>
EX1032	Erik Rolf & Viktor Nilsson, “Near Field Communication (NFC) for Mobile Phones” (Aug. 2006)
EX1033	Wall Street Journal, Vivotech (Aug. 12, 2005), <a href="https://web.archive.org/web/20060915080521if_/http://www.vivotech.com:80/newsroom/coverage/Videos/Wall_Street_Journal/Wall_Street_Journal.wmv">https://web.archive.org/web/20060915080521if_/http://www.vivotech.com:80/newsroom/coverage/Videos/Wall_Street_Journal/Wall_Street_Journal.wmv</a>
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)

<b>Exhibit</b>	<b>Description</b>
EX1038	Arumugam et al., “Consumer Electronics Application and Coverage Constraints Using Bluetooth and Proposed Bluetooth Evolution Technologies” (Aug. 2001)
EX1039	U.S. Pub. No. 2010/0082445
EX1040	Information Sciences Institute, RFC 793 Transmission Control Protocol (Sep. 1981), <a href="https://datatracker.ietf.org/doc/html/rfc793">https://datatracker.ietf.org/doc/html/rfc793</a>
EX1041	“Bluetooth Basics”, Bluetooth (Apr. 23, 2006), <a href="https://web.archive.org/web/20060423011921/http://www.bluetooth.com/Bluetooth/Learn/Basics/">https://web.archive.org/web/20060423011921/http://www.bluetooth.com/Bluetooth/Learn/Basics/</a>
EX1042	“iPhone Premieres This Friday Night at Apple Retail Stores”, Apple (Jun. 28, 2007), <a href="https://www.apple.com/newsroom/2007/06/28iPhone-Premieres-This-Friday-Night-at-Apple-Retail-Stores/">https://www.apple.com/newsroom/2007/06/28iPhone-Premieres-This-Friday-Night-at-Apple-Retail-Stores/</a>
EX1043	“Enabling Fast Wireless Networks with OFDM,” EETimes (February 1, 2001), <a href="https://www.eetimes.com/enabling-fast-wireless-networks-with-ofdm/">https://www.eetimes.com/enabling-fast-wireless-networks-with-ofdm/</a>
EX1044	IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999), IEEE Computer Society, June 12, 2007
EX1045	“Getting Base Stations Ready for LTE”, EETimes (April 17, 2007), <a href="https://www.eetimes.com/getting-base-stations-ready-for-lte/">https://www.eetimes.com/getting-base-stations-ready-for-lte/</a>
EX1046	3rd Generation Partnership Project; Technical Specification Group Radio Access Network; LTE Physical Layer – General Description (Release 8), 3rd Generation Partnership Project, March 2007
EX1047	Near Field Communication – Interface and Protocol (NFCIP-1), Standard ECMA-340 (2nd Edition)

IPR of U.S. Patent No. 11,770,756

Decl. of Dr. Kevin Almeroth

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 1-18 (“the challenged claims”) of U.S. Patent No. 11,770,756 (“the ’756 Patent”). I have been asked by the Petitioner to assist in evaluating the claims and the disclosure of the ’756 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

IPR of U.S. Patent No. 11,770,756

Decl. of Dr. Kevin Almeroth

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

IPR of U.S. Patent No. 11,770,756

Decl. of Dr. Kevin Almeroth

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,

IPR of U.S. Patent No. 11,770,756

Decl. of Dr. Kevin Almeroth

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 at the end of EX1004.

**C. Preparation for this Declaration**

22. In forming my opinions, I have considered the '756 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 '756 Patent (a "POSITA"). My understanding of "POSITA" and "priority date" are set forth below. I have also reviewed the file history of the '756 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

IPR of U.S. Patent No. 11,770,756

Decl. of Dr. Kevin Almeroth

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 '756 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 '756 Patent**

33. The '756 Patent is titled "Mobile Device Mode Enablement/Disablement Responsive To Sensing A Physiological Parameter."

34. The '756 Patent lists inventors Peter D. Karabinis and Rajendra Singh.

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

#### **A. Priority Date**

36. The '756 Patent claims priority to U.S. Patent Application No. 12/264,711, filed on November 4, 2008.

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

IPR of U.S. Patent No. 11,770,756

Decl. of Dr. Kevin Almeroth

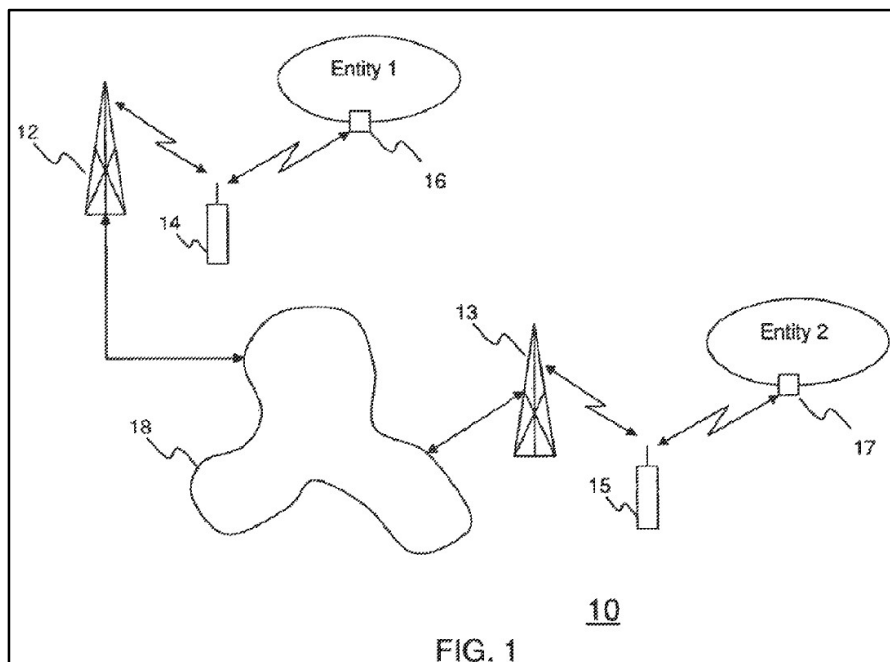
No. 12/264,711, filed on November 4, 2008, and issued as U.S. Patent No. 9,462,411 on October 4, 2016.

## **B. Specification**

38. The '756 Patent specification relies on long-existing technologies, such as “wireless communications device[s],” “air interface protocol[s],” “signal strength measurement such as RSSI,” “Radio Frequency (RF),” and the “Internet Protocol (IP).” EX1001 3:12-22, 7:17-27, 8:9-20, 10:1-31. It further relies on long-established, generic concepts of computer systems such as “authorization,” “identity,” “sensors,” and “communications system[s].” EX1001 4:5-30, 5:39-63, 6:13-30, 8:62-9:21. 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 1:34-47. It also assumes, in the “Background of the Invention” section, that mobile phones could act as digital wallets. *See* EX1001 1:44-47. The '756 Patent specification also relies on already-existing communications protocols. *See, e.g.*, EX1001 7:17-27. Nor does the specification disclose new or improved means of sensing (including physiological/biometric) or proximity detection by mobile phones.

39. At the heart of the disclosure is a mobile wireless device (element 14 in FIG. 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 3:13-22. 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 3:23-36, 3:51-59. For example, the device may determine proximity using well known means such as detecting a low-power or short range signal radiated from a (third) device (element 16 in FIG. 1) that is part of or associated with the entity. See EX1001 3:37-41, 3:60-4:20, FIG. 1.



## C. Prosecution History

### 1. Prosecution History of the '756 Patent (EX1011)

40. 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.

41. 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.

42. 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.

43. 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.

44. Finally, Applicant made what it characterized as “non substantive” amendments to claim 1. EX1011 at 158, 164.

## **2. ’172 Patent File History**

45. U.S. Patent Application No. 18/523,863 was filed on November 29, 2023, and issued on Mar. 19, 2024 as U.S. Patent No. 11,937,172 (“’172 patent”)

46. 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

IPR of U.S. Patent No. 11,770,756

Decl. of Dr. Kevin Almeroth

claims 1 and 9's limitations "receiving by the smartphone second data from the first device, comprising the authorization..." EX1014 at 348-49.

### **3. '411 Patent File History**

47. U.S. Patent Application No. 12/264,711 was filed on November 4, 2008 and issued on October 4, 2016 as U.S. Patent No. 9,462,411 ("411 patent").

48. 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.").

49. 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

IPR of U.S. Patent No. 11,770,756

Decl. of Dr. Kevin Almeroth

NFC transceiver plus biometric finger sensor did not yet exist in a mobile phone at the time of filing of Humbel.” EX1005 at 483.

50. 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.

51. 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.

#### **4. '708 Patent File History**

52. 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.

53. 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.

54. 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.

55. Applicant further argued to distinguish the cited prior art based on the limitation that “the entity is not involved in providing the communications service.”

IPR of U.S. Patent No. 11,770,756

Decl. of Dr. Kevin Almeroth

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.

## **5. ’199 Patent File History**

56. 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.

57. 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.

58. 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

IPR of U.S. Patent No. 11,770,756

Decl. of Dr. Kevin Almeroth

a smartphone that a proximity condition is satisfied between the smartphone and an entity.” EX1007 at 184-85.

59. 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.

60. 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.

## **6. ’015 Patent File History (Unasserted)**

61. 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”, unasserted) 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.

62. The Examiner rejected the claims as obvious four times. EX1008 at 77, 117, 155, 209. Applicant amended the claims and the Examiner provided an amendment before allowance. EX1008 at 92, 136, 188, 258.

63. 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 212-218.

#### **7. ’432 Patent File History**

64. 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.

65. 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.

66. 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

IPR of U.S. Patent No. 11,770,756

Decl. of Dr. Kevin Almeroth

“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.

## **8. '118 Patent File History (Unasserted)**

67. 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.

68. 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.

69. 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.

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

70. 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.

71. 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.

72. 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.

**10. '743 Patent File History**

73. U.S. Patent Application No. 18/489,517 was filed October 18, 2023, and issued as U.S. Patent No. 11,924,743 (“’743 patent”) on March 5, 2024. It is a continuation of above-described pending U.S. Patent Application No. 18/450,517.

74. Applicant made several preliminary amendments. EX1013 at 76, 98. The Examiner required an election of a group of claims, and Applicant elected the group “drawn to a method of establishing a capability at a smartphone to conduct a financial transaction; the method comprising: responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion, selectively establishing a master-slave relationship.” EX1013 at 150.

75. The Examiner rejected the pending claims 1 and 4 for double patenting “over claims 1, 6, 11, 14 of Patent No. 11,770,756.” EX1013 at 243. Applicant submitted a terminal disclaimer for the ’756 Patent. EX1013 at 251.

**11. '793 Patent File History**

76. 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.

77. 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.”

IPR of U.S. Patent No. 11,770,756

Decl. of Dr. Kevin Almeroth

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**

78. 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.

79. 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.

80. In my opinion, a person of ordinary skill in the art at the time of the '756 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.

81. 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**

82. 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.

83. 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.

84. 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**

85. I understand that claims 1-16 are at issue in Petitioner’s petition for *inter partes* review. They are reproduced below for reference.

Claim	Limitation
1[pre]	A method of operating a device, the method comprising:
1[a]	sensing by the device, using a device-based sensor, a parameter that is associated with the device, an environment of the device and/or a user of the device;
1[b]	determining by the device a value of the parameter that is sensed; and
1[c]	responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion, enabling by the device a number of functions of the device and disabling by the device a function of the device;
1[d]	wherein the parameter that is sensed using the device-based sensor, comprises a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state; and
1[e]	wherein the device comprises a smartphone.
2[pre]	The method of claim 1,
2[a]	wherein said enabling by the device a number of functions of the device comprises enabling by the device a number of functions of the device that is greater than or equal to one.

Claim	Limitation
3[pre]	The method of claim 1, further comprising:
3[a]	while said number of functions is enabled by having sensed by the device the parameter and by having determined by the device that the value of the parameter that is sensed satisfies the threshold criterion, requesting by the device from a second device an authorization to enable a function for conducting a financial transaction by the device;
3[b]	responsive to the requesting, receiving by the device from the second device the authorization to enable the function for conducting the financial transaction; and
3[c]	responsive to receiving the authorization, enabling at the device the function for conducting the financial transaction.
4[pre]	The method of claim 3, further comprising:
4[a]	responsive to the device satisfying a proximity condition relative to an entity and responsive to the device sensing the parameter and determining the value that is associated with parameter that is sensed satisfies the threshold criterion, using by the device the function for conducting the financial transaction and conducting by the device the financial transaction by paying for a product.
5[pre]	The method of claim 3, further comprising:
5[a]	enabling at the second device a function for conducting the financial transaction.
6[pre]	A device that is configured to perform operations comprising:
6[a]	sensing by the device, using a device-based sensor, a parameter that is associated with the device, an environment of the device and/or a user of the device;
6[b]	determining by the device a value of the parameter that is sensed; and
6[c]	responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion, enabling by the

Claim	Limitation
	device a number of functions of the device and disabling by the device a function of the device;
6[d]	wherein the parameter that is sensed using the device-based sensor, comprises a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state; and
6[e]	wherein the device comprises a smartphone.
7[pre]	The device of claim 6,
7[a]	wherein said enabling by the device a number of functions of the device comprises enabling by the device a number of functions of the device that is greater than or equal to one.
8[pre]	The device of claim 6, wherein the operations further comprise:
8[a]	while said number of functions is enabled by having sensed the parameter and by having determined by the device that the value of the parameter that is sensed satisfies the threshold criterion, requesting by the device from a second device an authorization to enable a function for conducting a financial transaction by the device;
8[b]	responsive to the requesting, receiving from the second device the authorization to enable the function for conducting the financial transaction; and
8[c]	responsive to receiving the authorization, enabling the function for conducting the financial transaction.
9[pre]	The device of claim 8, wherein the operations further comprise:
9[a]	detecting by the device that a proximity condition has been satisfied between the device and an entity;
9[b]	sensing by the device the parameter and determining by the device the value that is associated with the parameter that is sensed satisfies the threshold criterion; and

Claim	Limitation
9[c]	responsive to the value that is associated with the parameter that is sensed satisfying the threshold criterion, using by the device the function for conducting the financial transaction and conducting by the device the financial transaction by paying for a product.
10[pre]	The device of claim 8, wherein the operations further comprise:
10[a]	causing a function for conducting the financial transaction to be enabled at the second device.
11[pre]	A method of operating a wireless device, the method comprising:
11[a]	sensing by the wireless device, using a sensor of the wireless device, a parameter that is associated with the wireless device, an environment of the wireless device and/or a user of the wireless device;
11[b]	determining by the wireless device a value of the parameter that is sensed and determining by the wireless device whether or not the value that is sensed satisfies a threshold criterion;
11[c]	responsive to the value that is sensed satisfying the threshold criterion, enabling a number of functions of the wireless device and disabling a function of the wireless device;
11[d]	requesting by the wireless device from a second device an authorization to enable a function for conducting a financial transaction;
11[e]	responsive to the requesting, receiving by the wireless device from the second device the authorization to enable the function for conducting the financial transaction;
11[f]	responsive to receiving the authorization, enabling at the wireless device the function for conducting the financial transaction; and
11[g]	responsive to the wireless device satisfying a proximity condition relative to an entity and responsive to the wireless device sensing the parameter and determining that the value sensed satisfies the threshold criterion, using the function for conducting the financial transaction and conducting the financial transaction by paying for a product;

Claim	Limitation
11[h]	wherein the parameter that is sensed, using the sensor of the wireless device, comprises a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state; and
11[i]	wherein the wireless device comprises a smartphone.
12[pre]	The method of claim 11,
12[a]	wherein said enabling a number of functions of the wireless device comprises enabling a number of functions of the wireless device that is greater than or equal to one.
13[pre]	The method of claim 11, further comprising:
13[a]	enabling at the second device a function for conducting the financial transaction.
14[pre]	A wireless device that is configured to perform operations comprising:
14[a]	wherein said transmitting first data to a first device and said receiving second data from the first device comprises wirelessly transmitting/receiving by the smartphone using unlicensed frequencies, licensed frequencies, a WiFi air interface protocol, an Orthogonal Frequency Division Multiplexing air interface protocol and/or an Orthogonal Frequency Division Multiple Access air interface protocol.
14[b]	using a sensor of the wireless device and sensing a parameter that is associated with the wireless device, an environment of the wireless device and/or a user of the wireless device;
14[c]	determining a value that is associated with the parameter that is sensed and determining whether or not the value satisfies a threshold criterion;
14[d]	responsive to the value satisfying the threshold criterion, enabling a number of functions of the wireless device and disabling a function of the wireless device;

<b>Claim</b>	<b>Limitation</b>
14[e]	requesting from a second device an authorization to enable a function for conducting a financial transaction;
14[f]	responsive to the requesting, receiving from the second device the authorization to enable the function for conducting the financial transaction;
14[g]	responsive to receiving the authorization, enabling the function for conducting the financial transaction; and
14[h]	responsive to the wireless device satisfying a proximity condition relative to an entity and responsive to the wireless device sensing the parameter and determining that the value of the parameter sensed satisfies the threshold criterion, using the function for conducting the financial transaction and conducting the financial transaction by paying for a product;
14[i]	wherein the parameter that is sensed comprises a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state; and
14[j]	wherein the wireless device comprises a smartphone.
15[pre]	The wireless device of claim 14,
15[a]	wherein said enabling a number of functions of the wireless device comprises enabling a number of functions of the wireless device that is greater than or equal to one.
16[pre]	The wireless device of claim 14, wherein the operations further comprise:
16[a]	causing a function for conducting the financial transaction to be enabled at the second device.
17[pre]	wherein said selectively sending information to at least one device comprises selectively sending information to the access point

Claim	Limitation
	maintained by the vendor at the point of purchase counter and to at least one other device that is predetermined; and/or
17[a]	establishing by the wireless device a short-range wireless link with the entity;
17[b]	wirelessly transmitting information to the entity using unlicensed frequencies; and
17[c]	wirelessly receiving information from the entity using unlicensed frequencies;
17[d]	wherein said wirelessly transmitting and said wirelessly receiving comprises using a time domain duplex protocol; and
17[e]	wherein said establishing by the wireless device a short-range wireless link with the entity comprises establishing the short-range wireless link with the entity responsive to the wireless device satisfying the proximity condition relative to the entity and responsive to the wireless device sensing the parameter and determining that the value associated therewith satisfies the threshold criterion.
18[pre]	The wireless device of claim 14,
18[a]	wherein said requesting from a second device an authorization to enable a function for conducting a financial transaction and/or said receiving from the second device the authorization to enable the function for conducting the financial transaction comprises:
18[b]	establishing by the wireless device a link with the second device, comprising a wireless link that comprises a distance that is greater than a distance associated with the proximity condition;
18[c]	wirelessly transmitting information to the second device over said wireless link using unlicensed and/or licensed frequencies; and
18[d]	wirelessly receiving information from the second device over said wireless link using unlicensed and/or licensed frequencies;

Claim	Limitation
18[e]	wherein said wirelessly transmitting and/or said wirelessly receiving comprises using an orthogonal frequency division multiplexing and/or orthogonal frequency division multiple access protocol; and
18[f]	wherein said establishing by the wireless device a link with the second device comprises establishing the link with the second device responsive to the wireless device sensing the parameter and determining that the value sensed satisfies the threshold criterion.

