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. 11,937,172

"Systems/Methods Of A Two-Step Process In Establishing A Capability, And Using The Capability, To Execute A Financial Transaction By A Smartphone"

DECLARATION OF KEVIN ALMEROTH, PH.D., IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 11,937,172

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 '172 Patent....14
A. Priority Date....14
B. Specification....15
C. Prosecution History....17
1. Prosecution History of the '172 Patent (EX1014)....17
2. '411 Patent File History....17
3. '708 Patent File History....19
4. '199 Patent File History....20

5. '015 Patent File History (Unasserted) 21

6. '432 Patent File History 22

7. '118 Patent File History (Unasserted) 23

8. '756 Patent File History 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. Ground 1: Jain (EX1017) 39

1. Background 39

2. Analysis 45

B. Ground 2: Dua (EX1018) 97

1. Background 97

2. Analysis 102

VI. Secondary Considerations of Non-Obviousness 149

VII. Conclusion 150

LIST OF EXHIBITS

Exhibit	Description
EX1001	U.S. Patent No. 11,937,172 ("'172 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 '172 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. Pub. No. 2010/0082490
EX1021	U.S. Pub. No. 2009/0307140
EX1022	"Product Overview", Vivotech (Jun. 27, 2007), https://web.archive.org/web/20070627155330/ http://www.vivotech.com/products/vivo_pay/index.asp

Exhibit	Description
EX1023	"Kyocera Wireless Mobile Phones Excel in Cellular South WirelessWallet Consumer Trial", Kyocera (Oct. 18, 2007), https://americas.kyocera.com/press-releases/press-releases_201503201874.htm
EX1024	U.S. Pub. No. 2005/0137977
EX1025	U.S. Pub. No. 2001/0026632
EX1026	NTT DoCoMo FOMA F900iC Basic Manual
EX1027	Jain et al., "An Identity-Authentication System" (Sep. 1997)
EX1028	U.S. Patent No. 6,957,339
EX1029	Jin et al., "Biohashing: two factor authentication featuring fingerprint data and tokenised random number" (Apr. 27, 2004)
EX1030	Bhargav-Spantzel, "Privacy Preserving Multi-Factor Authentication with Biometrics" (2006)
EX1031	"About NFC Technology", NFC Forum (Jun. 15, 2006), https://web.archive.org/web/20060615050709/http://www.nfc-forum.org/aboutnfc/about_nfc_technology/
EX1032	Erik Rolf & Viktor Nilsson, "Near Field Communication (NFC) for Mobile Phones" (Aug. 2006)
EX1033	Wall Street Journal, Vivotech (Aug. 12, 2005), https://web.archive.org/web/20060915080521if_/http://www.vivotech.com:80/newsroom/coverage/Videos/Wall_Street_Journal/Wall_Street_Journal.wmv
EX1034	Near Field Communication - Interface and Protocol (NFCIP-1), Standard ECMA-340 (December 2002)
EX1035	NFC Forum News Conference, NFC Forum (June 5, 2006)
EX1036	Dean A. Gratton, "Developing Practical Wireless Applications", Elsevier Digital Press (2007)
EX1037	Jacki Katzman, "NFC Forum Unveils Technology Architecture and Announces Initial Specifications and Mandatory Tag Format Support", NFC Forum, at 3 (June 5, 2006)

Exhibit	Description
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), https://datatracker.ietf.org/doc/html/rfc793
EX1041	"Bluetooth Basics", Bluetooth (Apr. 23, 2006), https://web.archive.org/web/20060423011921/http://www.bluetooth.com/Bluetooth/Learn/Basics/
EX1042	"iPhone Premieres This Friday Night at Apple Retail Stores", Apple (Jun. 28, 2007), https://www.apple.com/newsroom/2007/06/28iPhone-Premieres-This-Friday-Night-at-Apple-Retail-Stores/

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 1-16 ("the challenged claims") of U.S. Patent No. 11,937,172 ("the '172 patent"). I have been asked by the Petitioner to assist in evaluating the claims and the disclosure of the '172 patent.

A. Qualifications

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

1. Educational Background

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

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

2. Career

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. Other Relevant Qualifications

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

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

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

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

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

B. Previous Expert Witness Testimony

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

C. Preparation for this Declaration

22. In forming my opinions, I have considered the '172 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 '172 patent (a "POSITA"). My understanding of "POSITA" and "priority date" are set forth below. I have also reviewed the file history of the '172 patent, the Exhibits that are listed in the list of Exhibits, and any other material cited in this declaration.

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

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

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

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

26. Throughout this declaration, I refer to specific pages of the '172 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 '172 Patent

33. The '172 patent is titled "Systems/methods of a two-step process in establishing a capability, and using the capability, to execute a financial transaction by a smartphone."

34. The '172 patent lists inventors Peter D. Karabinis and Rajendra Singh.

35. The '172 patent was filed as U.S. Patent Application No. 18/523,863 on Nov. 29, 2023, and issued on March 19, 2024.

A. Priority Date

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

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

B. Specification

38. The specification assumes familiarity with a "wireless communications device" such as "a wireless terminal, a wireless/mobile phone, a Personal Digital Assistant (PDA), a smart phone, a multi-media device including Global Positioning System (GPS) capability, etc." EX1001 at 3:17-21. It further relies on long-established, generic concepts of computer systems such as "authorization" (5:48-50 et seq.), "sensors" capable of detecting, inter alia, physiological input (mentioned only at 6:17-34), "short-range communications" (mentioned in the specification only at 8:29-34 and 8:56-65), "air interface[s]" (6:63-64 et seq., with a recitation of then-existing interfaces at 7:21-31), and "communications service[s]" (9:10 et seq.). For example, the specification acknowledges that the "adaptivity and mobility aspects of wireless communications" were already "important in people's lives" at the time of alleged invention. EX1001 at 1:39-40. It also assumes, in the "Background of the Invention" section, that mobile phones could act as digital wallets. *See* EX1001

at 1:49-52. The specification does not disclose or purport to disclose new or improved means of sensing (including physiological/biometric sensing) or proximity detection.

39. At the heart of the disclosure is a mobile wireless device (element 14 in Figure 1) that "may be configured to enable one or more modes/functions" of itself or of another device "responsive to a proximity criterion having been satisfied." EX1001 at 3:17-26. The proximity criterion is a measure of how close the wireless device (or the second device) is to an "entity" such as a person, product for sale, or POS terminal. EX1001 at 3:27-41, 3:55-63. For example, the device may determine proximity using well knowns means such as detecting a low-power or short range signal radiated from a (third) device (element 16 in Figure 1) that is part of or associated with the entity. *See* EX1001 at 3:42-45, 3:64-4:24.