#### IV. State of the Art

86. As the '756 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 1:34-55. 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.

87. 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.

88. 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:



89. 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. **EX1023Error! Hyperlink reference not valid.** (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)	1-18

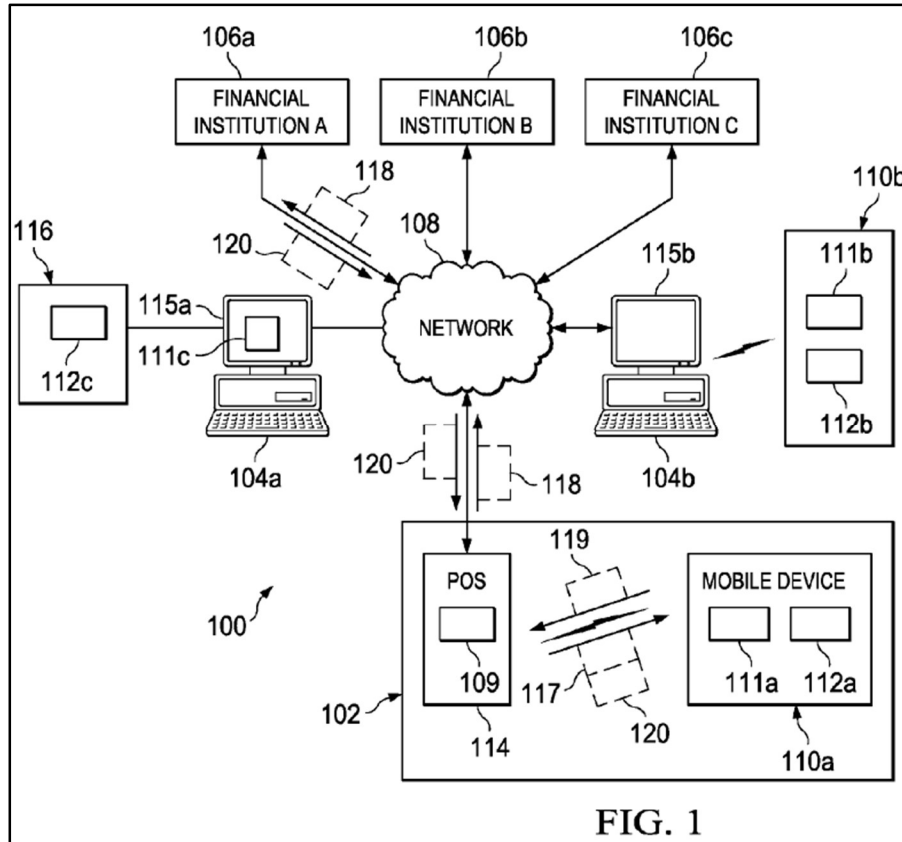
2	§103	Dua (U.S. Pat. Appl. Pub. No. 2006/0165060)	1-18
---	------	---	------

**A. Ground 1: Jain (EX1017)**

**1. Background**

90. 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 '756 Patent under at least pre-AIA 35 U.S.C. § 102(e).

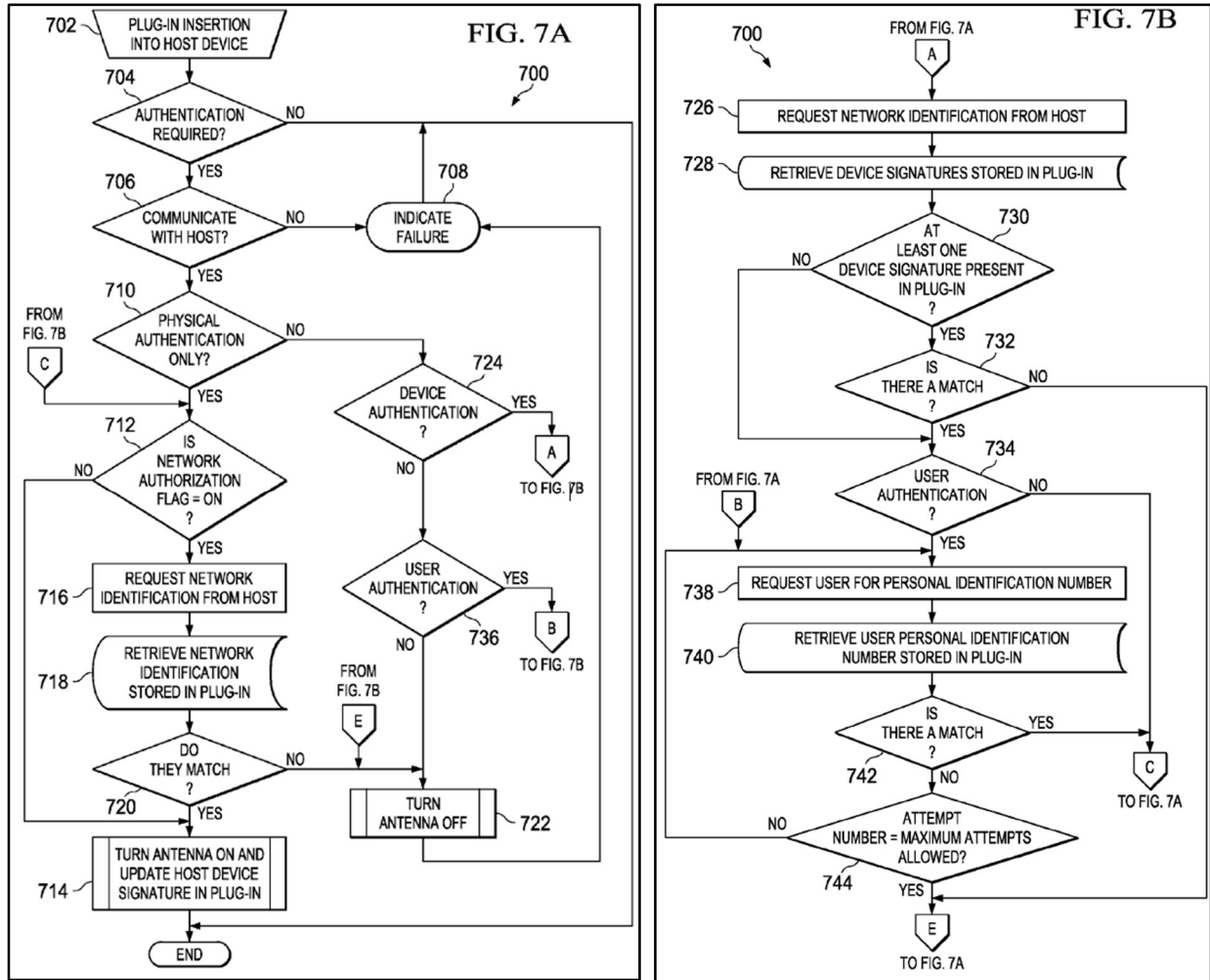
91. Jain describes systems and methods for interfacing intelligent transaction cards with mobile devices, such as smartphones with a Graphical User Interface (GUI), to wirelessly execute financial transactions with retail point-of-sale (POS) terminals. *See* Jain ¶¶[0005], [0018]. The transaction card 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:



92. 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].

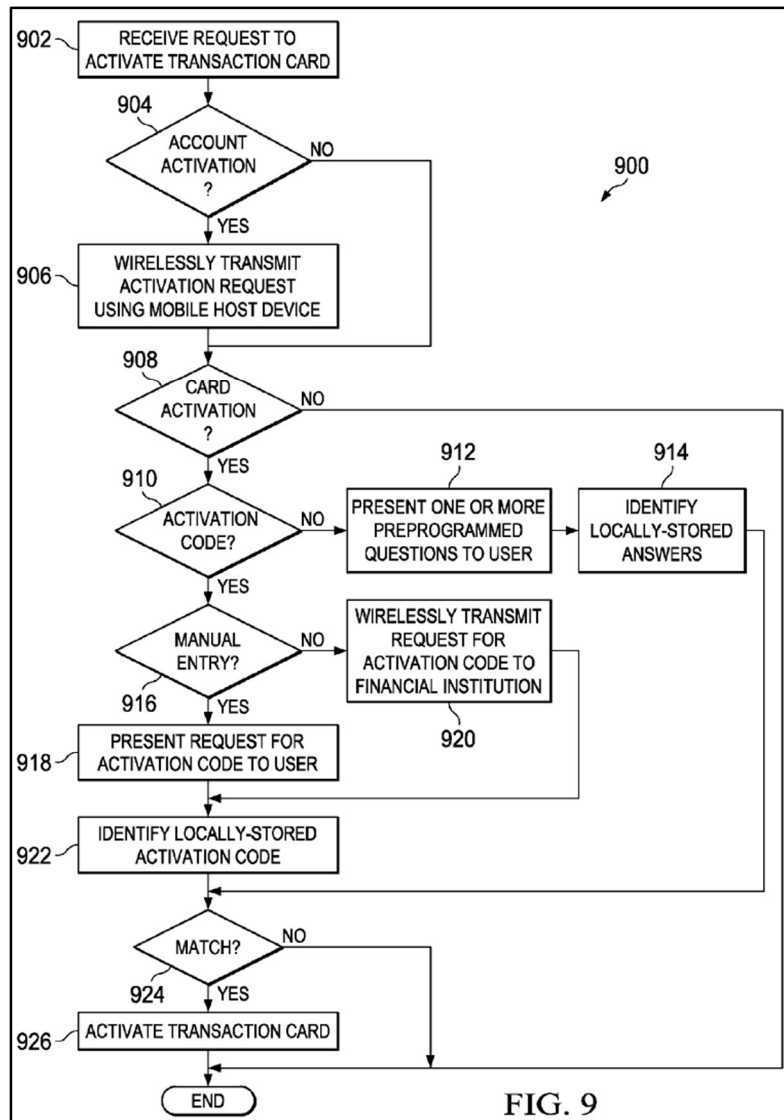
93. The transaction card 112 of the mobile device may first need to be authenticated with the mobile host device as part of an “automatically bootstrapping” operation. FIGS. 7A-7B illustrate those procedures, such as in response to detecting that the transaction card has been inserted into the mobile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



Jain 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].

94. 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].



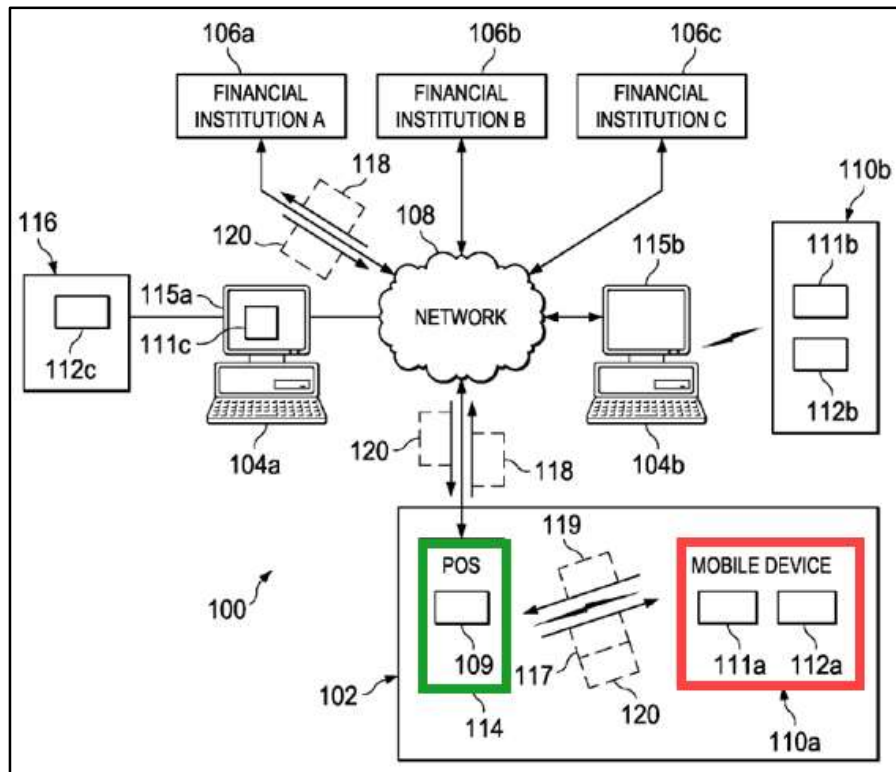
95. To activate the transaction card, the mobile device wirelessly communicates with the financial institution using cellular radio to transmit an activation request at step 906 and activates the transaction card at step 926 in response to a user entering a matching activation code or PIN through the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

**2. Analysis**

**(a) Claim 1**

**(i) 1[pre]: *A method of operating a device, the method comprising:***

96. In my opinion, Jain discloses limitation 1[pre]. Jain describes operating a “mobile device 110.” Jain ¶[0019], FIG. 1. Mobile device 110 can include a “transaction card 112” attached thereto or incorporated therein, where the mobile device and transaction card can “wirelessly execut[e] transactions” with retail point-of-sale terminal 114. See Jain ¶¶[0005], [0018]-[0019], [0021], [0029], FIG. 1:



97. Jain FIG. 1 shows a customer’s mobile device 110a with transaction card 112a and GUI 111a (red box) wirelessly executing transactions with a nearby POS device 114 (green box). See Jain ¶[0019]. The POS device 114 transmits

transaction request 117 to the transaction card, and the mobile device then sends a transaction response 119 that identifies information associated with a payment account. Jain ¶[0027]. Upon receipt of the response, the POS device 114 then sends a transaction authorization request to a financial institution, and the financial institution transmits authorization response 120 to the POS device. Jain ¶[0027]. In turn, the POS device transmits it to the mobile device's transaction card. Jain ¶[0027]. This response includes a payment transaction receipt presentable to the user through the mobile device's GUI. Jain ¶[0027]. The exchange between the mobile device's transaction card and POS device uses short range signals such as NFC or Bluetooth. Jain ¶[0023].

98. Jain interfaces the mobile device with a transaction card that “convert[s] the mobile device ... to a contactless payment device loaded with a financial vehicle ... that may be ... a credit card ... .” Jain ¶[0029]. In such embodiments, the transaction card is included as part of the mobile device. Jain ¶[0019] (“The offline store 102 includes a mobile device [110a<sup>1</sup>] having a transaction card 112a and a Point of Sale (POS) device 114 that executes transactions

---

<sup>1</sup> The reference to “10a” in the specification is an obvious typographic error. No figures show a “10a.” Jain's FIG. 1 clearly shows element 110a, matching the description of “10a” in the specification.

with customers.”), FIG. 1 (showing transaction card 112a within mobile device 110a).

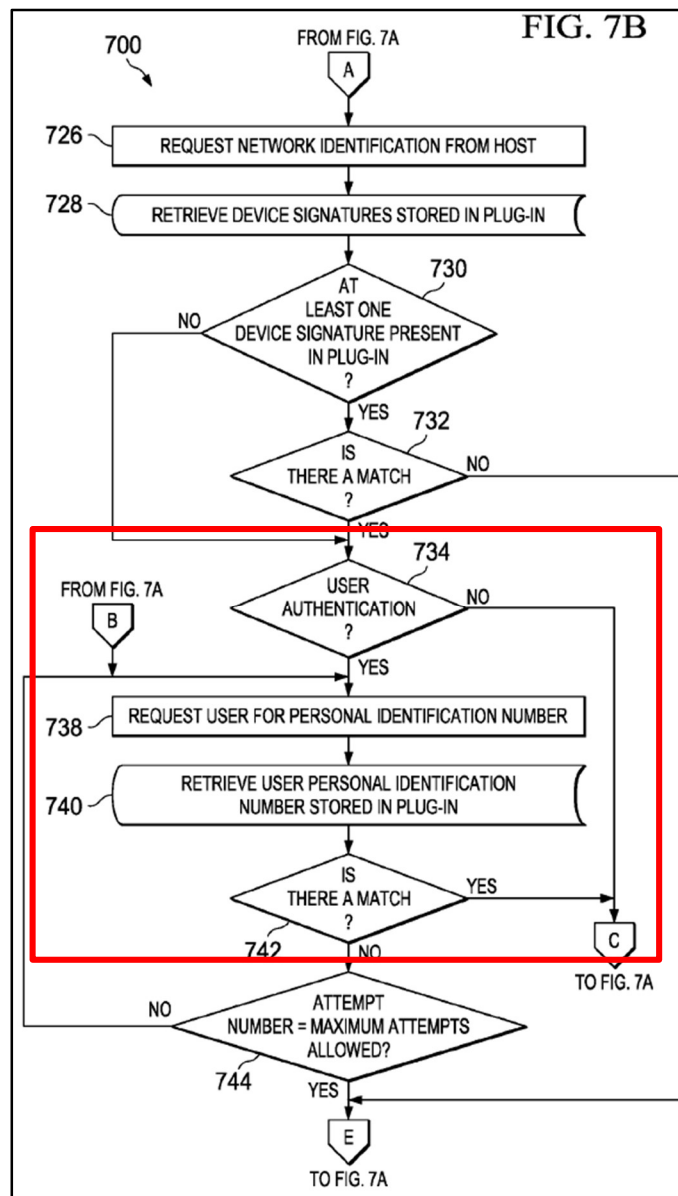
99. To the extent Patent Owner argues Jain’s transaction card cannot be considered part of the mobile device, in my opinion, a POSITA would find it obvious to implement the processes discussed herein with transaction card 112 integrated into mobile device 110. A POSITA would be motivated to integrate the transaction card into the mobile device because integration achieves the benefits disclosed in Jain, but a separate, independent transaction card does not need to be implemented. Instead, the transaction card can leverage the components of the mobile device, such as memory, battery, and processing power.