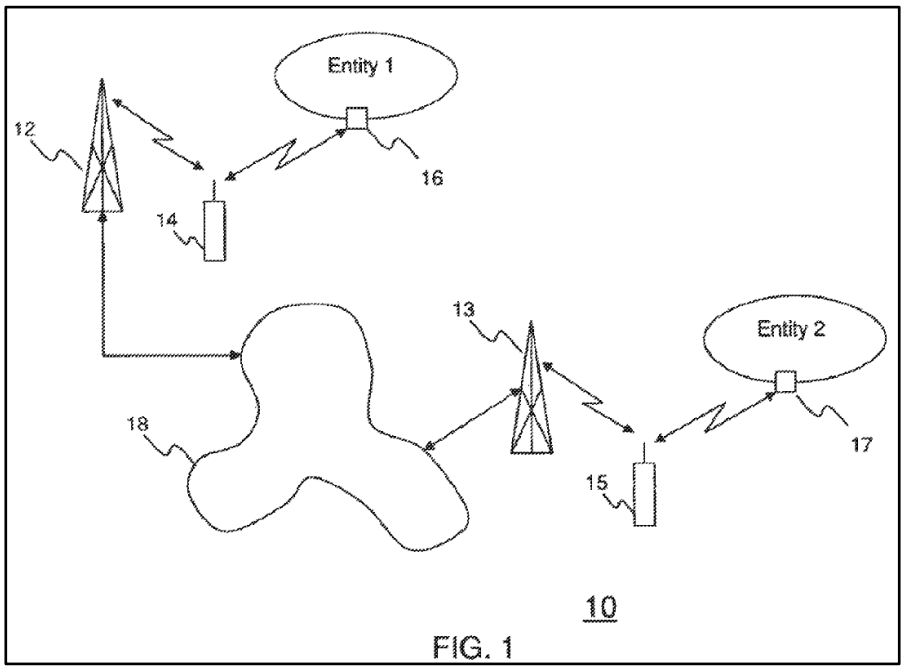


FIG. 1

C. Prosecution History

1. Prosecution History of the '172 Patent (EX1014)

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

2. '411 Patent File History

41. 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").

42. 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.").

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

44. 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.

45. 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.

3. '708 Patent File History

46. 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.

47. 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.

48. 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.

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

4. '199 Patent File History

50. 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.

51. 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.

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

53. 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.

54. 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.

5. '015 Patent File History (Unasserted)

55. 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.

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

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

6. '432 Patent File History

58. 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.

59. 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.

60. Additionally, the Examiner rejected the claims as obvious. EX1009 at 72, 169. Applicant substantially amended the claims in response. EX1009 at 154, 242. Specifically, the Examiner rejected all of the pending claims "under 35 U.S.C. 103 as being unpatentable over Dua (US 2006/0165060), hereinafter 'Dua', in view of Creamer et al (US 2004/0143550), hereinafter 'Creamer.'" EX1009 at 169. The Applicant amended claims 1 and 5, attempting to avoid Dua with the limitation of "responsive to at least one physiological parameter having been sensed by at least one sensor of the smartphone, enabling a mode to communicate by the smartphone information requesting an authorization; while the mode is enabled." EX1009 at 275-276.

7. '118 Patent File History (Unasserted)

61. 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.

62. 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.

63. 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.

8. '756 Patent File History

64. 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.

65. 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.

66. 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.

67. 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.

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

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

69. 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.

70. 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.

71. 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

72. 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.

73. 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.

74. 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

75. 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.

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

D. Level of Ordinary Skill in the Art

77. 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.

78. 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.

79. In my opinion, a person of ordinary skill in the art at the time of the '172 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.

80. 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

81. 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.

82. 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.

83. 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

84. 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 smartphone in performing at least one financial transaction; the method including a two-step process in establishing and using a capability in order to perform said at least one financial transaction; the method comprising:
1[a]	responsive to sensing at least one parameter by at least one sensor of the smartphone and responsive to determining that the at least one parameter that is sensed satisfies a criterion, performing a first step of said two-step process by enabling a mode to communicate by the smartphone information requesting an authorization to establish said capability;
1[b]	while the mode is enabled, and as a precursor to performing a second step of said two-step process, transmitting by the smartphone first data to a first device requesting the authorization to establish said capability to perform said at least one financial transaction; and
1[c]	receiving by the smartphone second data from the first device, comprising the authorization, responsive to said transmitting by the smartphone the first data; then
1[d]	performing the second step of said two-step process comprising performing a first transaction of said at least one financial transaction, responsive to detecting by the smartphone that a proximity condition is satisfied and responsive to sensing the at least one parameter and

Claim	Limitation
	determining that the at least one parameter sensed satisfies the criterion;
1[e]	wherein said performing the second step of said two-step process comprises sensing that the proximity condition is satisfied relative to an access point maintained by a vendor at a point of purchase counter, by detecting a short-range signal that is transmitted by the access point, determining that a value of the at least one parameter that is sensed satisfies the criterion and then, responsive to having sensed that the proximity condition is satisfied relative to the access point and having determined that the value of the at least one parameter sensed satisfies the criterion, paying for a product by selectively sending information to at least one device;
1[f]	wherein said paying for a product by selectively sending information to at least one device comprises selectively and wirelessly transmitting information to the at least one device using unlicensed frequencies; and
1[g]	wherein said at least one parameter comprises a signal, a number, a word, a code, 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.
2[pre]	The method of claim 1,
2[a]	wherein said enabling a mode to communicate by the smartphone information requesting an authorization comprises enabling a first function of the smartphone while disabling a second function of the smartphone responsive to the at least one parameter having been sensed by the at least one sensor of the smartphone and further responsive to having determined that the at least one parameter that is sensed satisfies the criterion; and
2[b]	then selectively communicating with the first device by using a communications capability of the first function, selectively establishing a master-slave relationship with the first device, and selectively requesting from the first device the authorization to

Claim	Limitation
	establish the capability to conduct said at least one financial transaction.
3[pre]	The method of claim 2, further comprising:
3[a]	repeatedly sensing the at least one parameter and repeatedly deciding, based on comparing a value of the at least one parameter sensed to the criterion, whether or not to maintain enabled said first function while maintaining disabled said second function; and
3[b]	maintaining enabled said first function while maintaining disabled said second function responsive to deciding that said value of the at least one parameter continues to satisfy the criterion; or
3[c]	disabling said first function and enabling said second function responsive to deciding that the value of the at least one parameter no longer satisfies the criterion.
4[pre]	The method of claim 1,
4[a]	wherein said transmitting by the smartphone first data to a first device is responsive to the at least one parameter having been sensed by the at least one sensor of the smartphone and is further responsive to having determined that the at least one parameter that is sensed satisfies the criterion; and
4[b]	wherein said receiving by the smartphone second data from the first device is responsive to said transmitting by the smartphone the first data and comprises receiving by the smartphone information relating to an acknowledgement and/or authorization to establish and use the capability to perform said at least one financial transaction.
5[pre]	The method of claim 1, further comprising:
5[a]	responsive to performing a financial transaction, causing data to be transmitted selectively to at least one device and further causing data to be received selectively from at least one device.
6[pre]	The method of claim 1,