100. Further, separability of the transaction card is not always advantageous. For instance, a smartphone vendor might find it commercially advantageous to provide transaction card functionality with their smartphone, but not allow users to leverage that functionality with other devices. Separability also risks inadvertent loss. But if the transaction card is incorporated into the mobile device, the transaction card cannot become detached and lost.

(ii) **1[a]:** *sensing by the device, using a device-based sensor, a parameter that is associated with the device, an environment of the device and/or a user of the device;*

**1[b]:** *determining by the device a value of the parameter that is sensed; and*

101. In my opinion, Jain discloses limitations 1[a]-[b]. Jain discloses authenticating a user using a PIN number or biometrics (e.g., fingerprint) (i.e., “*a parameter that is associated with ... a user of the device*”), as part of its authentication process for “automatically bootstrapping” transaction card 112 to mobile device 110. See Jain ¶¶[0072], [0075], FIG. 7B:



IPR of U.S. Patent No. 11,770,756

Decl. of Dr. Kevin Almeroth

Specifically, at step 738, the smartphone receives a PIN from the user. Jain ¶¶[0022], [0075]. At step 740, the smartphone retrieves a locally stored PIN. Jain ¶[0075]. Then, at step 742, the smartphone determines whether the PINs match. Jain ¶[0075], FIG. 7B.

102. Jain contemplates that “the user may be authenticated using ... biometric information (e.g., fingerprint)” (i.e., “*parameter that is associated with ... a user of the device*”) rather than “entering a PIN.” Jain ¶[0075]. Thus, steps 738, 740, and 742 are performed with biometric verification. In other words, this includes scanning a fingerprint (i.e., “*sensing by the device, using a device-based sensor*”), extracting a set of features representing the fingerprint (i.e., “*determining ... a value of the parameter that is sensed*”), retrieving locally-stored fingerprint data of the rightful owner, and comparing the two sets of fingerprint data (i.e., “*satisfying a threshold criterion*” for limitation 1[c]). At a minimum, this parameter-data comparison requires assigning values to the parameter.

103. Indeed, Patent Owner makes the same mapping in its infringement contentions. Patent Owner’s infringement contentions allege that the use of biometric verification is sufficient to show “*sensing*,” “*determining*,” and “*threshold criterion*.” EX1016 at 5-20.

104. At a minimum, a POSITA would be find it obvious to implement Jain’s teaching of “authentication using ... biometric information” in this manner. Such

implementations are well known in the art at the time. *See, e.g.*, EX1021 ¶¶[0040]-[0042]; EX1024 ¶¶[0009], [0025]; EX1025 ¶¶[0044], [0086]-[0092]; EX1026 at 196. For instance, EX1024 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]. Biometric authentication is to ensure biometric information of a user matches that of the rightful owner. The rightful owner’s biometric information must be stored during device setup, and then used to compare against a current user’s biometric information. To pass, the two must correlate to provide adequate confidence that the current user is the device’s owner.

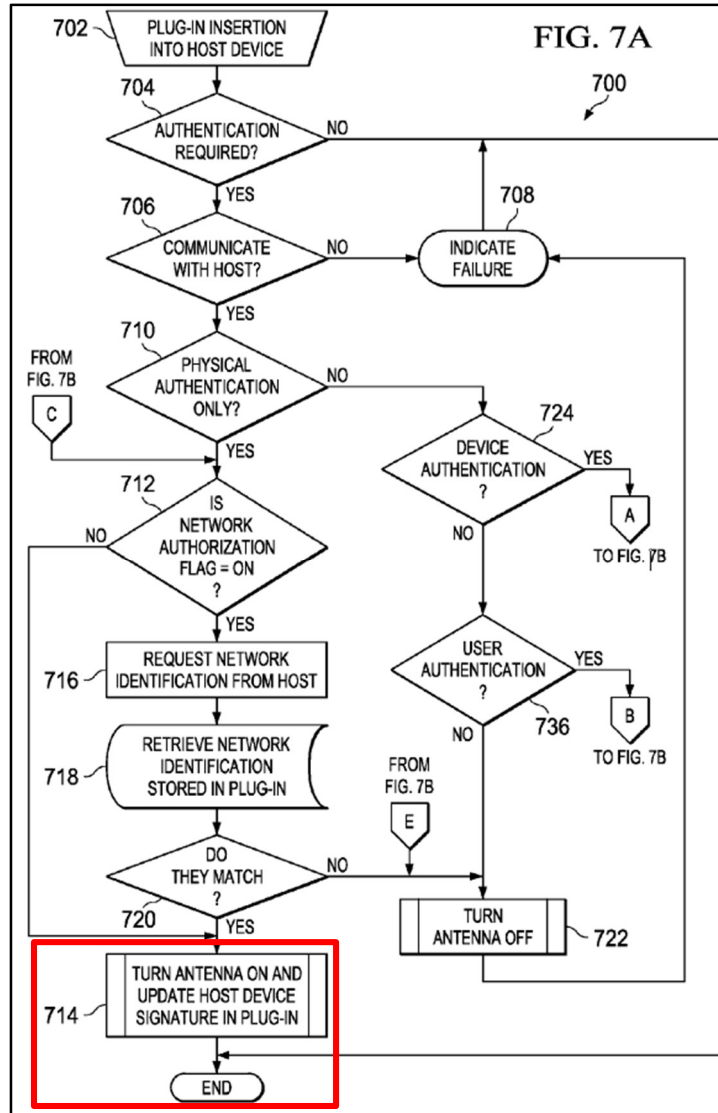
- (iii) 1[c]: *responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion, enabling by the*

***device a number of functions of the device and disabling by the device a function of the device;***

105. In my opinion, Jain discloses limitation 1[c]. This limitation recites (1) determining if the “***parameter ... satisf[ies] a threshold criterion,***” and (2) if it does, (a) “***enabling by the device a number of functions,***” where the “***number of functions***” could be just one (see limitation 2[a] (specifying “***the number of functions***” is “***greater than or equal to one***”).), and (b) “***disabling by the device a function.***” Jain discloses all of those requirements.

106. First, as with limitations 1[a]-[b], Jain discloses an authentication process with fingerprint authentication (*i.e.*, “***value that is determined ... for the parameter***”) for “automatically bootstrapping” transaction card 112 to mobile device 110. And part of the authentication process is step 742 or at least an obvious variation thereof, where the scanned fingerprint data would be compared to the locally-stored fingerprint data associated with the rightful owner to determine if they are sufficiently close (*i.e.*, “***satisfying a threshold criteria***”). See limitations 1[a]-[b].

107. Second, in response to user authentication (in steps 738-744 of FIG. 7B) (*i.e.*, “***responsive to satisfying a threshold criterion***”), Jain process 700 returns to step 712 (see label C in both figures) and proceeds to step 714: “turn antenna on and update host device signature in plug-in” (*i.e.*, “***enabling by the device a number of functions of the device***”). See Jain ¶¶[0072]-[0075], FIG. 7A.



108. Specifically, if the host-device signature is updated (as described in FIG. 7) to match the host device, the transaction card completes the bootstrap operation and can communicate with the host; otherwise, the “host device is rejected, bootstrap is aborted and the card 400 is returned to the mode it was before being inserted into the device.” Jain ¶[0065]. Only after bootstrapping/authentication (FIG. 7) is complete can activation (FIG. 9) begin, where activation includes communicating with a financial institution “using cellular radio technology of the

host device.” Jain ¶¶[0065], [0072] (“an intelligent card may execute one or more authentication procedures prior to activation.”), [0081]. Thus, successful authentication as part of “automatically bootstrapping” (Jain ¶[0072].) enables cellular radio technology required to communicate, and thereby activate the transaction card, with a financial institution (*i.e.*, “***number of functions of the device***”).

109. As for “***disabling by the device a function of the device***,” Jain discloses this part of the claim under two theories:

110. **First Theory for Enabling/Disabling Limitation:** While the mobile device is enabled to use cellular radio technology communicate with a financial institution to perform the activation process (*i.e.*, “***enabling by the device a number of functions***”), payment transactions are disabled (*i.e.*, “***disabling by the device a function of the device***”) because the transaction card is not yet activated. Jain ¶[0081]. Only once bootstrapping/authentication (Jain FIG. 7) is complete can activation (Jain FIG. 9) begin, which includes communicating with a financial institution “using cellular radio technology of the host device.” Jain ¶¶[0065], [0072], [0081]. Otherwise, the transaction card lacks access to the host-device’s cellular radio technology, because it lacked access to this cellular radio technology “before being inserted into the device.” Jain ¶[0065].

111. Performing successful authentication also causes disabling fraud control processes related to authentication (*i.e.*, “***disabling by the device a function of the device***”). A “fraud control process” includes “determin[ing] a violation of one or more rules.” Jain ¶[0026]. The bootstrapping/authentication “method 700 may be implemented as a fraud control process ... .” Jain ¶[0075]. Once the bootstrapping/authentication process is done (*e.g.*, reaching the “END” step after performing authentication and turning on the antenna), the mobile device no longer monitors for violations of one or more rules associated with bootstrapping/authentication. *See* Jain FIG. 7A. For instance, step 744 of bootstrapping/authentication counts the number of invalid PINs or fingerprints provided during authentication. “If the number of [PIN-entry] attempts has exceed[ed] ... [a] threshold, then the antenna is deactivated ... .” Jain ¶[0075]. Monitoring for violation of the maximum threshold is no longer performed after providing a valid PIN or fingerprint.

112. **Second Theory for Enabling/Disabling Limitation:** Jain meets this limitation by “***enabling a number of functions of the smartphone***” (turning its antenna on and enabling cellular communications when the user is authenticated) and “***disabling a function of the smartphone***” (mode before transaction card was inserted into the device). Patent Owner asserted in its infringement contentions that this limitation is met by “enabling a number of functions of the smartphone, such as

unlocking the smartphone or an application, and disabling a function of the smartphone, such as disabling the lock function.” EX1016 at 20. Similarly, Jain’s bootstrapping/authorization process (FIG. 7) must be fully completed prior to turning on the antenna and updating the host device signature to enable cellular communication (step 714), and conversely, the “host device is rejected, bootstrap is aborted and the card 400 is returned to the mode it was before being inserted into the device” if that bootstrapping/authorization process was unsuccessful. Jain ¶[0065].

- (iv) **1[d]:** *wherein the parameter that is sensed using the device-based sensor, comprises a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state; and*

113. In my opinion, Jain discloses limitation 1[d]. As discussed with limitations 1[a]-[b], Jain discloses authenticating a user using a fingerprint (*i.e.*, “*physiological state*”). See Jain ¶[0075]; *see also* EX1016 at 28.

- (v) **1[e]:** *wherein the device comprises a smartphone.*

114. In my opinion, Jain discloses limitation 1[e]. Jain’s “mobile device 110” can be a “*smartphone*.” See Jain ¶[0018], [0021].

**(b) Claim 2**

- (i) **2[pre]:** *The method of claim 1,*

115. As addressed in Section V.A.2.a, it is my opinion that Jain discloses limitation 2[pre].

- (ii) **2[a]:** *wherein said enabling by the device a number of functions of the device comprises enabling by the device a number of functions of the device that is greater than or equal to one.*

116. In my opinion, Jain discloses limitation 2[a]. As discussed with limitation 1[c], Jain discloses enabling one or more (*a number ... that is greater than or equal to one*) functions.

(c) **Claim 3**

- (i) **3[pre]:** *The method of claim 1, further comprising:*

117. As addressed in Section V.A.2.a, it is my opinion that Jain discloses limitation 3[pre].

- (ii) **3[a]:** *while said number of functions is enabled by having sensed by the device the parameter and by having determined by the device that the value of the parameter that is sensed satisfies the threshold criterion, requesting by the device from a second device an authorization to enable a function for conducting a financial transaction by the device;*  
**3[b]:** *responsive to the requesting, receiving by the device from the second device the authorization to enable the function for conducting the financial transaction; and*

118. After “*enabling ... functions*” as discussed with limitation 1[c], Claim 3 identifies additional steps. It is my opinion that Jain discloses these steps recited in limitations 3[a]-[c].

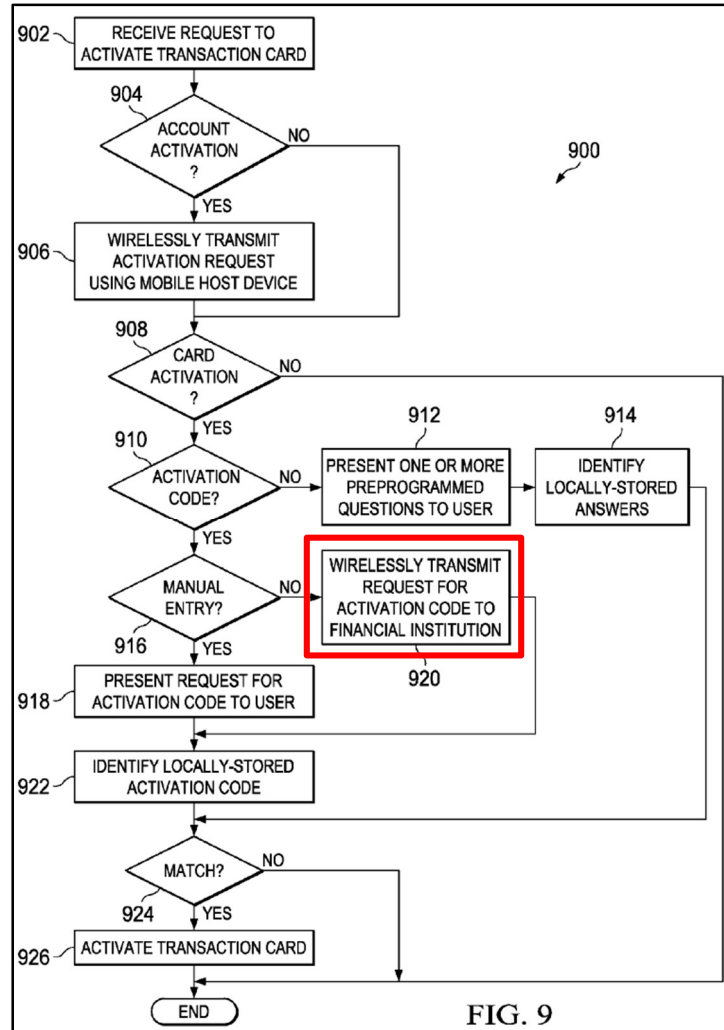
119. The first of these additional steps is “*requesting by the device from a second device an authorization to enable a function for conducting a financial transaction by the device.*”

120. Jain’s smartphone performs “method 900 for activating a wireless transaction system” with the financial institution, after authenticating the user and enabling the mobile device to use cellular technology. Jain ¶[0080]. During step 920 of this method, the transaction card, via the smartphone, “wirelessly transmits a request for the activation code using the cellular... technology” to the financial institution<sup>2</sup> (*i.e.*, “*requesting by the device from a second device authorization*”).

Jain ¶[0081], FIG. 9:

---

<sup>2</sup> Jain uses the term “financial institution” to refer to devices. In particular, “financial institution” refers to an enterprise’s devices that authorize transactions through network 108 by accepting data from clients and returning responses using. Jain ¶¶[0038], [0039].



121. In response to the request of step 920, mobile device 110 “*receiv[es]*” an activation code (*i.e.*, “*authorization*”) from the financial institution (*i.e.*, “*second device*”). The received activation code is then checked against a stored activation code (retrieved at step 922). Jain ¶[0081]. If the codes match, “the transaction card is activated” at step 926. Jain ¶[0081]. This “activation process may include activating the transaction card and/or financial account.” Jain ¶[0026]. The transaction card can then perform payments with the associated financial account by “signifying activation of the financial vehicle carried on the card.” Jain ¶[0071].

122. Thus, steps 920 and 924 are performed in order to “activat[e] the transaction card and/or financial account.” A matching “activation code” is an “*authorization*” to engage in financial transactions. The “activation code” is required to enable transactions with that card (*i.e.*, “*function for conducting a financial transaction*”), and the receipt of an activation code matching a stored activation code is the last step before the card is activated in step 926. *See* Jain FIG. 9. Requesting and receiving the activation code are thus “*requesting*” and “*receiving ... the authorization.*” *See* Jain FIG. 9. This tracks the assertions in Patent Owner’s infringement contentions, asserting that adding a credit card is sufficient to establish “*requesting authorization*” and “*receiving... authorization to enable the function for conducting the financial transaction.*” EX1016 42-55.

123. In my opinion, a POSITA would also understand that the smartphone receives an “*authorization*” by receiving an activation code from the financial institution. A POSITA would find it obvious that the financial institution would not provide a valid activation code to a smartphone that is not authorized to perform payment services with the financial institution. That is supported by steps 924, which compares the activation code received by the financial institution with a locally stored activation code from step 922 to determine “[i]f the locally stored information matches the provided” activation code. Jain ¶[0081]; FIG. 9. Further, because the activation code is not only the result of authenticating a user to engage

in financial transaction, but also causes activation of a transaction card for financial transactions, the activation code constitutes “*authorization.*” Indeed, Patent Owner asserts similar reasoning in its infringement contentions, where receiving an issued credit card authorized to conduct financial transactions, like receiving a code to activate a transaction card, is sufficient to establish “*receiving ... authorization.*” EX1016 at 42.

124. At a minimum, a POSITA would find such implementation well known, thereby rendering it obvious. Several references describe similar processes. *See, e.g.*, EX1019 ¶¶[0145]-[0146] (describing “verification process” whereby “transmitted to the corresponding credit card provider” so the provider can confirm the information is “valid” and “confirm the identify [sic] of the user by transmitting one or more verification codes” to the user device, thereby “ensur[ing] that only the authorized user or users will receive the verification code”). A POSITA would be motivated to treat Jain’s matching activation code as an authorization (and not provide the same if the transaction card is unauthorized) in order to improve system security and guard financial institutions against fraudulent transaction cards. For instance, if Jain’s system returned a matching activation code every time, including in response to requests from fraudulent transaction cards, there would be no reason to implement steps 920-924 of Jain’s process 900.

- (iii) **3[c]: *responsive to receiving the authorization, enabling at the device the function for conducting the financial transaction.***

125. In my opinion, Jain discloses limitation 3[c]. “[**R**]*esponsive to receiving the authorization*” discussed with limitation 3[b], Jain discloses that the mobile device with the transaction card checks that the received activation code matches the stored activation code. Jain ¶[0081]. Upon finding a match, the transaction card is activated at step 926, allowing the smartphone and transaction card to engage in financial transactions (*i.e.*, “*enabling at the device the function for conducting the financial transaction*”). See Jain ¶¶[0071], [0081], FIG. 9.

**(d) Claim 4**

- (i) **4[pre]: *The method of claim 3, further comprising:***

126. As addressed in Section V.A.2.c, it is my opinion that Jain discloses limitation 4[pre].

- (ii) **4[a]: *responsive to the device satisfying a proximity condition relative to an entity and responsive to the device sensing the parameter and determining the value that is associated with parameter that is sensed satisfies the threshold criterion, using by the device the function for conducting the financial transaction and conducting by the device the financial transaction by paying for a product.***

127. In my opinion, Jain discloses limitation 4[a]. Claim 4 builds on claim 3, and claim 3 builds on claim 1. Claim 1 recites steps for “*enabling ... functions.*”

IPR of U.S. Patent No. 11,770,756

Decl. of Dr. Kevin Almeroth

Claim 3 adds steps for using those enabled for enabling a “*function for conducting a financial transaction.*” Claim 4 further recites steps for engaging in a financial transaction. The added steps include requires two prerequisites: (1) “*satisfying a proximity condition relative to an entity*” and (2) “*sensing the parameter... satisf[ying] the threshold criterion.*” These are the prerequisites for *paying for a product.*

128. For the first prerequisite—“*satisfying a proximity condition*”—Jain’s smartphone and transaction card determine proximity with a POS terminal through use short range signals, such as NFC or “proximity signals,” prior to executing a transaction. *See* Jain ¶[0023]. The smartphone first “wirelessly receive[s] a request from the POS device 114 to execute a transaction and/or provide a response.” Jain ¶[0023]. A POSITA would understand that processing the “request” is only possible if Jain’s mobile device 110 is sufficiently close to POS device 114 to actually receive and decode the requests short-range signal (*i.e.*, “*responsive to the device satisfying a proximity condition*”). EX1034 at 11-12; *see also* EX1036 at 220. Jain’s NFC and other short range wireless communication protocols are only effective when sufficient signal strength is detected. Sufficient signal strength is the detected strength that allows the mobile device and POS terminal can communicate using a short-range wireless communication protocol. EX1035 at 4, 36; EX1037 at 3. That signal strength rapidly deteriorates as distance increase. EX1035 at 4, 36; EX1037

at 3. Jain recognizes that NFC requires proximity of “10 cm or less.” Jain ¶¶[0030].

For Jain’s mobile device to receive and process a request over NFC, the mobile device and POS device must be sufficiently close. A POSITA would understand that this corresponds to *satisfying a proximity condition*.

129. Further, Jain’s use of the NFC also allows for “*satisfying a proximity condition*” earlier in the exchange. Jain’s NFC “wireless connection” is based on the “ISO 18092/ECMA 340” standards. Jain ¶¶[0018], [0023], [0051]. The ECMA 340 Interface and Protocol Standard for NFC<sup>3</sup> explains that an NFC “transaction” requires an “initialization” and then a “data exchange.” EX1034 §§4.25, 10-12, FIG.

---

<sup>3</sup> ECMA 340 is a well-known communications standard that defined NFC communication. This standard was publicly available and known to a POSITA even at the time of Jain’s filing, which in turn predates the earliest priority date of the challenged patent. Included herewith as Exhibit XXX is a true and correct copy of the The 2nd edition of the ECMA 340 Interface and Protocol Standard for NFC (“ECMA-340”), which was publicly available as of released in December 2004 and not updated again until June 2013. <https://ecma-international.org/publications-and-standards/standards/ecma-340/>. This version was also published as the “ISO 18092.” Id. In addition, the same disclosure of ECMA-340 discussed below is found in both the 1st edition (released December 2002) and the 2nd edition.

5. The standard specifies two devices (“Initiator” and “Target”) and two communication modes (“Passive” and “Active”). EX1034 §§1, 4.1, 4.16, 7. It does not matter whether Jain’s POS device or mobile device is the “Initiator,” with the other being the “Target,” or what communication mode they use: every combination results in Jain’s mobile device “*satisfying a proximity condition*” and subsequently establishing a connection for 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.” EX1034 § 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). *See* EX1034 §§ 11.2.1.16-17, 11.2.1.23, 11.3.2, 12.2-.3, FIGS. 13, 24-25. Thus, regardless of what mode is being used and which device in Jain is the Initiator and which device is the Target, the Target device detects a sufficiently strong field from the Initiator (*i.e.*, “*satisfying a proximity condition*”), and the Initiator device detects that a Target is within its field by receiving a response to a command from the Target (*i.e.*, “*satisfying a proximity condition*”). In addition, this exchange of commands and responses results in the selection of a particular “Target” and attributes/parameters for further communication with the same, thereby establishing a “*short-range link*.” EX1034 §§7, 11.2.1.24-25, 12, 12.1, FIGS. 22, 24-25. After this “*link*” is established, the Initiator and the Target communicate using ECMA 340’s data

exchange protocol. EX1034 Figures 5, 23, and 24. This includes transmission of Jain's transaction request 117, transaction response 119, and authorization response 120.

130. Indeed, Patent Owner's infringement contentions confirm this. Patent Owner's infringement contentions assert his limitation is met, Patent Owner alleges in its infringement contentions in district court litigation that NFC shows "*the device satisfying a proximity condition.*" EX1016 at 29-42.

131. A POSITA would also find it obvious that Jain's smartphone would detect proximity to the POS device (*i.e.*, "*satisfying a proximity condition*") based on a signal from the POS device (*e.g.*, a "request," Jain ¶[0023], or earlier commands and responses exchanged as part of implementing ECMA 340) prior to communicating with that POS device. To ensure communications would be successful and not wasted signaling, and further to avoid the security risk of indiscriminately transmitting sensitive financial information, Jain's smartphone first needs to detect it is near the POS device prior to proceeding with a payment transaction with the POS device. Otherwise, the NFC communication would fail. Indeed, such implementations were well-known to a POSITA. For example, EX1020 discloses and leverages NFC to limit the range at which communication may take place. EX1020 ¶¶[0041], [0063]. Indeed, in the context of Wi-Fi, EX1020 even more explicitly discloses using the ability to receive such signals as an

indication of proximity. Jain ¶[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.”). A POSITA would be motivated and able to use Jain’s “request” or ECMA 340’s commands and responses in the same manner.

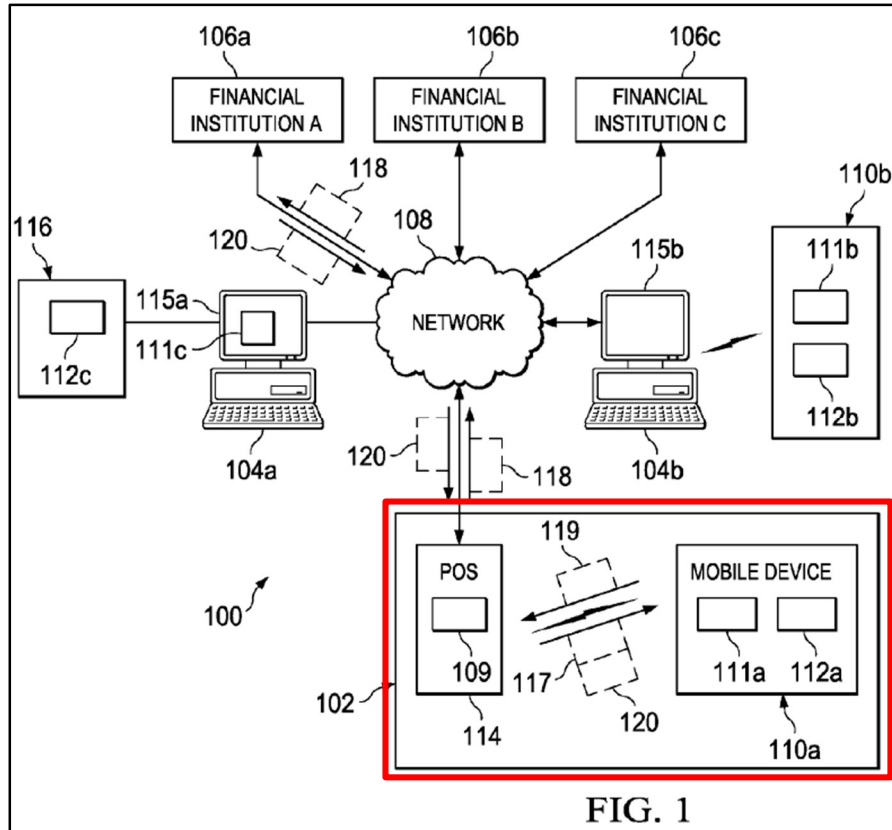
132. According to Patent Owner, limitation 4[a]’s “*determining the ... parameter ... satisfies the threshold criterion*” does not impose any new requirement relative to limitations 1[a]-[b]. Patent Owner’s infringement contentions allege that the same sensing of “*the*” at least parameter and determining it meets “*the*” criterion prior to establishing the function to conduct the financial transaction is also a prerequisite to then “*using*” that function. Compare EX1016 at 6-19 with EX1016 at 46-55 (pointing to the same “fingerprint unlock” and similar security functionality for both limitations).

133. Even if the claims require an additional transaction-specific “*determining*,” Jain discloses or renders this limitation obvious. For example, Jain discloses that during payment, the merchant terminal may “prompt the user to authorize a transaction such as by” fingerprint. Jain ¶¶[0029], [0075]. This request is presented, and user information is received, via GUI 111 of mobile device 110. Jain ¶¶[0023]-[0025]. Authorization via PIN involves or at least obviously involves the authentication process of Jain ¶[0075], as discussed with limitations 1[a]-[c]. At a minimum, a POSITA would find that using the previously disclosed authentication

process to be a simple and natural, and thus obvious, way of implementing PIN authorization: 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.

134. Using biometrics instead of a PIN for authenticating or otherwise authorizing individual transactions is also rendered obvious (*i.e.*, “**determining the value that is associated with parameter that is sensed satisfies the threshold criterion**”). Jain already contemplates using biometrics (*e.g.*, fingerprints) for its user authentication process (Jain ¶[0075], FIG. 7.), and reusing that software and hardware for individual transactions would not further complicate the system or incur material additional costs.

135. To “**pay[] for a product,**” Jain’s smartphone with the transaction card performs a contactless payment transaction by transacting with a nearby retail POS terminal 114. *See* Jain ¶¶[0019], [0023], [0029]; *see also* FIG. 1:



136. The smartphone with the transaction card uses NFC to transact with the POS terminal (*i.e.*, “**using by the device the function for conducting the financial transaction**”). Therefore, the transaction is “**responsive to the**” smartphone with the transaction card being within “**proximity relative to**” the POS terminal, and is “**responsive to**” user authentication with the bootstrapping process or with the transaction (*i.e.*, “**parameter... satisf[ying] the threshold criterion**”), both of which are discussed above. See Jain ¶[0023].

(e) **Claim 5**

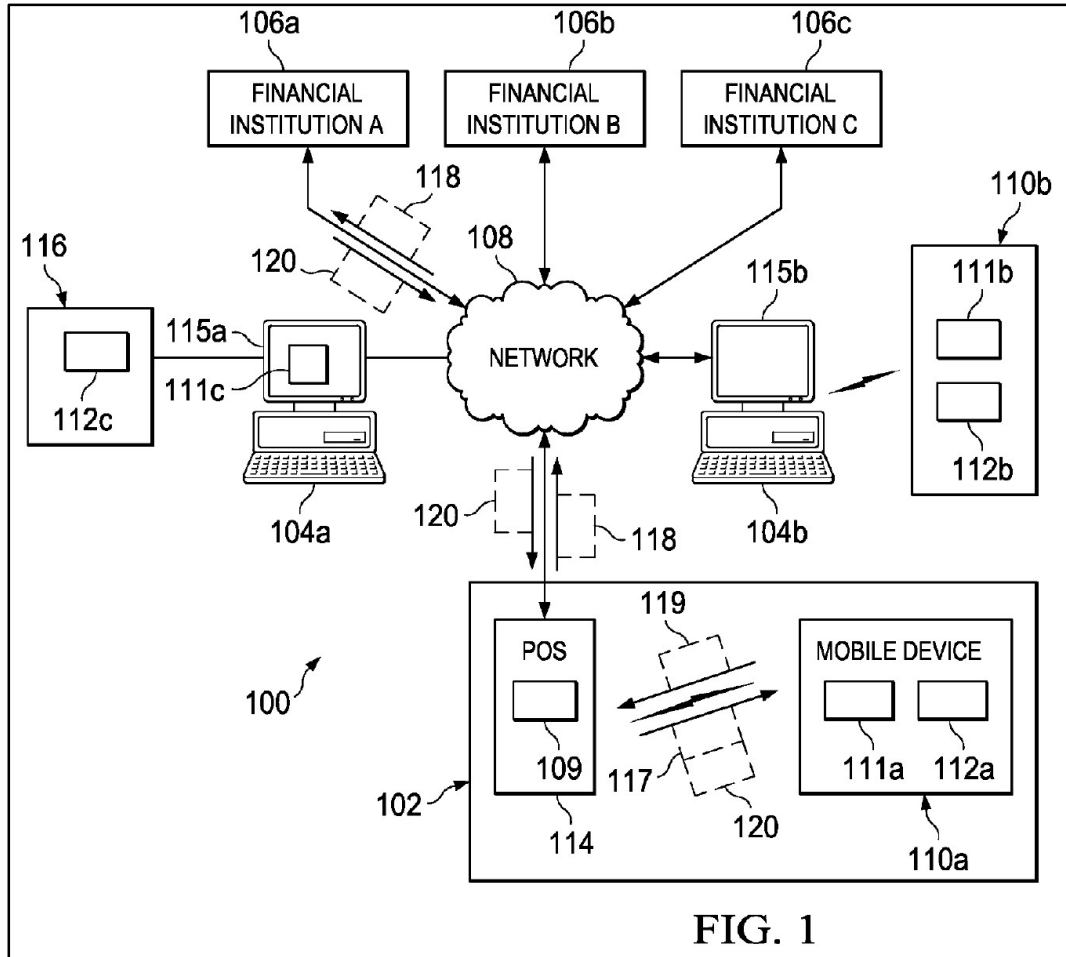
(i) **5[pre]:** *The method of claim 3, further comprising:*

137. As addressed in Section V.A.2.c, it is my opinion that Jain discloses limitation 5

```
[pre].
```

**(ii) 5[a]: *enabling at the second device a function for conducting the financial transaction.***

138. In my opinion, Jain discloses limitation 5[a]. Jain's smartphone conducts transactions by wirelessly communicating with a POS terminal. Jain Abstract. But the conducting a transaction includes an additional step. The POS terminal further sends transaction requests to a financial institution (*second device*) for authorization (*enabl[ed] ... function for conducting the financial transaction*). See Jain ¶¶[0019], [0027], FIG. 1:



For instance, “the POS device 114 may transmit a request 118 to authorize a transaction to the financial institution 106.” Jain ¶[0027]. “The financial institution 106 may authorize the transaction based... on information transmitted by the transaction card 112,” and may transmit an authorization response 120 to the POS device 114. Jain ¶¶[0019],[0027].

139. Jain discloses that the financial institution’s authorization checks whether the transaction card and mobile device used in the transaction is authenticated and activated. See Jain ¶[0026]. Specifically, Jain’s

bootstrapping/authentication process is a fraud control process, where, if the process is failed, the mobile device “may execute one or more processes to ... notify financial institutions of fraudulent activity,” and “block ... the transaction card.” Jain ¶¶[0026], [0075]. Therefore, the financial institution must check whether a transaction is conducted by a blocked mobile device and transaction card (*i.e.*, “***function for conducting the financial transaction***”). Jain ¶[0026]. This is an authorization function that is specific to the transaction card and mobile device, and must be turned on at the financial institution (*i.e.*, “***enabling at the second device function for conducting the financial transaction***”).

**(f) Claims 6-16**

140. In my opinion, claims 6-16 are substantively identical to claims 1-5. Claims 6-10 are directed to “[a] device that is configured to perform operations,” whereas claims 1-5 are directed to “[a] method of operating a device.” This distinction is immaterial since Jain discloses both methods and systems. Jain Title.