Claim	Limitation
6[a]	wherein said transmitting by the smartphone first data to a first device and receiving by the smartphone 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.
7[pre]	The method of claim 1,
7[a]	wherein said paying for a product further comprises deducting/withdrawing an amount of money from an account.
8[pre]	The method of claim 7,
8[a]	wherein said using unlicensed frequencies comprises using unlicensed frequencies in a Time Division Duplex operation;
8[b]	wherein said selectively sending information to at least one device comprises selectively, sending information to the access point maintained by the vendor at the point of purchase counter and to at least one other device that is predetermined; and/or
8[c]	wherein the method further comprises selectively receiving information from the access point maintained by the vendor at the point of purchase counter and from at least one other device that is predetermined.
9[pre]	A smartphone that is configured to perform operations, comprising a two-step process, associated with establishing and using a capability in order to perform at least one financial transaction; the operations comprising:
9[a]	responsive to sensing at least one parameter by at least one sensor of the smartphone and responsive to determining that the at least one parameter that is sensed satisfies a criterion, performing a first step of said two-step process by enabling a mode to communicate information requesting an authorization to establish said capability;

Claim	Limitation
9[b]	while the mode is enabled, and as a precursor to performing a second step of said two-step process, transmitting first data to a first device requesting the authorization to establish said capability to perform said at least one financial transaction; and
9[c]	receiving second data from the first device, comprising the authorization, responsive to said transmitting the first data; then
9[d]	performing the second step of said two-step process comprising performing a first financial transaction of said at least one financial transaction, responsive to detecting by the smartphone that a proximity condition is satisfied and responsive to sensing the at least one parameter and determining that the at least one parameter sensed satisfies the criterion;
9[e]	wherein said performing the second step of said two-step process comprises sensing that the proximity condition is satisfied relative to an access point maintained by a vendor at a point of purchase counter, by detecting a short-range signal that is transmitted by the access point, determining that a value of the at least one parameter that is sensed satisfies the criterion and then, responsive to having sensed that the proximity condition is satisfied relative to the access point and having determined that the value of the at least one parameter sensed satisfies the criterion, paying for a product by selectively sending information to at least one device;
9[f]	wherein said paying for a product by selectively sending information to at least one device comprises selectively and wirelessly transmitting information to the at least one device using unlicensed frequencies; and
9[g]	wherein said at least one parameter comprises a signal, a number, a word, a code, 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.
10[pre]	The smartphone of claim 9,

Claim	Limitation
10[a]	wherein said enabling a mode to communicate by the smartphone information requesting an authorization comprises enabling a first function of the smartphone while disabling a second function of the smartphone responsive to the at least one parameter having been sensed by the at least one sensor of the smartphone and further responsive to having determined that the at least one parameter that is sensed satisfies the criterion; and
10[b]	then selectively communicating with the first device by using a communications capability of the first function, selectively establishing a master-slave relationship with the first device, and selectively requesting from the first device the authorization to establish the capability to conduct said at least one financial transaction.
11[pre]	The smartphone of claim 10, wherein the operations further comprise:
11[a]	repeatedly sensing the at least one parameter and repeatedly deciding, based on comparing a value of the at least one parameter sensed to the criterion, whether or not to maintain enabled said first function while maintaining disabled said second function; and
11[b]	maintaining enabled said first function while maintaining disabled said second function responsive to deciding that said value of the at least one parameter continues to satisfy the criterion; or
11[c]	disabling said first function and enabling said second function responsive to deciding that the value of the at least one parameter no longer satisfies the criterion.
12[pre]	The smartphone of claim 9,
12[a]	wherein said transmitting first data to a first device is responsive to the at least one parameter having been sensed by the at least one sensor of the smartphone and is further responsive to having determined that the at least one parameter that is sensed satisfies the criterion; and

Claim	Limitation
12[b]	wherein said receiving by the smartphone second data from the first device is responsive to said transmitting by the smartphone the first data and comprises receiving by the smartphone information relating to an acknowledgement and/or authorization to establish and use t capability to perform said at least one financial transaction.
13[pre]	The smartphone of claim 9, wherein the operations further comprise:
13[a]	responsive to performing a financial transaction, causing data to be transmitted selectively to at least one device and further causing data to be received selectively from at least one device.
14[pre]	The smartphone of claim 9,
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.
15[pre]	The smartphone of claim 9,
15[a]	wherein said paying for a product further comprises deducting/withdrawing an amount of money from an account.
16[pre]	The smartphone of claim 9,
16[a]	wherein said using unlicensed frequencies comprises using unlicensed frequencies in a Time Division Duplex operation;
16[b]	wherein said selectively sending information to at least one device comprises selectively sending information to the access point maintained by the vendor at the point of purchase counter and to at least one other device that is predetermined; and/or
16[c]	wherein the operations further comprise selectively receiving information from the access point maintained by the vendor at the

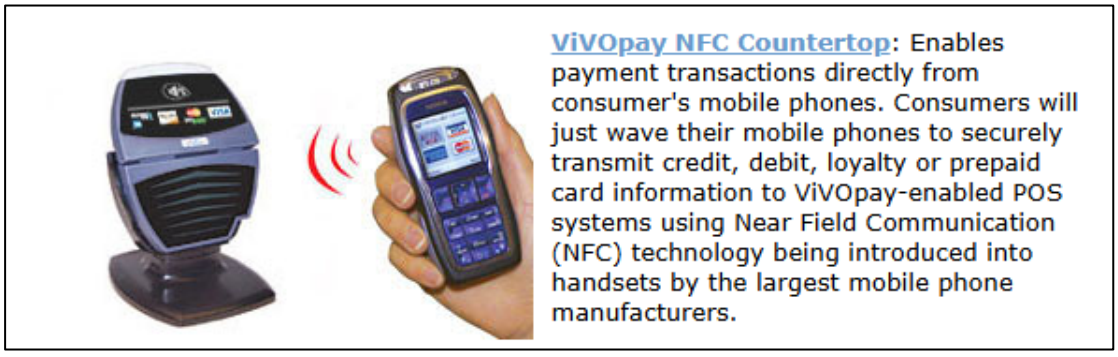
Claim	Limitation
	point of purchase counter and from at least one other device that is predetermined.

IV. State of the Art

85. As the ’172 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 1:60-2:19. 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.

86. 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.

87. 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:

88. As mobile phones (which were evolving into smartphones) were increasingly used for sensitive activities (*e.g.*, financial transactions) and to store sensitive user data (*e.g.*, payment account information), mobile phone security received industry attention. One security mechanism that gained popularity in the early 2000s was biometric authentication. By the early 2000s, fingerprint scanners were routinely integrated into mobile phones, such as the 2000 SAGEM MC 959, the 2003 Fujitsu F505i, the 2004 Pantech GI100, and the 2007 Toshiba G500 and G900. For example, the 2007 Kyocera and MasterCard trial used mobile phones with fingerprint scanners and required biometric authentication. EX1023**Error! 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)	1-16

2	§103	Dua (U.S. Pat. Appl. Pub. No. 2006/0165060)	1-16

A. Ground 1: Jain (EX1017)

1. Background

89. 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 '172 patent under at least pre-AIA 35 U.S.C. § 102(e).