141. In my opinion, independent claims 11 and 14 is substantively identical to independent claim 1 incorporated with dependent claims 3 and 4. And dependent claims 12-13 and 15-16 are substantively identical to dependent claims 2 and 5. Claims 11-13 are directed to “[a] method of operating a wireless device,” and claims 14-16 are directed to “[a] wireless device that is configured to perform operations,” whereas claims 1-5 are directed to “[a] method of operating a device.” These

distinctions are immaterial since Jain is directed to a wireless “mobile device,” such as “smartphone,” and discloses both methods and systems. *E.g.*, Jain Title, Abstract, ¶[0018].

**(g) Claim 17**

**(i) 17[pre]: *The wireless device of claim 14, wherein said conducting the financial transaction by paying for a product comprises:***

142. As addressed in Sections V.A.2.a and V.A.2.c-d, it is my opinion that Jain discloses limitation 17[pre].

**(ii) 17[a]: *establishing by the wireless device a short-range wireless link with the entity;***

143. In my opinion, Jain discloses limitation 17[a]. Jain discloses performing transactions between the mobile device with the transaction card and a nearby retail POS terminal 114 (*i.e.*, “**entity**”) by using a “wireless connection (*e.g.*, NFC ...)” (*i.e.*, ***a short-range wireless link***) to send requests and responses between one another. *See* Jain ¶¶[0018]-[0019], [0023], [0027], [0029], [0051], [0054]. Jain implements the ECMA 340 standard. As addressed in more detail with limitation 4[a], an “Initiator” device and a “Target” device exchange communications to select a particular “Target” and attributes/parameters for further communication (*i.e.*, “***establishing ... a short-range wireless link***”).

144. Patent Owner agrees that the use of NFC is sufficient here. Patent Owner's infringement contentions allege the use of NFC as sufficient to show "*establishing ... a short-range wireless link.*" EX1016 at 309-10.

(iii) 17[b]: *wirelessly transmitting information to the entity using unlicensed frequencies; and*

17[c]: *wirelessly receiving information from the entity using unlicensed frequencies;*

17[d]: *wherein said wirelessly transmitting and said wirelessly receiving comprises using a time domain duplex protocol; and*

145. In my opinion, Jain discloses limitations 17[b]-[d]. Jain's mobile device with the transaction card transmit information to the POS device (*i.e.*, "*entity*") "using short range signals such as NFC (*e.g.*, ISO 18092/ECMA 340), ... proximity signals, and/or other signals compatible with retail payment terminals (*e.g.*, POS 114)" (*i.e.*, "*wirelessly transmitting information*"). Jain ¶[0023]. The transmitted information relates to transaction execution and authentication to the POS terminal. Jain ¶¶[0019], [0027]. The POS terminal responds by transmitting back to the wireless device "receipts of the transaction" (*i.e.*, "*wirelessly receiving information from the entity*"). Jain ¶¶[0019], [0027]. These transmissions are done with protocols including NFC and Bluetooth. Jain ¶[0023].

146. NFC uses unlicensed frequencies. Frequencies labeled as ISM—industrial, scientific, and medical—are "*unlicensed.*" NFC operates at 13.56MHz. EX1031. The frequency of 13.56MHz is an ISM frequency. EX1032 at 2.

147. Indeed, Patent Owner agrees. In its Infringement Contentions, Patent Owner alleges that “NFC operates at the globally unlicensed 13.56 MHz frequency.” EX1016 at 313.

148. Similarly, Bluetooth also uses unlicensed frequencies. Specifically, “Bluetooth technology operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHz.” EX1041.

149. Further, “NFC systems can take place as [a] half ... duplex system” (*i.e.*, “*time domain duplex protocol*”). EX1032 at 21. Patent Owner agrees with this mapping: “NFC, a short-range half duplex communication technology,” uses “*time domain duplex protocol*.” EX1016 at 316.

150. Bluetooth is also a “*time domain duplex protocol*.” Not unlike NFC, Bluetooth can operate on half-duplex. *See* EX1038 at 1.

(iv) 17[e]: *wherein said establishing by the wireless device a short-range wireless link with the entity comprises establishing the short-range wireless link with the entity responsive to the wireless device satisfying the proximity condition relative to the entity and responsive to the wireless device sensing the parameter and determining that the value associated therewith satisfies the threshold criterion.*

151. In my opinion, Jain discloses limitation 17[e]. This limitation further requires that “*establishing the short range link*” occurs “*responsive to ... satisfying the proximity condition*” (addressed with limitation 4[a]) and “*responsive to the ...*

*parameter ... satisf[ying] the threshold criterion*” (addressed with limitations 1[a]-[c] and 4[a]).

152. As addressed in more detail above in connection with limitations 4[a] and 17[a], Jain incorporates an NFC standard that teaches or at least renders obvious conducting a command/response exchange that concludes with the “Initiator” device selecting one or more “Target” devices and attributes/parameters for communication (*i.e.*, “*establishing ... a short-range wireless link with the entity*”) after the “Initiator” and “Target” first detect RF signals from each other (*i.e.*, “*responsive to ... satisfying the proximity condition*”).

153. As discussed with limitations 1[a]-[c], Jain’s bootstrapping/authentication process includes fingerprint authentication (*i.e.*, “*parameter ... satisf[ying] the threshold criterion*”) prior to activating the mobile device with the transaction card. Because the activation is required to execute transactions, executing transactions over NFC (*i.e.*, “*establishing by the wireless device a short-range wireless link with the entity*”) also requires fingerprint authentication (*i.e.*, “*responsive to... sensing the parameter and determining that the value associated therewith satisfies the threshold criterion*”).

154. At a minimum, a POSITA would find it obvious for Jain’s smartphone to establish a NFC connection with the POS device (*i.e.*, “*establishing by the wireless device a short-range wireless link with the entity*”) after detecting “*the*

*wireless device satisfying the proximity condition relative to the entity” and “sensing the parameter and determining that the value associated therewith satisfies the threshold criterion.”* To ensure communications would be successful and not wasted signaling, and further to avoid the security risk of indiscriminately transmitting sensitive financial information, Jain’s smartphone needs to detect proximity and then establish a short-range communications link prior to proceeding with a payment transaction with the POS device. Use of a link after detecting proximity further improves reliability and security, because once a link is established, Jain’s mobile device can receive confirmation of receipt of individual packets. Indeed, such implementations of devices communicating via NFC establishing a connection prior to transmitting information were well-known to a POSITA. EX1019 ¶¶[0011], [0124], [0182]. For example, in EX1019, “to facilitate the establishment of an NFC connection (e.g., typically 2-4 cm)” (*satisfying the proximity condition*), an “RF field generated by the payee device [] may induce [] transition to an active mode of operation, thus establishing an NFC connection between the two devices.” EX1019 ¶[0124]. “Accordingly, by way of this established NFC connection, the payment [information] may be transmitted to and received by the payor device.” EX1019 ¶[0124]. Additionally, EX1020 discloses and leverages NFC to limit the range at which communication may take place. EX1020 ¶¶[0041], [0063]. Indeed, in the context of Wi-Fi, EX1020 even more

explicitly discloses using the ability to receive such signals as an indication of 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.”). A POSITA would be motivated and able to use Jain’s “request” or ECMA 340’s commands and responses in the same manner.

155. Similarly, establishing a link prior to authentication, such as through fingerprint authentication discussed with limitation 4[a], would be undesirable from the perspective of the POS device. An established link with no prior authentication can be hijacked by an unauthorized user, such as if the device is in possession of an unauthorized user. This provides a POSITA motivation to delay completing the ECMA initiation process detailed above with limitation 4[a] that “*establish[es] ... a short-range wireless link with the entity*” until after the user has completed the biometric authorization process detailed above with limitation 4[a]) (*responsive to the wireless device sensing the physiological parameter and determining that the physiological parameter sensed satisfies the criterion*).

**(h) Claim 18**

**(i) 18[pre]: *The wireless device of claim 14,***

156. As addressed in Sections V.A.2.a and V.A.2.c-d, it is my opinion that Jain discloses limitation 18[pre].

**(ii) 18[a]: *wherein said requesting from a second device an authorization to enable a function for***

***conducting a financial transaction and/or said receiving from the second device the authorization to enable the function for conducting the financial transaction comprises:***

157. It is my opinion that Jain discloses limitation 18[a]. Limitation 18[a] repeats language found in claim 14, also found in limitations 3[a]-[c] and addressed above.

**(iii) 18[b]: *establishing by the wireless device a link with the second device, comprising a wireless link that comprises a distance that is greater than a distance associated with the proximity condition;***

158. In my opinion, Jain discloses limitation 18[b]. Jain discloses the smartphone and transaction card “wirelessly transmit[ting] a request for the activation code using the cellular radio technology” to the financial institution. Jain ¶[0081]. Those cellular transmissions are over established links (*i.e.*, “***establishing by the wireless device a link with the second device***”). Jain ¶¶[0041]-[0043] (“establishing connections between packet-switched networks and communication devices” where a financial institution is part of a packet switched network), [0046], [0081], FIG. 2. Indeed, Patent Owner agrees. Patent Owner’s infringement contentions assert that using mobile data is sufficient to show “***establishing ... a link.***” EX1016 at 309-10.

159. Further, a POSITA would be motivated to implement Jain’s cellular communication with TCP. TCP is a very well-known connection-based protocol

that would improve reliability of a connection. EX1040 at 1. Even Jain references TCP. Jain ¶[0052]. Moreover, part of this “*link*,” from mobile device 110 to base station 210, is a “*wireless link*.” Jain FIG. 2.

160. As an alternative to cellular radio technology, Jain also discloses “the mobile device 110 transmit[ting] packet data using its own connection to the external world (e.g.,... Wi-Fi).” Jain ¶[0053], claims 13-14. This includes using “WiFi technology” to “wirelessly interface” with financial institutions. Jain ¶[0068], FIG. 5. This use of Wi-Fi involves establishing a “*link*,” part of which (from mobile device 110f to client 104e) is “*wireless*.” Jain ¶[0068], FIG. 5.

161. In Jain, the “*distance associated with the proximity condition*” is the distance between a mobile device and a nearby POS device. See Jain ¶[0023]. NFC is used between the mobile device and POS terminal to execute a transaction, and the distance. See Jain ¶[0023]. This distance for NFC use is “10 cm or less.” Jain ¶[0030]. The mobile device and the financial institution (i.e., “*second device*”) communicate using cellular radio technology, traversing intermediary nodes, including a base station. Jain ¶¶[0041]-[0043], FIG. 2. A wireless link to a base station (e.g., the top of a cell tower) is already going to be “*greater than a distance*” of the NFC wireless link—“10 cm or less.” Jain ¶[0030], FIG. 2.

- (iv) 18[c]: *wirelessly transmitting information to the second device over said wireless link using unlicensed and/or licensed frequencies; and*

**18[d]: *wirelessly receiving information from the second device over said wireless link using unlicensed and/or licensed frequencies;***

162. In my opinion, Jain discloses limitations 18[c]-[d]. Jain discloses the mobile device with the transaction card transmitting a request (*i.e.*, “***information***”) to the financial institution (*i.e.*, “***second device***”) and receives an activation code (*i.e.*, “***information***”) using cellular radio technology (*i.e.*, “***wirelessly ... over said wireless link***”). Jain ¶[0081]. Cellular radio technology “***us[es] ... licensed frequencies.***”

163. To the extent Patent Owner argues that such cellular radio technology instead uses “***unlicensed ... frequencies,***” that is also covered by claim 18. Either way, this limitation is met.

(v) **18[e]: *wherein said wirelessly transmitting and/or said wirelessly receiving comprises using an orthogonal frequency division multiplexing and/or orthogonal frequency division multiple access protocol; and***

164. In my opinion, Jain discloses limitation 18[e]. As discussed with limitations 18[c]-[d], Jain’s smartphone with the transaction card “***us[es]... cellular radio technology,***” including GSM, CDMA, UMTS, and “***any other cellular technology.***” Jain ¶¶[0041]-[0043], [0081]. A POSITA would be motivated to use the most advanced and performant cellular radio technologies. This includes LTE and WiMAX (*i.e.*, 4G) in addition to the cellular radio technology mentioned in Jain

to keep up with ever-evolving technologies that allow for higher data rates.

Moreover, Jain mentions using “any other cellular technology.” Jain ¶[0041]. LTE

and WiMAX were known to a POSITA as of the ’756 Patent’s priority date to be in

line to displace older technologies in the near future. *See also* EX1045; EX1046.

Wi-Max and LTE “*us[e] ... orthogonal frequency division multiplexing and/or*

*orthogonal frequency division multiple access protocol.*” EX1045; EX1046.

- (vi) 18[f]: *wherein said establishing by the wireless device a link with the second device comprises establishing the link with the second device responsive to the wireless device sensing the parameter and determining that the value sensed satisfies the threshold criterion.*

165. In my opinion, Jain discloses limitation 18[f]. This limitation requires that the “*establishing*” of limitation 18[b] is performed that in response to the “*sensing the parameter,*” “*determining ... the value,*” and “*satisf[ying] the threshold*” of limitations 14[a]-[b]. Jain requires completion of authorization process 700. This includes user authentication steps 734-742 (*i.e.*, “*sensing the parameter,*” “*determining ... the value,*” and “*satisf[ying] the threshold*”) prior to enabling the mobile device to communicate with the financial institution (*i.e.*, “*second device*”). *See* Jain ¶¶[0072], [0080]-[0081], FIGS. 7, 9. Enabling communication is done by “turning antenna on” in step 714, where cellular radio technology enabled and then used in connection with process 900, including steps 920-926. *See* Jain ¶¶[0072], [0080]-[0081], FIGS. 7, 9. Therefore, “*establishing*

IPR of U.S. Patent No. 11,770,756

Decl. of Dr. Kevin Almeroth

*the link*” between the mobile device and financial institution over cellular wireless technology is “*responsive to*” Jain’s user authentication.

**B. Ground 2: Dua (EX1018)**

**1. Background**

166. 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 ’756 Patent under at least pre-AIA 35 U.S.C. § 102(b).

167. 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 devices (*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.

168. 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:

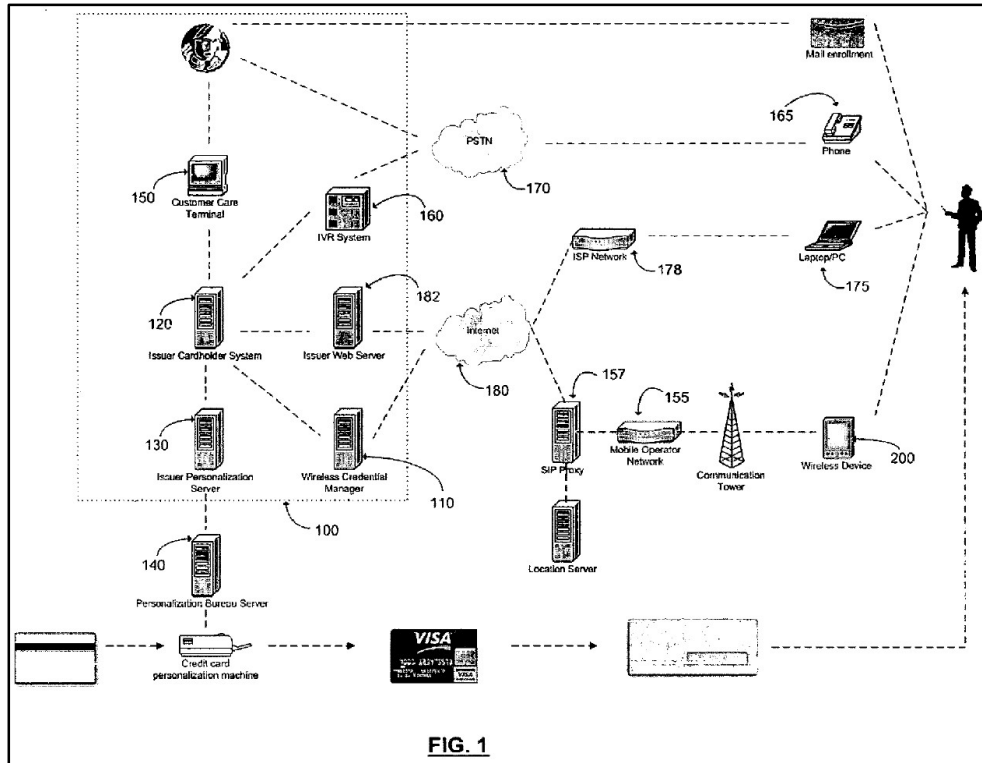
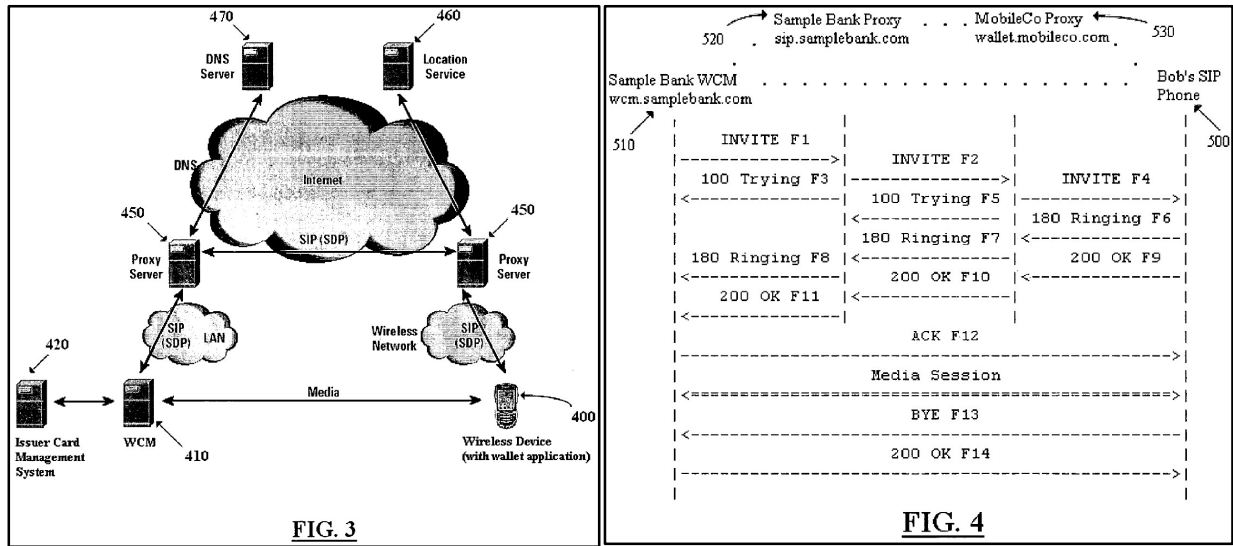


FIG. 1

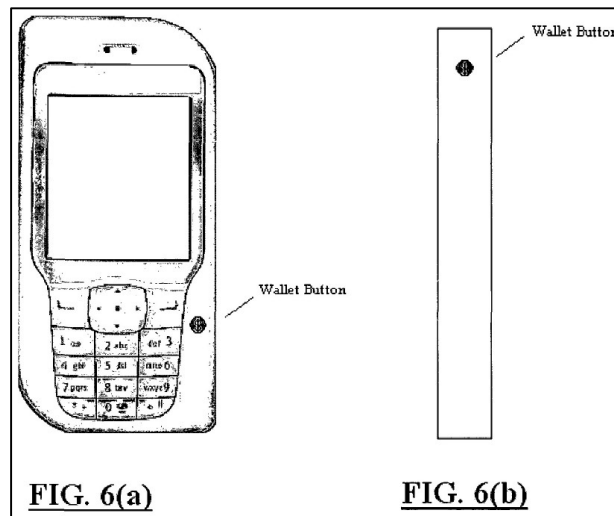
169. Figure 1 shows a network by which a wireless credential manager “WCM 110 [can] ... issu[e], cancel[], and manag[e] electronic credentials [to] wireless device[]” 200. Dua ¶[0046]. An issuer can issue a physical credit card to a user, and the user “may also request a digital card for use with [a] 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].