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

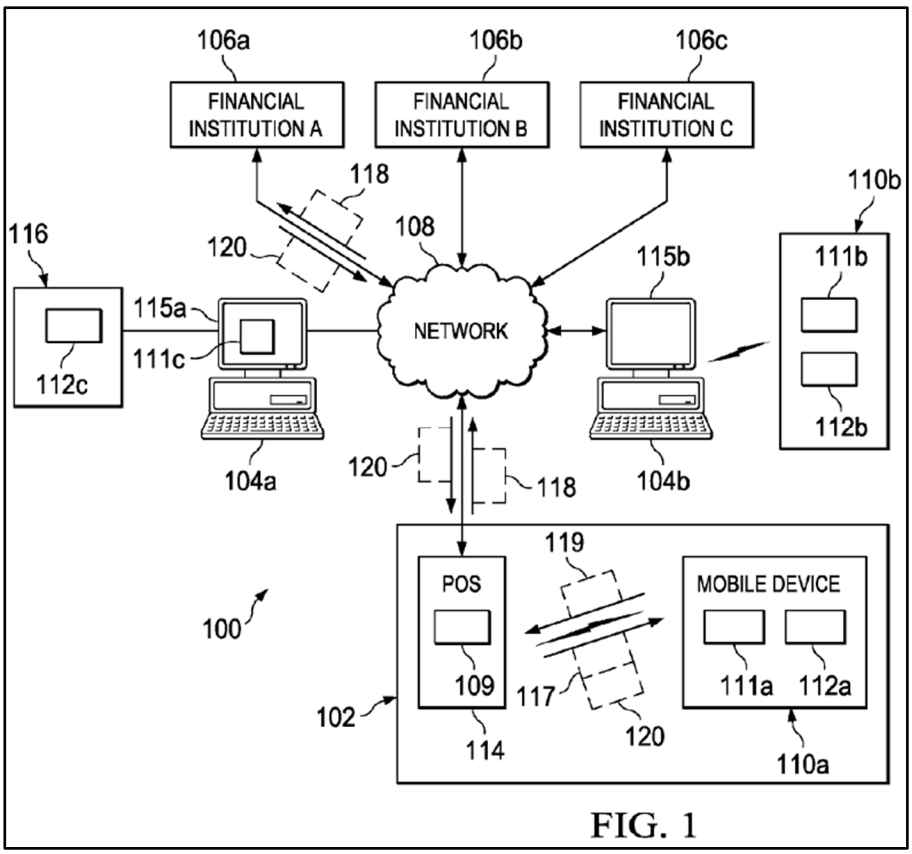
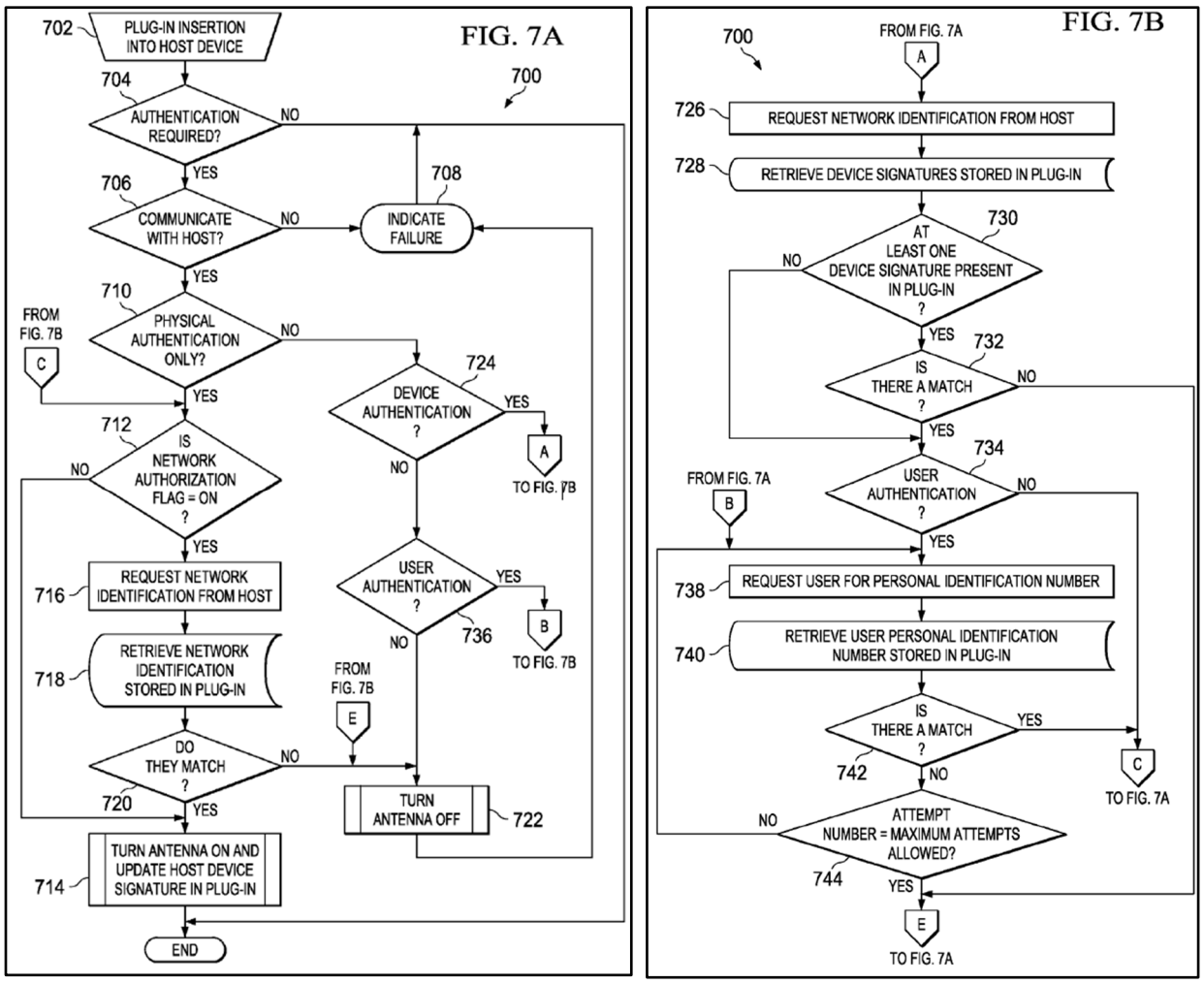


FIG. 1

91. 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].