170. 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:



171. 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].

172. 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.



173. 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]: *A method of operating a device, the method comprising:***

174. In my opinion, Dua discloses limitation 1[pre]. Dua discloses a wireless “*device*,” “such as a mobile telephone.” Dua Abstract, FIGS. 3, 5, 6(a)-8. The wireless device includes phone applications like a “wallet application,” which can be operated to “conduct[] financial... transactions” (*i.e.*, “*method of operating*”). Dua Abstract, ¶¶[0041], [0312]-[0313], [0333].

**(ii) 1[a]: *sensing by the device, using a device-based sensor, a parameter that is associated with the device, an environment of the device and/or a user of the device;***

**1[b]: *determining by the device a value of the parameter that is sensed; and***

**1[c]: *responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion, enabling by the device a number of functions of the device and disabling by the device a function of the device;***

175. In my opinion, Dua discloses limitations 1[a]-[c]. Limitations 1[a]-[c] constitutes two steps—(1) checking whether a “*parameter ... satisf[ies] a threshold criterion*,” which includes “*sensing*” and “*determining*” the “*parameter*,” and (2), upon passing the check, “*enabling ... number of functions*,” where a “*number of functions*” can be one function (’756 Patent, limitation 2[a] (“*enabling ... a number*

*of functions ... comprises enabling ... a number of functions ... that is greater than or equal to one*).), and disable another, different *function*. Dua discloses these requirements under two theories: **Card-Issuing Theory** and **External-Storage Theory**.

176. Under the **Card-Issuing Theory**, Dua discloses the wallet application being opened for the wireless device to be issued a credit card. 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[s] the user access to the application.” Dua ¶¶[0366], [0429]. Thus, PIN-entry is required for credit card issuance. Dua confirms this with other disclosures. 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

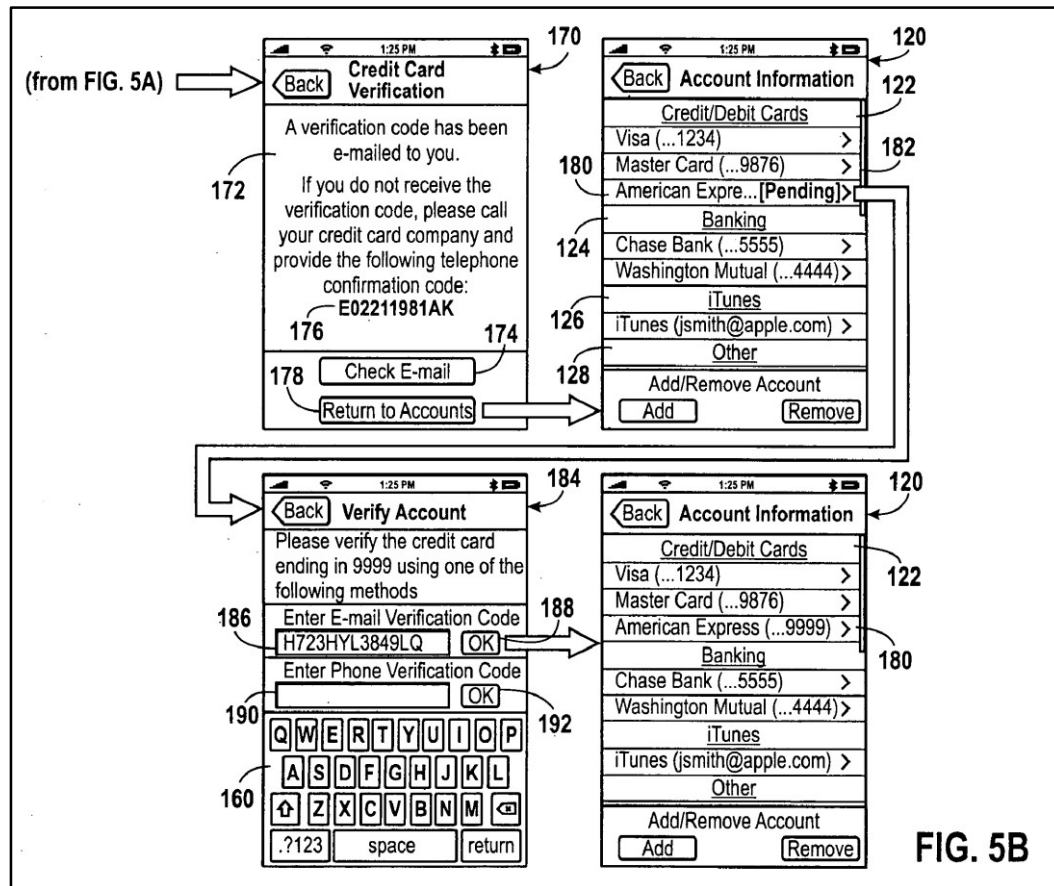
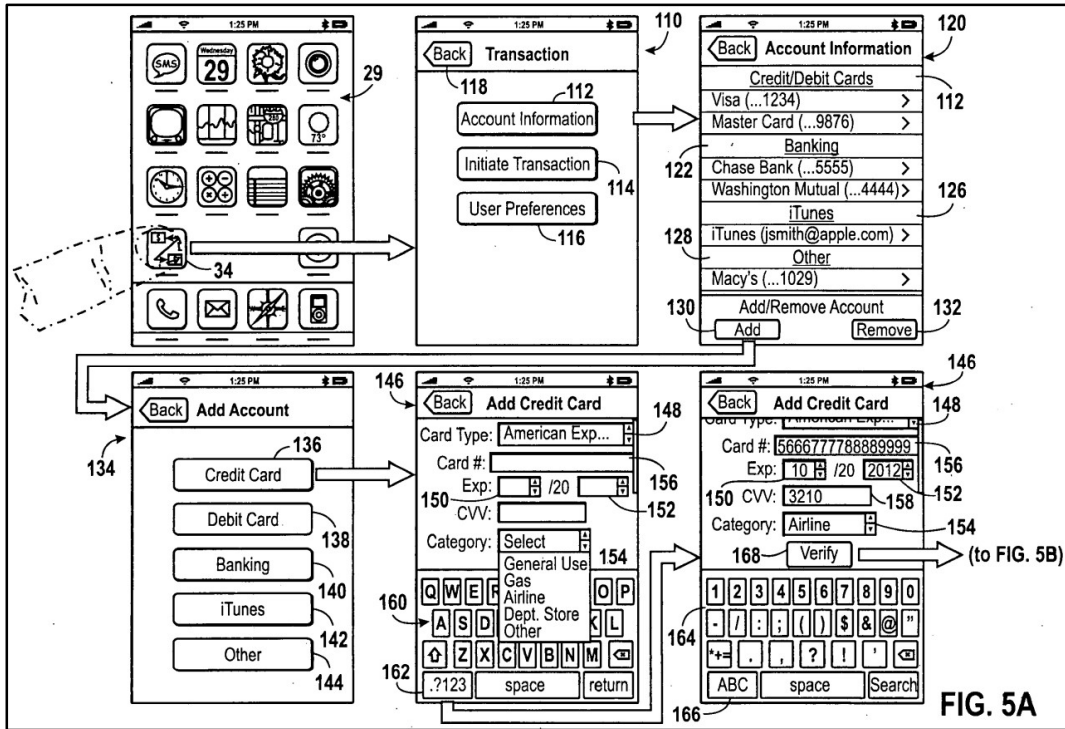
that credit card issuance requires the wallet application to connect with, and accept data from, a remote server—usually a WCM. Dua ¶¶[0038], [0179]-[0180], FIGS. 3-4. But without requiring PIN-entry to open the wallet for credit card issuance, anyone could allow the wallet application to connect and 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].

177. 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.

178. 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 issues "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.

179. At a minimum, requiring PIN entry under these circumstances would be obvious. To ensure security of the other credentials, alongside allowing use of an encrypted wallet application and changes to the wallet application by an authenticated user, a POSITA would retain Dua's "default" user authentication for credit card issuance. Dua ¶[0366]. Indeed, it was well known to require such verification before permitting access to such sensitive functionality. EX1019 ¶[0107], FIGS. 10A-10B:



180. A POSITA would be motivated to include this feature in Dua's wallet application because being able to add credit cards directly within the wallet application increases the user's control over credit card management from the wallet application. The wallet application user no longer has to "request the new credential over the phone [(i.e., by calling an issuer),] ... by logging into the issuer's secure website[,] ... or in person at a branch" to issue a credit card to the wallet application, as disclosed by Dua. Dua ¶¶[0055]-[0056]. Instead, an add-account feature simplifies credit card issuance. The wallet application becomes a one-stop shop for credit card management and transactions. Dua requires requesting through those other means to "validat[e] ... [the] identity [of] the user." Dua ¶[0055]. But Dua's PIN-entry to open the wallet application (Dua ¶¶[0366], [0429].) coupled with Lin's security features ensures valid card issuance to the correct user. EX1019 ¶¶[0143]-[0146], FIGS. 5A-B.

181. Dua 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 (*i.e.*, "**sensing ... using a device-based sensor a parameter**"). 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. Either constitutes "*determining ... a value of the parameter*" and "*satisfying a threshold criterion.*" Dua ¶¶[0050], [0366], [0399], [0429].

182. A POSITA would also understand that biometric authentication can be implemented in this manner. Biometric verification ensures that the current user's fingerprint matches the biometrics of the rightful owner of the device. To compare the user's fingerprint against the biometrics of the rightful owner, the wireless device needs to store the biometrics of the rightful owner during setup, and then use the stored valid biometrics to compare against scanned biometrics of the current user. Comparing scanned biometrics against the valid biometrics requires the scanned biometrics to sufficiently match such that there is adequate confidence that the current user is the device's owner. Otherwise, biometric verification would not serve its central purpose.

183. 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.

184. This type of implementation was well known to a POSITA, as indicated by the numerous prior art references describing it. *See, e.g.*, EX1021 ¶¶[0040]-[0042]; EX1024 ¶¶[0009], [0025]; EX1025 ¶¶[0044], [0086]-[0092]; EX1026 at 196. For instance, EX1024 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

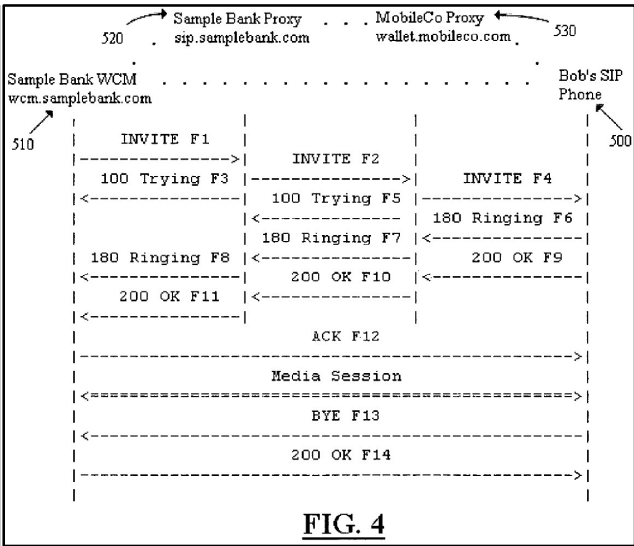
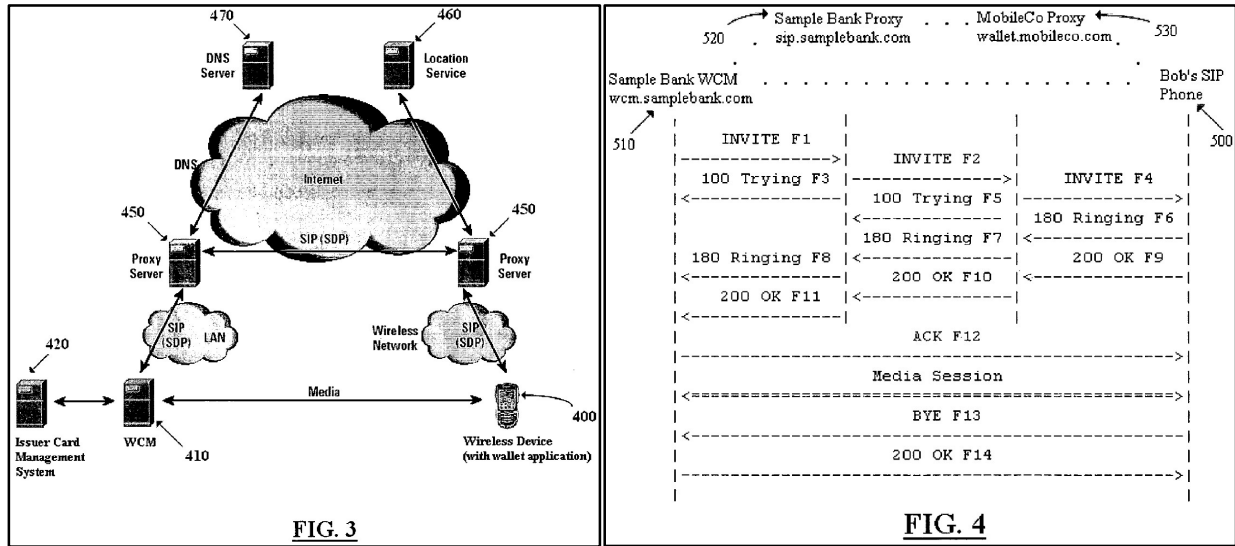
device ... acquire[s] biometric measurements of a person who is attempting to use the payment device to make a proximity payment. These field biometric measurements are internally compared with the previously recorded biometric profile of the authorized individual.” EX1024 ¶¶[0009]. Similarly, EX1025 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].

185. Patent Owner makes the same mapping. Patent Owner’s infringement contentions asserts that the Accused Products “sen[se,]... using a device-based sensor such as... a fingerprint scanner... a parameter... associated with the... a user of the device,” and “determin[e]... a value of the parameter, such as... a fingerprint... .” EX1016 at 6, 13.

186. After finding a valid fingerprint (*responsive to... the parameter... satisfying a threshold criterion*), the wallet application is opened to be issued a credit card. As part of issuance, the issuer’s wireless credential manager (“WCM”) “authenticate[s] the mobile user’s identity in real-time.” Dua ¶[0180]. The authentication process includes “prompting the user for some cardholder or accountholder authentication information,” and the “user would see such a request... within the wallet application screen.” Dua ¶[0180]. The wallet application establishes a Session Initiation Protocol (“SIP”) communication session (*i.e.*,

“enabling ... a number of functions”) between the wireless device and the issuer’s WCM for this authentication process (i.e., “enabling ... a number of functions”).

Dua ¶¶[0046], [0104], [0128], [0178], FIGS. 3 and 4:



187. Further, Dua discloses how “[d]ata in the wallet application is encrypted and protected with a ... PIN ... .” Dua ¶[0366]. For instance, if data in the wallet application is encrypted, opening the wallet application and allowing “[u]sers [to] scroll through... and select credentials” requires the wallet application data to be decrypted. Dua ¶¶[0371]-[0377]. Thus, opening the wallet application, such as for credit card issuance, causes the wallet application data to be decrypted (i.e., “enabling ... a number of functions”) and disables the encryption function for wallet application data (i.e., “disabling ... a function”).

188. Other security mechanisms are also “disabl[ed]” upon successfully opening the wallet application, such as functions for tracking authentication

attempts. For instance, “[i]f a user keys in ... incorrect biometric identification ... three consecutive times, the wallet application will not function.” ¶[0441]. A POSITA would understand that providing a valid fingerprint would disable this security subroutine (*i.e.*, “**disabling ... a function**”). Or a POSITA would find it obvious to disable this function because, upon receiving a valid fingerprint, the wireless device must wait an indefinite amount of time until the user is prompted again for a fingerprint. The wireless device should not waste processing power on tracking authentication attempts when an authentication process is not being performed.

189. Opening the wallet application also allows a user to change the wallet application’s settings, allowing for functions and features to be enabled and disabled. *See* ¶¶[0310], [0324]-[0331], [0351], [0366], [0384]. For instance, PIN-entry to open the wallet application is a “default security setting,” and could be turned off (*i.e.*, “**disabling ... a function**”). ¶[0366]. The settings also “allow users to delete extensions” on the wallet application (*i.e.*, “**disabling ... a function**”), (¶[0310].) where “[e]xtensions ... ‘extend’ the capability of the wallet platform by enabling a new set of features ... .” ¶[0289]. The mobile device has modifiable “hot buttons,” where a “user could use the ‘Wallet Settings’ functionality in the wallet application to link [a] favorite/preferred credit card to [a hot] button” (*i.e.*, “**enabling ... a number of functions**”). Changing the favorite/preferred credit card

also entails an ability to delink a credit card from a hot button (*i.e.*, “**disabling ... a function**”). See Dua ¶[0392], FIGS. 6A-7B. Also, “[a] user can ... choose to designate certain credentials ... to be used without requiring [PIN-]entry” (*i.e.*, “**disabling ... a function**”). Dua ¶[0367].

190. Alternatively, Dua also discloses the assertions made in Patent Owner’s infringement contentions, where the “**enabling a number of functions**” limitation is met by “unlocking the smartphone or an application.” EX1016 at 20. And the “**disabling a function of the smartphone**” limitation is met by “disabling the lock function.” EX1016 at 20. The same disclosure is found in Dua. The wallet application must be opened for credit card issuance. The “default security setting... is that PIN-entry is required before the wallet application can be ‘opened,’” or otherwise “allow the user access to the application.” Dua ¶¶[0366], [0429]. Therefore, the wallet application is unlocked and thereby engaging functions related to operating the wallet application (*i.e.*, “**enabling a number of functions**”), and the lock function of the wallet application is disabled (*i.e.*, “**disabling a function of the smartphone**”).

191. Under the **External-Storage Theory**, Dua discloses using an external wallet storage service to store a wallet application’s credentials. Dua ¶[0491]. “The external storage performs two basic functions: storage and retrieval of information registered in the user’s wallet application.” Dua ¶[0491]. Opening the wallet

application causes credentials to be retrieved from the external storage for viewing and use. ¶[0495]. Therefore, retrieval of credentials from the external storage is only possible after performing fingerprint authentication. ¶¶[0353]-[0354], [0366], [0429]. As addressed above in connection with the **Card-Issuing Theory**, requiring fingerprint authentication to open the wallet application discloses or at least renders obvious the claimed “*sensing ... a parameter*,” “*determining... a value*,” and “*satisfying a threshold criterion*.”

192. After opening the wallet application, communicating with external storage, such as for credential retrieval, requires (1) establishing a connection with the external storage, (2) the wallet application authenticating itself to the external storage, and (3) credential transmission back to the wallet application. ¶¶[0491]-[0492], [0495]. “[W]henver the wallet application is launched[,] ... a real-time connection is initiated between the wallet application and ... [external] storage” by “utiliz[ing] SIP” (*i.e.*, “*enabling ... a number of functions*”). ¶¶[0494]-[0495]. The “real-time connection” includes “encrypt[ion] [for] all messages between the wallet application and the storage service,” where “[n]ew communication keys can be dynamically generated for each communication session” (*i.e.*, “*enabling ... a number of functions*”). ¶¶[0493], [0495].

193. As addressed above in connection with the **Card-Issuing Theory**, opening the wallet application, such as for viewing and using credentials, causes the

wallet application data to be decrypted (*i.e.*, “**enabling ... a number of functions**”).

Further, when the wallet application uses external storage, the wallet application only holds retrieved credentials and data temporarily. *Dua* ¶[0495]. The wallet application’s **function** for encrypting (*see* *Dua* ¶[0366].) and permanently storing received credentials and data is “**disabl[ed]**.” *See* *Dua* ¶[0495].

194. Also as addressed above in connection with the **Card-Issuing Theory**, opening the wallet application via fingerprint authentication also allows a user to change the settings of the wallet application, thereby enabling and disabling certain functions and features of the wallet application. *See* *Dua* ¶¶[0310], [0324]-[0331], [0351], [0366], [0384]. For instance, a user can turn off several features via the settings (*i.e.*, “**disabling ... a function**”), including the PIN-entry for opening the wallet application (*Dua* ¶[0366].), “delet[ing] extensions” (*Dua* ¶[0310].), de-linking credentials from hot buttons (*see* *Dua* ¶[0392].), and designating a credential for PIN-less use (*Dua* ¶[0367].).

195. Similar to the **Card-Issuing Theory**, this embodiment with the external storage tracks the assertions made in Patent Owner’s infringement contentions. In its infringement contentions, Patent Owner asserts that the “**enabling a number of functions**” is met by “unlocking the smartphone or an application,” and “**disabling a function of the smartphone**” is met by “disabling the lock function” respectively. EX1016 at 20. In *Dua*, using fingerprint authentication to open the wallet

application causes the wallet application to be unlocked thereby enabling functions related to operating the wallet application (*i.e.*, “**enabling a number of functions**”), and the lock function of the wallet application is disabled (*i.e.*, “**disabling a function of the smartphone**”).

- (iii) 1[d]: *wherein the parameter that is sensed using the device-based sensor, comprises a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state; and*

196. In my opinion, Dua discloses limitation 1[d]. As discussed with limitations 1[a], Dua discloses several possible biometric inputs—a fingerprint, iris, voiceprints, facial recognition, and/or hand geometry (*i.e.*, “**parameter ... sensed using the device-based sensor ... compris[ing] ... a physiological state**”). See Dua ¶¶[0366], [0414], [0534].

- (iv) 1[e]: *wherein the device comprises a smartphone.*

197. In my opinion, Dua discloses limitation 1[e]. Dua discloses wireless device as a “**smartphone**”—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]-[0051], [0287]-[0288], FIGS. 3, 5, 6(a)-8.

**(b) Claim 2**

- (i) 2[pre]: *The method of claim 1,*

198. As addressed in Section V.B.2.a, it is my opinion that Jain discloses limitation 2

```
].
```

- (ii) **2[a]:** *wherein said enabling by the device a number of functions of the device comprises enabling by the device a number of functions of the device that is greater than or equal to one.*

199. In my opinion, Dua discloses limitation 2[a]. As discussed with limitation 1[c], Dua discloses enabling one or more (*a number ... that is greater than or equal to one*) functions.

**(c) Claim 3**

- (i) **3

```
]:
```** *The method of claim 1, further comprising:*

200. As addressed in Section V.B.2.a, it is my opinion that Jain discloses limitation 3

```
].
```

- (ii) **3[a]:** *while said number of functions is enabled by having sensed by the device the parameter and by having determined by the device that the value of the parameter that is sensed satisfies the threshold criterion, requesting by the device from a second device an authorization to enable a function for conducting a financial transaction by the device;*

**3[b]:** *responsive to the requesting, receiving by the device from the second device the authorization to enable the function for conducting the financial transaction; and*

201. Claim 3 identifies additional steps to be performed after *enabling... functions* discussed with limitation 1[c]. It is my opinion that Jain discloses these steps recited in limitations 3[a]-[c].

202. Specifically, the first of these additional steps is *requesting by the device from a second device an authorization to enable a function for conducting a financial transaction by the device*. The second of these additional steps is, *responsive to the requesting, receiving by the device from the second device the authorization to enable the function for conducting the financial transaction*. It is my opinion that Dua discloses these two steps under the **Card-Issuing Theory** and **External-Storage Theory**.

203. Under the **Card-Issuing Theory**, Dua discloses the wireless device “*requesting ... from*” the issuer’s WCM (*i.e.*, “*second device*”) a credential (*e.g.*, credit card) (*authorization to ... conduct ... a financial transaction*). Specifically, after opening the wallet application, the “issuer’s system will authenticate the ... user’s identity ... to ensure that the [user] ... is ... the person that requested the digital credential.” Dua ¶[0180]. The “authentication process [is] ... accomplished by ... the issuer system prompting the user for some cardholder ... information,” where the “user would see such a request for information within the wallet application.” Dua ¶[0180]. The credential-issuance request asks for a “special code or PIN that was mailed to the user in advance of the issuance.” Dua ¶[0180].

204. The wireless device's wallet application then sends the "special code or PIN" to the WCM (*i.e.*, "***requesting by the device from the second device an authorization to enable a function for conducting a financial transaction by the device***"). This response is for user authentication. The response "ensur[es] that the [user] ... is in fact the person that requested the digital credential." Dua ¶[0180]. "Subsequent to ... validating the user's identity[,]" (*i.e.*, "***responsive to the requesting***") "the WCM 510 will transmit the credential to the wallet application" (*i.e.*, "***receiving... the authorization to enable the function for conducting the financial transaction***"). Dua ¶[0180].

205. The wallet application's response with the "special code or PIN" results in an issued credit card transferred to the wallet application, where the credit card is authorization to execute financial transactions with an account. Therefore, it is my opinion that the transmission of the PIN code and reception of the credit card constitutes "***requesting***" and "***receiving ... authorization to enable the function for conducting the financial transaction,***" respectively.

206. Patent Owner makes the same mapping in its infringement contentions. Patent Owner asserts in its infringement contentions that receiving an issued credit card for conducting financial transactions is sufficient to establish "request[] an ***authorization*** to establish a function to conduct a financial transaction." EX1016 at 42, 44-46, 51-54.

207. The wallet application transmits the PIN code—“*request*[.]”—to the WCM occurs “*while said number of functions [are] enabled.*” The enabled functions are mentioned with the discussion of limitation 1[c]. The enabled functions include (1) establishment of a communication channel with the WCM, (2) authentication process with the WCM, (3) decrypted credentials and wallet application data, and (4) unlocked wallet application.

208. The “*request*[.]” is transmitted over a communication channel with the WCM. The transmission can only occur “*while*” the communication channel is established and transmission functionality is enabled (*i.e.*, “*enabl[ed] ... functions*”).

209. The “*request*[.]” is also part of the authentication procedures for credit card issuance by the WCM. Therefore, the wallet application has already *enabl[ed]* the authentication subroutine for credit card issuance with the WCM prior to the “*request*[.]”

210. This authentication subroutine requires the wallet application to be open for the user to provide a PIN. *See* Dua ¶[0180]. “PIN-entry is [used] before the wallet application can be ‘opened,’” and the wallet application’s “*request*[.]” occurs from the user responding to the “issuer system prompting the user” “within the wallet application.” Dua ¶[0180]. Thus, the wallet application has to be

unlocked, and wallet application data decrypted, for the user to respond to the prompt and submit the request.

211. Under the **External-Storage Theory**, Dua discloses the wireless device “**requesting ... from**” the external storage (*i.e.*, “**second device**”) a credential (*e.g.*, credit card) (*i.e.*, “**authorization to ... conduct ... a financial transaction**”). “Whenever the wallet application is launched on the device and a user logs in with his valid PIN, a real-time connection is initiated between the wallet application and the storage service. The wallet application automatically authenticates itself and gains access to the stored credentials” (*i.e.*, “**requesting... authorization to enable a function for conducting a financial transaction by the device**”). Dua ¶[0495]. The wallet application automatically authenticates itself to the external storage by transmitting a “username/password,” and the wallet application’s access to the storage area allows for retrieval of credentials. Dua ¶¶[0491]-[0492], [0495]. From the external storage the “credential information is securely transmitted to the wireless device and temporarily made available for use by the wireless device” (*i.e.*, “**receiving ... the authorization to enable the function for conducting the financial transaction**”). Dua ¶[0495].

212. The automatic authentication and retrieval constitutes “**requesting**” and “**receiving ... authorization to enable the function for conducting the financial transaction**” because the resulting credential on the wallet application can be used

to execute transactions. *See also* EX1016 at 42. This mapping is also found in the Patent Owner's infringement contentions, where Patent Owner asserts that receiving a credit card for conducting financial transactions is sufficient to establish "request[] an **authorization** to establish a function to conduct a financial transaction." EX1016 at 42, 44-46, 51-54.

213. The wallet application's automatic authentication to the external storage occurs "**while said number of functions [are] enabled.**" As mentioned previously with limitation 1[c], the enabled functions include (1) establishment of a communication channel with the external storage, (2) decrypted wallet application data, and (3) unlocked wallet application.

214. The wallet application "automatically authenticat[ing] itself" to the external storage requires communication with the external storage over a communication channel. Dua ¶¶[0495]. Said communication must be "**enabl[ed]**" in order to end the underlying request.

215. Automatic authentication means transmitting a "username/password" to the external storage. *See* Dua ¶¶[0492], [0495]. The username/password is data in the wallet application. *See* Dua ¶¶[0492], [0495]. The wallet application also has data regarding "headers for information in storage," which allows a user to see what credentials are stored and select credentials to retrieve. Dua ¶[0494]. "Data in the wallet application is encrypted and protected with a special wallet PIN set by the

wireless device owner ... .” Dua ¶[0366]. “The PIN may serve as a decryption key ... .” Dua ¶[0399]; *see also* Dua ¶¶[0180], [0366], [0429]. The username/password and headers are used, and therefore must be decrypted “*while ... requesting*” retrieval of a credential. Dua ¶[0495].

216. Separately, the wallet application establishes a communication channel with the external storage, and request credentials over that channel, after the wallet application is opened. Specifically, “whenever the wallet application is launched... with [a] valid PIN,” the “wallet application automatically authenticates itself [to the external storage] and gains access the stored credentials.” The wallet application is unlocked “*while*” the wallet application automatically authenticates itself (*i.e.*, “*requesting ... authorization*”).

(iii) 3[c]: *responsive to receiving the authorization, enabling at the device the function for conducting the financial transaction.*

217. Limitations 3[a]-[b] discussed “*requesting*” and “*receiving*” under the **Card-Issuing Theory** and **External-Storage Theory**. The *requesting* results in the wallet application *receiving* a credential, either from the WCM or external storage. “[*R*]*esponsive to ... receiving*” the credential, the wireless device can use the “credential... to conduct... transactions via... a short range wireless link with a point-of-sale terminal” (*enabling at the device the function for conducting the financial transaction*). Dua Abstract.

218. Under the **Card-Issuing Theory**, the wallet application uses issued credentials to conduct financial transactions. A “credential ... to conduct ... transactions via ... a short range wireless link with a point-of-sale terminal.” Dua Abstract. The “short-range wireless link” is created through communications by the wireless device’s “integrated RFID chip” and using the Near-Field-Communications (“NFC”) protocol (*i.e.*, “**enabling at the device the function for conducting the financial transaction**”). Dua ¶¶[0016], [0315]. These transaction functionalities—transmitting the credential to a POS terminal (*i.e.*, “**function for conducting the financial transaction**”)—are only available after the credential issuance (*i.e.*, “**responsive to receiving the authorization, enabling ... the function for conducting the financial transaction**”) because credential cannot be transmitted prior to being issued.

219. **External-Storage Theory:** The wallet application uses credentials retrieved from external storage to conduct financial transactions. A retrieved “credential ... is ... temporarily made available for use by the device’s RFID interface. Dua ¶[0495]. “[**R**]esponsive to receiving” the credential, a wireless device can transmit the credential to a POS terminal to execute a transaction, which means transmission functionalities—a wireless device’s “integrated RFID chip” and NFC implementations—are “enabl[ed]” (*i.e.*, “**enabling ... the function for conducting the financial transaction**”). Dua Abstract, ¶[0495].

**(d) Claim 4**

**(i) 4[pre]: *The method of claim 3, further comprising:***

220. As addressed in Section V.B.2.c, it is my opinion that Jain discloses limitation 4[pre].

**(ii) 4[a]: *responsive to the device satisfying a proximity condition relative to an entity and responsive to the device sensing the parameter and determining the value that is associated with parameter that is sensed satisfies the threshold criterion, using by the device the function for conducting the financial transaction and conducting by the device the financial transaction by paying for a product.***

221. In my opinion, Dua discloses limitation 4[a]. Claim 4 builds on claim 3, and claim 3 builds on claim 1. Claim 1 recites steps for “*enabling ... functions.*” Claim 3 adds steps for using those enabled for enabling a “*function for conducting a financial transaction.*” Claim 4 further recites steps for engaging in a financial transaction. The added steps include requires two prerequisites: (1) “*satisfying a proximity condition relative to an entity*” and (2) “*sensing the parameter... satisf[ying] the threshold criterion.*” These are the prerequisites for “*paying for a product.*”

222. Dua discloses the wireless device using a “credential... to conduct... transactions via... a short range wireless link with a point-of-sale terminal” (*i.e.*, “*conducting by the device the financial transaction*”). The short-range wireless

link is created through communications by the wireless device's "integrated RFID chip" and using the Near-Field-Communications ("NFC") protocol (*i.e.*, "**using by the device the function of conducting the financial transaction**"). Dua ¶¶[0016], [0315].

223. Establishing and using the short-range wireless link to execute the transaction is "**responsive to the device satisfying a proximity condition relative to**" the POS terminal. The wireless device's short range wireless link with the point-of-sale reader includes NFC. Dua Abstract, ¶¶[0016], [0318]. Therefore, the transaction follows (*i.e.*, "**responsive to**") the wireless device being in "close proximity" to the point-of-sale terminal—detecting the POS terminal's NFC communications (*i.e.*, "**the device satisfying a proximity condition relative to an entity**"). Dua Abstract, ¶¶[0016], [0318]. NFC and other short range wireless communication protocols are only effective at short ranges, where the signal strength is sufficient enough to allow communication over these protocols. Signal strength attenuates with increasing distance. Indeed, Patent Owner asserts as much in its infringement contentions. Patent Owner asserts the use of NFC as establishing "**the device satisfying a proximity condition relative to an entity.**" EX1016 at 61. Thus, Dua's wireless device using NFC to communicate with the POS terminal means that, the wireless device "**detected that a proximity condition is satisfied**" by receiving

and decoding a short-range NFC signal from the POS device. Dua Abstract, ¶¶[0041], [0314]-[0315], [0382], [0395].