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



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

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

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

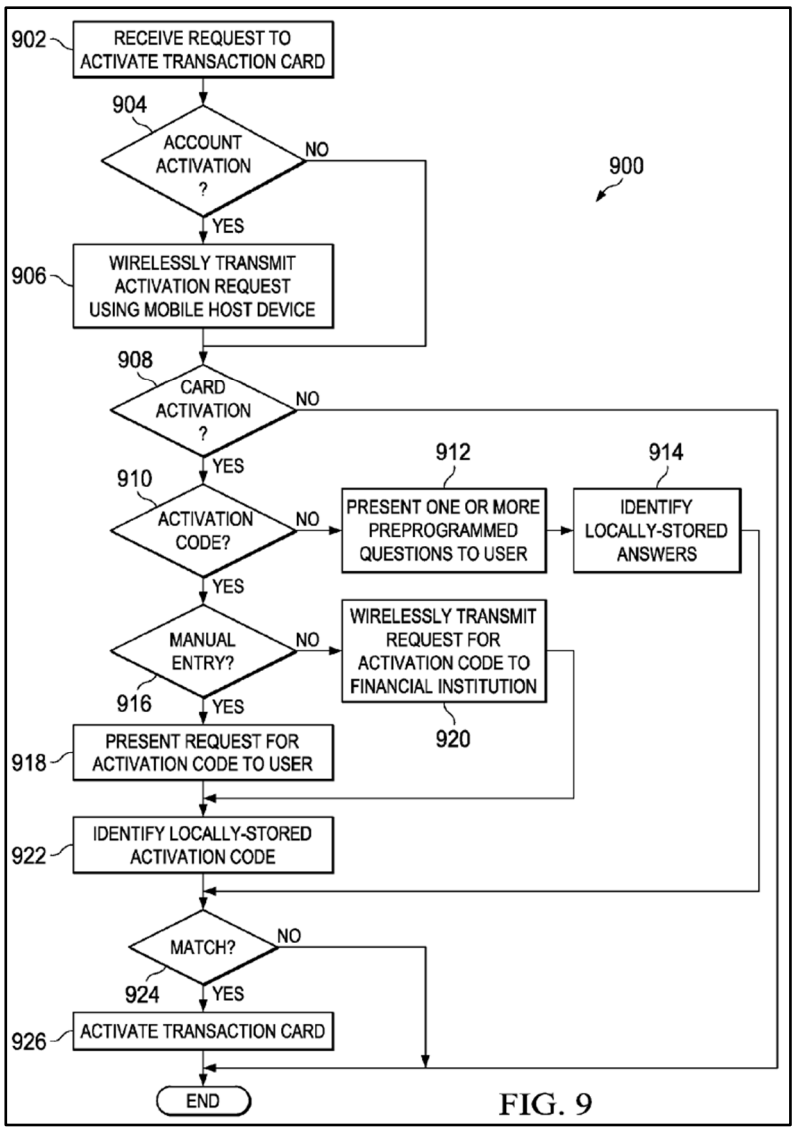


FIG. 9

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

2. Analysis

(a) Claim 1

(i) 1[pre][i]: *A method of operating a smartphone in performing at least one financial transaction;*

95. In my opinion, Jain discloses this limitation. Jain describes operating a "mobile device 110." Jain ¶¶[0005], [0019], [0021], [0029], FIG.1. Mobile device 110 can be a smartphone. Jain ¶¶[0005], [0018], [0021], FIG. 1. Mobile device 110 can include a "transaction card 112" attached thereto or incorporated therein (*e.g.*, via " active-card-emulation mode") to "wirelessly execut[e] transactions" with retail point-of-sale terminal 114. *See* Jain ¶¶[0005], [0019], [0021], [0029]. Further, a POSITA would understand would understand that transaction card 112 can be a more non-removable part of the smartphone. Transaction card 112 can be "software, hardware, and/or firmware," and "mobile device 110 does not require additional hardware, software, and/or firmware." Jain ¶[0023]; *see also* FIG. 1:

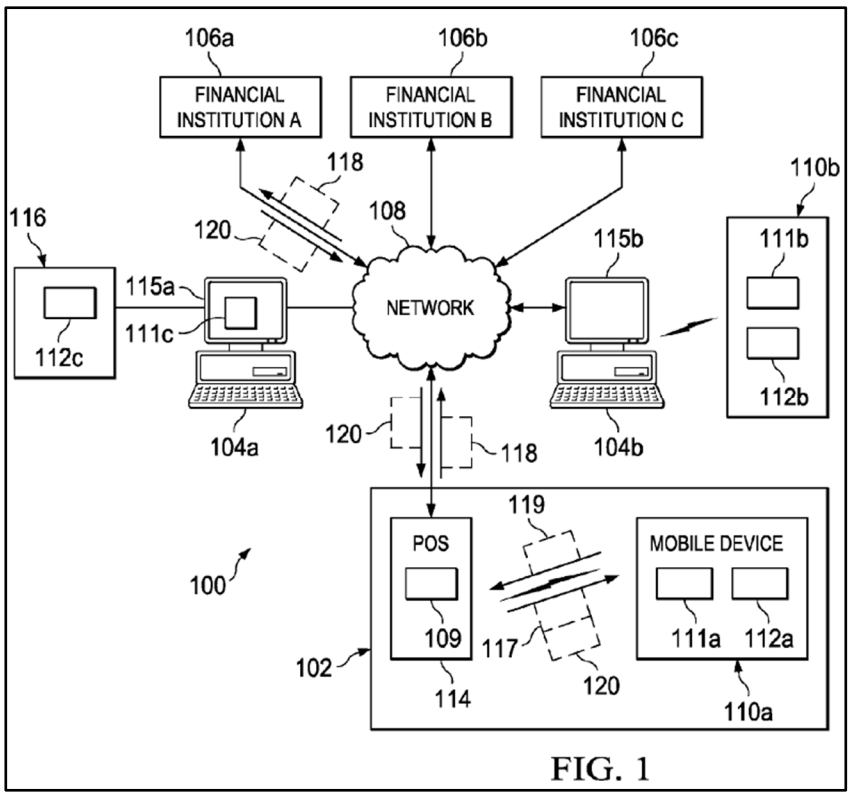


FIG. 1

96. Further, a POSITA would understand that transaction card 112 can be a permanent part of the smartphone. Transaction card 112 can be "software, hardware, and/or firmware," and "mobile device 110 does not require additional hardware, software, and/or firmware." Jain ¶[0023], Fig. 1.

97. Jain FIG. 1 provides an example of such wireless transactions, where a customer's mobile device 110a with transaction card 112a wirelessly execute transactions with a nearby POS device 114. Jain ¶[0019]. POS device 114 first transmits transaction request 117 to mobile device 110. Jain ¶[0027]. The mobile device 110 then sends a transaction response 119 that identifies information associated with a payment account. Jain ¶[0027]. The POS device 114 then sends

a transaction authorization request 118 to a financial institution 106 (shown as either 106a, 106b, or 106c). Jain ¶[0027]. The financial institution transmits authorization response 120 to the POS device 114, which in turn transmits it to mobile device 110. Jain ¶[0027]. This response 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 110 and POS device 114 uses short range signals such as NFC or Bluetooth. Jain ¶[0023].

98. Moreover, in my opinion, a POSITA would understand that Jain discloses, or otherwise renders obvious, a transaction card 112 integrated into mobile device 110 such that it is not readily separable. Integrating transaction card 112 improves the simplicity and efficiency of the design. Additional functionalities associated with an independent transaction card 112 and independent mobile device 110 are no longer needed. For instance, an additional translation or communication step between transaction card 112 and mobile device 110 (*see* Jain ¶¶[0023] ("[T]ransaction card 112 may execute … the following: … translat[ion] between wireless protocols and protocols compatible with the transaction card 112 [and] translate between transaction-card protocols and protocols compatible with mobile device 110 … ."), [0052] ("The API/UTI layer 304 can include any software, hardware, and/or firmware that operates as an API between the mobile device 110 and the transaction card 112.").) can be removed or otherwise simplified.

99. Removing additional functionalities also reduce the risk of errors. Each functionality provides one or more fault vectors. For instance, requiring transaction card 112 to wirelessly communicate with mobile device 110 allows for errors to occur in the transmission of the data. Jain ¶¶[0023] ("[T]ransaction card 112 may execute … the following: … translat[ion] between wireless protocols and protocols compatible with the transaction card 112 [and] translate between transaction-card protocols and protocols compatible with mobile device 110 … ."), [0052], FIG. 3. And because transaction card 112 can act as a standalone "desktop … unit," there are several potential areas of fault. Jain ¶[0029], FIG. 3 (listing as part of transaction card 112 "interface," "API+UI," "web server," "real-time framework," "payment applications," "value added applications," "user credentials," "real-time operating system," "contactless chipset," "antenna control functions," "antenna," "bank used memory," and "memory").

100. Further, transaction card 112 can leverage mobile device 110's resources or components. For instance, transaction card 112 can rely on mobile device 110, and still effectively be "implemented in the form of an industrial integrated circuit chip for mounting on a PCB" or "in the form of a self contained desktop standalone unit powered by external AC adapter" without the extra hardware, firmware, and software. Jain ¶[0029]. Otherwise, transaction card 112 is a whole separate self-contained desktop independent is bulky or otherwise unwieldy,

and seemingly redundant when a user also carries a smartphone. *See* Jain ¶¶[0018], [0029], [0052], FIG. 3 (depicting an example transaction card):

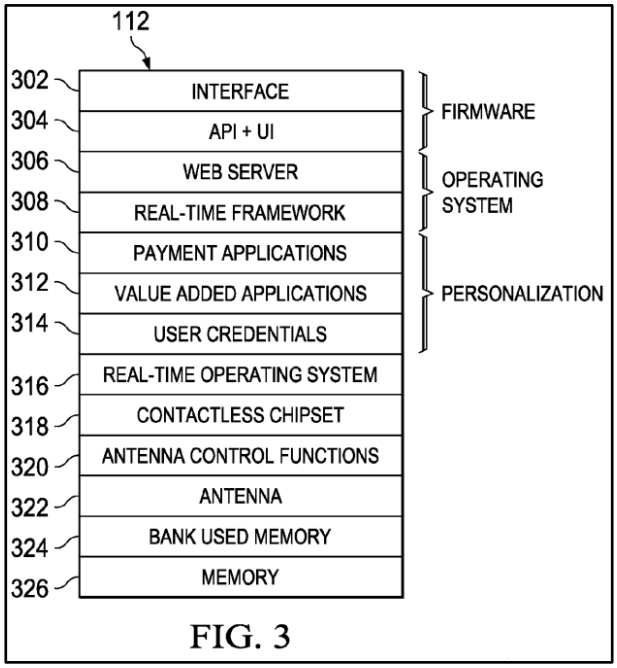


FIG. 3

Instead, transaction card 112 can use mobile device 110's power, processors, and memory.

101. Removability of the transaction card is also not always beneficial. For instance, from the perspective of a smartphone vendor, removability of the transaction card allows for modularity—allowing for a transaction card to be used with other smartphones, as opposed to being more proprietary to the smartphone vendor's smartphone. Further, integrating a transaction card 112 into mobile device 110 in a more permanent manner reduces the risk of losing the transaction card 112—either through inadvertent loss or theft. *See* Jain ¶[0033].

(ii) 1[pre][ii]: ***the method including a two-step process in establishing and using a capability in order to perform said at least one financial transaction; the method comprising:***

102. In my opinion, Jain discloses this limitation—the ***two-step process***. The first step of Jain's ***two-step process*** involves authenticating (*see* Jain ¶¶[0072]-[0075], FIG. 7.) and activating (*see* Jain ¶¶[0080]-[0081], FIG. 9.) a transaction card with an associated financial institution to ***establish … a capability in order to perform said at least one financial transaction***.

103. Specifically, in connection with Figure 7, Jain discloses an "automatic[] bootstrapping" process which includes "one or more authentication procedures" such as "user authentication." The bootstrapping/authentication procedure of the transaction card and smartphone must be completed before activating the card with the associated financial institution. Jain ¶¶[0070] ("the intelligent card may require device authentication **before** activation") (emphasis added), [0072] ("an intelligent card may execute one or more authentication procedures **prior to** activation") (emphasis added).

104. This would makes sense to a POSITA. It reduces the risk of fraud. Requiring an "automatic" "authentication procedure," like "user authentication," prior to activating the card prevents the unauthorized use of the transaction card and smartphone, thereby reducing the risk of fraud. *See* Jain ¶[0072], [0075].

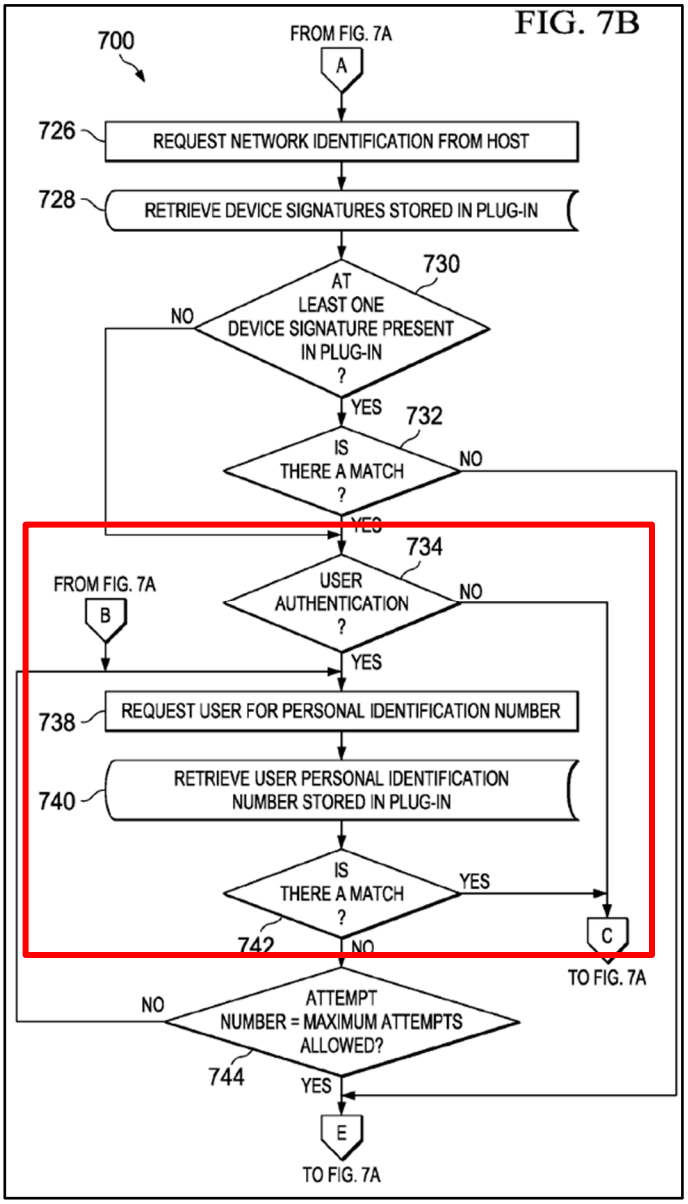
105. Further, in connection with Figure 9, Jain discloses that the smartphone transaction card is activated for transactions by transmitting a wireless communication request to activate the associated financial account with the financial institution. Jain ¶¶[0070], [0081]. This first ***establishing*** step is detailed in my analysis for limitations 1[a] -1[c] below.