224. In addition, a POSITA would find proximity detection based on signal strength obvious. The wireless device establishes, with the POS terminal, a peer-to-peer communication session over NFC. *E.g.*, Dua ¶[0016], Claims 33, 36, 50. Dua contemplates these sessions transferring a large amount of data, including encryption keys and several credentials. Dua ¶[0359]. For instance, this may “require the user to hold the wireless device in front of the reader for a longer period of time while the processing ... takes place.” Dua ¶[0359]. As previously mentioned, these communication sessions use short range signals, such as near-field communication (NFC) or proximity signals. *See* Dua Abstract, ¶¶[0016], [0041], [0314]-[0315], [0382], [0395]. Short-range signal communications are dependent on proximity between the two devices communicating.

225. Ensuring successful data transfer requires the wireless device to detect that the wireless device is nearby the POS terminal. Without a reaching a certain signal strength or otherwise satisfying a “*proximity condition*,” Dua’s wireless device transmits communications are wasted signals, processing time, and user time because the communications are guaranteed to be lost. The communications are also at risk of miscommunication. Without ensuring proximity, sending communications across a distance outside the effective range will likely subject the communications

to errors, like packet loss. 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.

226. Further, transmission without ensuring proximity is a security risk. Without ensuring proximity, the wireless device is indiscriminately transmitting without ensuring communication to the correct device. This is especially important for executing financial transactions, where sensitive financial information is being communicated.

227. To ensure communications will be successful and not just wasted signals and wasted user time, Dua's wireless device first needs to detect it is near the POS prior to proceeding with a payment transaction with the POS device. In addition, transmitting sensitive financial information when there is no bona fide POS in proximity poses a security risk. As such, it would have been obvious for a POSITA to configure the smartphone to first detect that it is proximate to Dua's POS device prior to attempting short-range signal communication to prevent the error condition of a smartphone sending short-range signals with a POS device that is too far or to the wrong device, *e.g.* a fraudulent device.

228. 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.

229. Under the second prerequisite—“*sensing the parameter ... satisf[ying] the threshold criterion*”—Dua’s fingerprint authentication to open the wallet application constitutes “*sensing ... a parameter,*” “*determining ... a value of the parameter,*” and “*satisfying a threshold criterion*” under the **Card-Issuing Theory** and **External-Storage Theory** as discussed with limitations 1[a]-[c].

230. Fingerprint authentication is also a prerequisite to executing transactions (*i.e.*, “*responsive to the device sensing the parameter and determining the value that is associated with parameter that is sensed satisfies the threshold criterion*”). Fingerprint authentication opens the wallet application for card issuance or credential retrieval under the **Card-Issuing Theory** or **External-Storage Theory**, respectively, and thereby is a prerequisite to later navigating, selecting, and using the issued or retrieved credentials in transactions. *See* Dua ¶¶[0371], [0378], [0384].

231. To the extent the claim recites an additional transaction-specific *sensing, determining, and satisfying*, Dua discloses this. A valid fingerprint can be required for transactions. The “default security setting in the wallet application is that PIN-entry is required before” (*i.e.*, “*responsive to*”) “any credentials [are] transmitted to an external device,” including “inputting a PIN before RF

communication can be enabled,” such as for a transaction with a point-of-sale reader.

Dua Abstract, ¶¶[0366], [0395]; *see also* Dua ¶¶[0368], [0377]. PIN codes can be replaced with fingerprints scanned by the “wireless device’s embedded biometric technologies.” Dua ¶¶[0366], [0414], [0414].

232. To finally “*pay[] for a product,*” Dua discloses the wireless device using a “credential... to conduct... transactions via... a short range wireless link with a point-of-sale terminal” (*i.e.*, “*conducting by the device the financial transaction*”). The executed transaction entails “*paying for a product,*” such as groceries or train tickets. *See* Dua ¶¶[0352]-[0353].

233. The short-range wireless link is created through communications by the wireless device’s “integrated RFID chip” and using the NFC protocol (*i.e.*, “*using by the device the function of conducting the financial transaction*”). Because executing the transaction is done over NFC, the transaction “*responsive to the*” wireless device being within “*proximity relative to*” the POS terminal, as discussed above. Dua ¶¶[0016], [0315]. Also as discussed above, fingerprint authentication is required to establish the short range wireless link only (*i.e.*, “*responsive to the ... parameter ... satisf[y]ing the threshold criterion*”).

(e) **Claim 5**

- (i) **5[pre]:** *The method of claim 3, further comprising:*

234. As addressed in Section V.B.2.c, it is my opinion that Jain discloses limitation 5[pre].

(ii) **5[a]: *enabling at the second device a function for conducting the financial transaction.***

235. In my opinion, Dua discloses limitation 5[a], under the **Card-Issuing Theory** and **External-Storage Theory**.

236. Under the **Card-Issuing Theory**, Dua discloses the issuer's WCM (*second device*) "authentical[ing] a mobile user's identity in real-time during a transaction," such as for transactions executed with issued cards. Dua ¶¶[0180], [0250]. "[I]ssuers may issue a credential to a wireless device, require the wallet PIN with every transaction, but also prompt the user for an issuer PIN" either on the POS terminal or wallet application. Dua ¶[0402]. One "type of PIN verification scheme" includes over-the-air or "OTA PIN verification," where the "WCM ... can ... handle over-the-air PIN verification for electronic credentials ... ." Dua ¶¶[0404], [0406].

237. When the wireless device transmits credentials to a POS terminal for a transaction, the POS "terminal ... can ... transmit [the received] credential ... for online authorization," such as through over-the-air PIN verification. Dua ¶[0405]. A transaction request from a POS to a WCM "will be held until a PIN request is sent to [the] wireless device ... and ... the entered PIN is validated." Dua ¶[0407]. The "WCM ... is used to deliver a PIN request to [the] wireless device ... and to receive a user-input response from [the] wireless device." Dua ¶[0405]. Because the

authorization for the transaction is withheld until the “PIN ... validation,” and because the “WCM ... deliver[s] [the] PIN request ... and ... receive[s] [the] user-input response,” the WCM’s over-the-air PIN verification is “*a function for conducting the financial transaction.*”

238. The WCM must have the “OTA PIN verification turned on” for an account (*i.e.*, “*enabling ... a function*”), (Dua ¶[0406].) which occurs with credential issuance to a wallet application. *See* Dua ¶¶[0406], [0408], [0413]. Issued “credential[s] ... [are] labeled by an issuer as using over-the-air... PIN verification credential issuance.” Dua ¶[0413]. In order to label an issued credential as such, “[t]here must be a valid E.164 mobile phone number in the account record in order to enable OTA PIN verification,” (Dua ¶[0408].) where an E.164 phone number is previously provided through the wireless device. *See* Dua ¶[0056].

239. Under the **External-Storage Theory**, Dua discloses that the external storage is setup by to store and provide access to credentials and transaction receipts. “[T]he wallet application registers an external wallet storage service as an ‘extension’ within the wallet application on the wireless device.” Dua ¶[0491]. For instance, “[d]uring the storage setup process, the storage server will establish a valid username/password for the wallet application to automatically access the storage area.” Dua ¶[0492]. Then, “[t]he user is then free to use the wallet menu to select stored credentials or profiles to facilitate a transaction” (*function for conducting the*

*financial transaction*). Dua ¶[0495]. Further, “even electronic receipts... are stored in the external storage service, and made available for use by the wireless device” (*function for conducting the financial transaction*). Dua ¶[0495]. Setting up external storage for the wallet application constitutes “*enabling ... function[s] for conducting ... financial transaction[s]*” because providing access to credentials used in transactions.

**(f) Claims 6-16**

240. In my opinion, claims 6-16 are substantively identical to claims 1-5. The differences are immaterial. Claims 6-10 are directed to “[a] device that is configured to perform operations,” whereas claims 1-5 are directed to “[a] method of operating a device.” This distinction is immaterial since Dua discloses both methods and systems. Dua at Title.

241. In my opinion, independent claims 11 and 14 is substantively identical to independent claim 1 incorporated with dependent claims 3 and 4. And dependent claims 12-13 and 15-16 are substantively identical to dependent claims 2 and 5. Claims 11-13 are directed to “[a] method of operating a wireless device,” and claims 14-16 are directed to “[a] wireless device that is configured to perform operations,” whereas claims 1-5 are directed to “[a] method of operating a device.” These distinctions are immaterial since Dua is directed to a “wireless device,” and discloses both methods and systems. *E.g.*, Dua Title, Abstract.

**(g) Claim 17**

- (i) 17[pre]:** *The wireless device of claim 14, wherein said conducting the financial transaction by paying for a product comprises:*

242. As addressed in Sections V.B.2.a and V.B.2.c-d, it is my opinion that Jain discloses limitation 17[pre].

- (ii) 17[a]:** *establishing by the wireless device a short-range wireless link with the entity;*

243. In my opinion, Dua discloses limitation 17[a]. Dua discloses the wireless device establishing “a short range wireless link with [a]” point-of-sale terminal (*i.e.*, “*establishing by the wireless device a short-range wireless link with the entity*”). Dua Abstract. “The wallet application ... support[s] peer-to-peer connectivity to a device in close proximity,” such as “[c]onnectivity between the wireless device and ... POS terminal.” Dua ¶[0318]. And “[c]onnectivity could initially be established by exchanging encryption key” (*i.e.*, “*establishing by the wireless device a short range wireless link*”). Dua ¶[0318].

- (iii) 17[b]:** *wirelessly transmitting information to the entity using unlicensed frequencies; and*

**17[c]:** *wirelessly receiving information from the entity using unlicensed frequencies;*

**17[d]:** *wherein said wirelessly transmitting and said wirelessly receiving comprises using a time domain duplex protocol; and*

244. In my opinion, Dua discloses limitations 17[b]-[d]. To execute a transaction, Dua's wireless device "*wirelessly transmit[s]*" credential "*information*" to a point-of-sale terminal (*i.e.*, "*entity*"). Dua Abstract, ¶¶[0352], [0353]. The point-of-sale terminal responds by transmitting back an indication of a "successful transmission of credentials to [the] reader" after a transaction is complete (*i.e.*, "*wirelessly receiving information from the entity*"). Dua ¶¶[0364]-[0365]; *see also* Dua ¶¶[0015], [0041], [0293]. The wireless device and point-of-sale terminal use short range wireless communication, such as NFC and Bluetooth (*i.e.*, "*using unlicensed frequencies*"), to perform these transmissions. Dua Abstract, ¶¶[0016], [0318].

245. NFC uses unlicensed frequencies. Frequencies labeled as ISM— industrial, scientific, and medical—are "*unlicensed.*" NFC operates at 13.56MHz. EX1031. The frequency of 13.56MHz is an ISM frequency. EX1032 at 2.

246. Indeed, Patent Owner agrees. In its Infringement Contentions, Patent Owner alleges that "NFC operates at the globally unlicensed 13.56 MHz frequency." EX1016 at 313.

247. Similarly, Bluetooth also uses unlicensed frequencies. Specifically, "Bluetooth technology operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHz." EX1041.

248. Further, “NFC systems can take place as [a] half ... duplex system” (i.e., “*time domain duplex protocol*”). EX1032 at 21. Patent Owner agrees with this mapping: “NFC, a short-range half duplex communication technology,” uses “*time domain duplex protocol*.” EX1016 at 310-14.

249. Bluetooth is also a “*time domain duplex protocol*.” Not unlike NFC, Bluetooth can operate on half-duplex. See EX1038 at 1.

- (iv) 17[e]: *wherein said establishing by the wireless device a short-range wireless link with the entity comprises establishing the short-range wireless link with the entity responsive to the wireless device satisfying the proximity condition relative to the entity and responsive to the wireless device sensing the parameter and determining that the value associated therewith satisfies the threshold criterion.*

250. In my opinion, Dua discloses limitation 17[e]. As discussed with limitations 17[pre]-[a], Dua discloses or renders obvious that “*paying for a product comprises establishing by the wireless device a short-range wireless link with the entity*.” As discussed with limitation 4[a], Dua discloses or renders obvious that “*paying for a product*,” including “*establishing*” an NFC connection between the wireless device and POS terminal, is “*responsive to the device satisfying a proximity condition relative to an entity and responsive to the device sensing the parameter and determining the value that is associated with parameter that is sensed satisfies the threshold criterion*.”

**(h) Claim 18**

**(i) 18[pre]: *The wireless device of claim 14,***

251. As addressed in Sections V.B.2.a and V.B.2.c-d, it is my opinion that Jain discloses limitation 18[pre].

**(ii) 18[a]: *wherein said requesting from a second device an authorization to enable a function for conducting a financial transaction and/or said receiving from the second device the authorization to enable the function for conducting the financial transaction comprises:***

252. It is my opinion that Dua discloses limitation 18[a]. Limitation 18[a] repeats language found in claim 14, also found in limitations 3[a]-[c] and addressed above.

**(iii) 18[b]: *establishing by the wireless device a link with the second device, comprising a wireless link that comprises a distance that is greater than a distance associated with the proximity condition;***

253. In my opinion, Dua discloses limitation 18[b]. Dua's wireless device establishes a connection with the WCM and external storage through SIP, under the **Card-Issuing Theory** and **External-Storage Theory**, respectively. "The ... SIP architecture ... establish[es] direct communication between ... WCM and wallet application ... for ... transferring ... credentials" (*i.e.*, "***establishing by the wireless device a link with the second device***"). Dua ¶¶[0128], [0178], FIGS. 3-4. A "real-time connection is initiated between the wallet application and the storage service" by "utiliz[ing] SIP" (*i.e.*, "***establishing by the wireless device a link with the second***").

*device*”). Dua ¶¶[0494]-[0495]. A connection established through SIP can entail several servers and various electronic communication protocols such as cellular wireless technology (*e.g.*, “2.5G” and “3G”) and “Wi-Fi.” *E.g.*, Dua ¶[0104], FIG 3.

254. Connections between a wireless device and WCM or external storage occur over a greater distance than the “short range wireless link” established with NFC between the wireless device and POS terminal (*i.e.*, “***distance that is greater than a distance associated with the proximity condition***”). For instance, a POSITA would understand that a single cellular transmission to a base station (*e.g.*, at the top of a cell tower), let alone the separate transmissions between servers to reach a WCM or external storage, is a greater distance than the “short range wireless link” established with NFC.

(iv) 18[c]: ***wirelessly transmitting information to the second device over said wireless link using unlicensed and/or licensed frequencies; and***

18[d]: ***wirelessly receiving information from the second device over said wireless link using unlicensed and/or licensed frequencies;***

255. In my opinion, Dua discloses limitations 18[c]-[d]. As discussed with limitation 18[b], Dua’s wireless device communicates with the WCM and external storage through cellular wireless technology (*e.g.*, “2.5G” and “3G”) and “Wi-Fi” (*i.e.*, “***wirelessly transmitting information to the second device over said wireless***

*link*”) (i.e., “*wirelessly receiving information from the second device over said wireless link*”). See Dua ¶[0104]. Cellular wireless technology/protocols 2.5G and 3G “*us[e] ... licensed frequencies,*” and WiFi “*us[es] unlicensed frequencies.*” To the extent said technology/protocols do not use the corresponding licensed/unlicensed frequency, said technology/protocols use the other frequency and still satisfy “*using unlicensed and/or licensed frequencies.*”

- (v) **18[e]:** *wherein said wirelessly transmitting and/or said wirelessly receiving comprises using an orthogonal frequency division multiplexing and/or orthogonal frequency division multiple access protocol; and*

256. In my opinion, Dua discloses this limitation. As discussed with limitations 18[c] and 18[d], Dua discloses the wireless device using Wi-Fi or cellular wireless technology to communicate with the WCM and external storage, including “GSM/GPRS, CDMA2000, W-CDMA, EDGE, HDR, 1xRTT, UMTS, IMT-2000, 802.11a, 802.11b, 802.11g,... or other relevant protocols developed hereinafter.” Dua ¶¶[0041], [0104]. WiFi protocols “802.11a” and “802.11g” “*us[e] ... orthogonal frequency division multiplexing.*” Dua ¶[0041]; EX1043; EX1044.

257. A POSITA would also be motivated to use the most advanced and performant cellular radio technologies such as LTE and WiMAX (a competitor to LTE) (also known as 4G cellular technologies), well-known next generation technologies for cellular communications, in addition to the cellular technologies

IPR of U.S. Patent No. 11,770,756

Decl. of Dr. Kevin Almeroth

and protocols explicitly mentioned in Dua to keep up with ever-evolving technologies that allow for higher data rates. As of the priority date of the '756 Patent, LTE and WiMAX were known to a POSITA, and known to be displace older technologies in the near future. EX1045; EX1046. Wi-Max and LTE “*us[e]... orthogonal frequency division multiplexing and/ orthogonal frequency division multiple access protocol.*”

- (vi) **18[f]:** *wherein said establishing by the wireless device a link with the second device comprises establishing the link with the second device responsive to the wireless device sensing the parameter and determining that the value sensed satisfies the threshold criterion.*

258. In my opinion, Dua discloses limitation 18[f]. This limitation requires that the “*establishing*” of limitation 18[b] is performed that in response to the “*sensing the parameter,*” “*determining ... the value,*” and “*satisf[ying] the threshold*” of limitations 14[a]-[b]. The discussion of Dua’s disclosure of limitation 1[c] applies here.

259. Under the **Card-Issuing Theory** and **External-Storage Theory**, scanning a valid fingerprint causes the wireless device to open the wallet application and establish a connection with WCM and external storage, respectively.

## **VI. Secondary Considerations of Non-Obviousness**

260. 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.

261. In my opinion, there is a lack of commercial success for any product practicing the '756 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 '756 patent and the prior art is minimal, and any secondary considerations would have minimal impact on the invalidity analysis.

262. In my opinion, there was no long-felt, unresolved need met by the '756 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 '756 Patent. To the extent wide-scale deployment in the United States post-dated the '756 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 '756

IPR of U.S. Patent No. 11,770,756

Decl. of Dr. Kevin Almeroth

priority date. *See, e.g.*, Section IV. 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**

263. 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.


IPR of U.S. Patent No. 11,770,756  
Decl. of Dr. Kevin Almeroth

\* \* \*

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,

Date: May 2, 2025

  
Kevin C. Almeroth, Ph.D.