106. The second step of Jain's ***two-step process*** is the use of the activated card for contactless transactions with the financial institution. Specifically, once activated, the smartphone is capable of performing transactions with a point-of-sale device. Jain ¶[0027]. For instance, Jain discloses performing transactions a nearby retail payment terminal POS 114 to pay for a product. *See* Jain ¶¶[0019], [0023]. Such POS terminals may be contactless-enabled terminals at merchants accepting financial transactions using various payment programs (*e.g.*, Mastercard, Visa, Amex, Discover). Jain at [0028]. This second step is detailed in my analysis for limitations 1[d] -1[f] below.

(iii) 1[a][i]: *responsive to sensing at least one parameter by at least one sensor of the smartphone and responsive to determining that the at least one parameter that is sensed satisfies a criterion,*

107. In my opinion, Jain discloses this limitation. Jain discloses an authentication process for "automatically bootstrapping" transaction card 112 to mobile device 110. Part of that authentication process includes authenticating a user

using a PIN number or biometrics (*e.g.*, fingerprint). *See* Jain ¶¶[0072], [0075], FIG. 7B at steps 734-742:



108. In my opinion, the PIN inputted by the user constitutes ***at least one parameter***. To ***sens***[***e***] the PIN, the smartphone's touch screen or keypad constitutes ***at least one sensor of the smartphone*** to ***sens***[***e***] the PIN. A POSITA would understand a touch screen or keypad as sensing touch, such as through a capacitive

touch screen. *See also* EX1042. And validating the PIN constitutes ***determining that the at least one parameter that is sensed satisfies a criterion***. Specifically, at step 738, the smartphone receives as user input a PIN via the smartphone's touch screen or keypad of GUI 111. Jain ¶¶[0022], [0075]. At step 740, the smartphone also retrieves a locally stored PIN. Jain ¶[0075]. Then, at step 742 ("is there a match?"), the smartphone determines whether the user-inputted PIN matches the locally-stored PIN—***satisfies a criterion***. Jain ¶[0075], FIG. 7B.

109. In addition, Jain discloses that rather than "entering a PIN," "the user may be authenticated using … biometric information (*e.g.*, fingerprint)." Jain ¶[0075]. In this case, in my opinion, the biometric information, such as a fingerprint, provided by the user constitutes ***at least one parameter***. The smartphone's biometric sensors, such as a fingerprint scanner, constitutes ***at least one sensor of the smartphone*** to ***sens***[***e***] the PIN. And validating the fingerprint constitutes ***determining that the at least one parameter that is sensed satisfies a criterion***. Specifically, for the previous discussion of Jain's steps 738, 740, and 742, the PIN can be substituted with biometric information, such as a fingerprint.

110. Thus, Jain discloses performing steps 738, 740, and 742, where step 738 includes sensing "biometric information" using a biometric sensor, step 740 includes retrieving locally stored biometric information, and step 742 includes

determining if the sensed biometric information matches the stored biometric information. Jain ¶[0075].

111. Further confirming that this limitation is met, Patent Owner alleges in its infringement contentions in the district court litigation that the use of biometric verification is itself sufficient to show ***sensing at least one parameter by at least one sensor of the smartphone*** and ***determining that the at least one parameter that is sensed satisfies a criterion***. EX1016 at 29-42.

112. It is also my opinion that, at a minimum, it would be obvious to implement Jain's teaching of "authentication using … biometric information" in this manner. Not unlike using a PIN, the purpose of biometric authentication is to ensure biometric information of a current user matches the biometric information of the rightful owner of the device. So, the biometric information of the current user must be compared against the biometric information of the rightful owner.

113. 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.

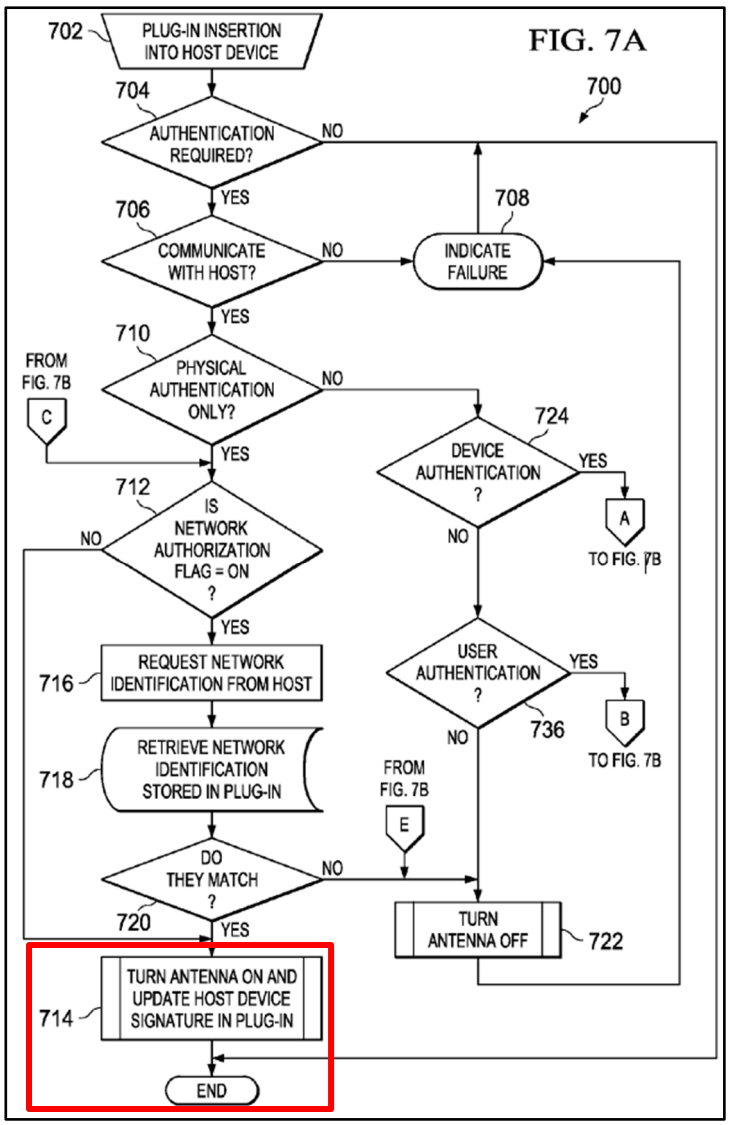
114. This type of implementation was well known to a POSITA, as indicated by the numerous prior art references describing it. *See, e.g.*, EX1026 at 196; EX1024 ¶¶[0009], [0025]; EX1025 ¶¶[0044], [0086]-[0092]; EX1021 ¶¶[0040]-[0042]. For instance, U.S. Pub. No. 2005/0137977 discloses a payment device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

to use the payment device to make a proximity payment. These field biometric measurements are internally compared with the previously recorded biometric profile of the authorized individual." EX1024 ¶[0009]. Similarly, EX1025 also discloses a portable telephone receiving biometric data and comparing that biometric data to locally stored biometric data of an authorized individual. EX1025 ¶¶[0044], [0086]-[0092].

(iv) 1[a][ii]: ***performing a first step of said two-step process by enabling a mode to communicate by the smartphone information requesting an authorization to establish said capability;***

115. In my opinion, Jain discloses this limitation. Jain's user authentication allows transaction card 112 to engage in the cellular radio communication required to actually activate the transaction card with a financial institution. Jain ¶[0072]. In other words, the user authentication allowing cellular radio communication constitutes ***enabling a mode to communicate by the smartphone***. And that communication requests activation of the transaction card with a financial institution, thereby constituting ***communicat*[*ing*] **. . . *information requesting an authorization to establish said capability***.

116. Specifically, in response to authenticating the user (in steps 738-744 of Fig. 7B), 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." *See* Jain ¶¶[0072]-[0075]:



See Jain, FIG. 7A (annotated).

117. If all authentication steps succeed, then the transaction card and smartphone are updated to store a host-device signature. Jain ¶[0073].

118. If the host-device signature is updated (as described in FIG. 7) to match the host device, the transaction card completes the bootstrap operation to 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].

119. If the transaction card "is returned to the mode it was before being inserted into the device," then the transaction card lacks access to the host-device's cellular radio technology, since the transaction card lacked access to this cellular radio technology "before being inserted into the device." Jain ¶[0065].

120. Only after bootstrapping/authentication (FIG. 7) is complete can activation (FIG. 9) begin, which 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].) allows transaction card 112 to engage in the cellular radio communication required to actually activate the transaction card with a financial institution—***enable[s] a mode to communicate by the smartphone information requesting an authorization to establish said capability***.

(v) 1[b]: ***while the mode is enabled, and as a precursor to performing a second step of said two-step process, transmitting by the smartphone first data to a first device requesting the authorization to establish said capability to perform said at least one financial transaction; and***

121. In my opinion, Jain discloses this limitation. As previously stated in my analysis for limitation 1[a][ii], the smartphone's cellular radio communication is

enabled after user authentication. ***While the mode is enabled***, Jain discloses the smartphone performing "method 900 for activating a wireless transaction system" with the financial institution. Jain ¶[0080]. During this method, the transaction card, via smartphone 110, transmits to the financial institution a request for an activation code, as shown by annotated FIG. 9.

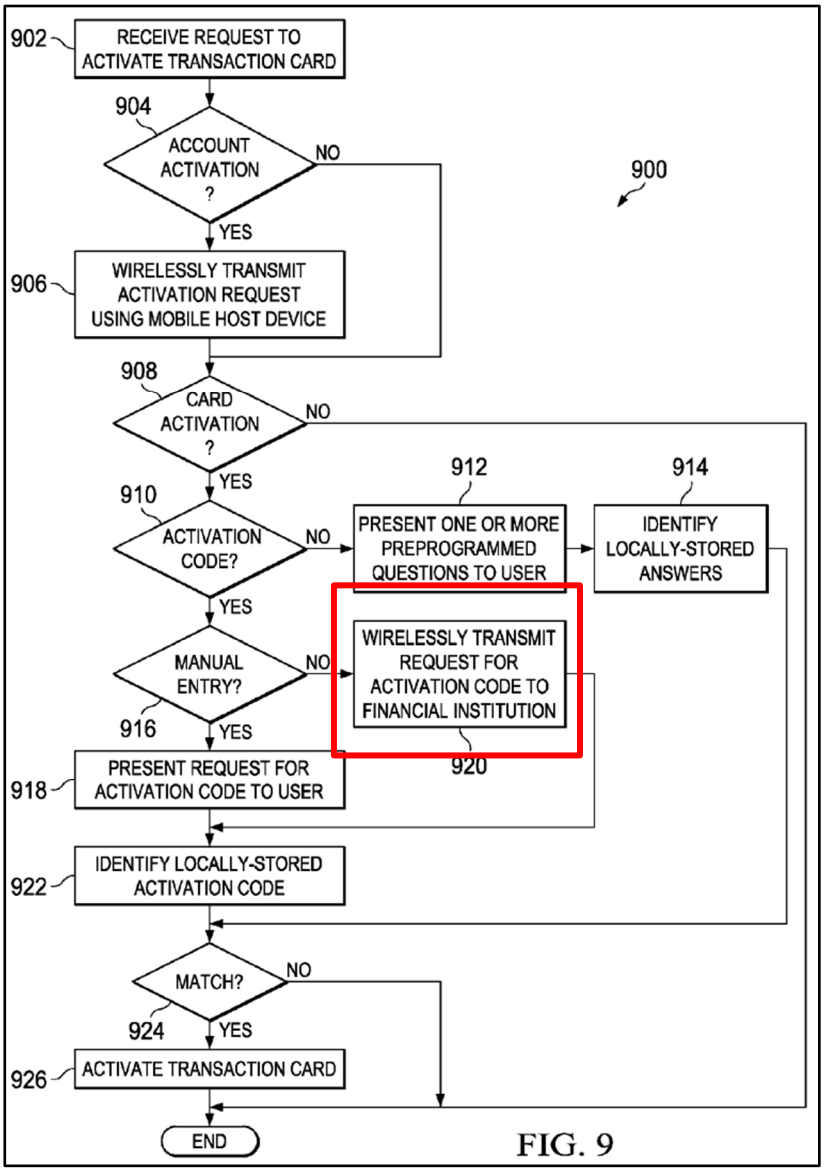


FIG. 9

122. In my opinion, the request sent by the smartphone to a financial institution—devices in an enterprise that authorize transactions through the network by accepting data from clients and returning appropriate responses (Jain ¶¶[0038]-[0039]—constitutes ***transmitting by the smartphone first data to a first device***. Specifically, at step 920, the transaction card, via the smartphone, "wirelessly transmits a request for the activation code using the cellular radio technology" of the smartphone to the financial institution—***to a first device***. Jain ¶[0081]. ***Transmitting by the smartphone*** the request for an activation code—***first data . . . requesting the authorization***—to the financial institution is performed in order to "activat[e] the transaction card and/or financial account." Jain ¶[0026].

123. In my opinion, because the "activation code" is required to enable financial transactions with that card, the sent request constitutes ***requesting the authorization to establish said capability to perform said at least one financial transaction***. The receipt of an activation code matching a stored activation code is the last step before the card is activated in step 926. Thus, a matching "activation code" is an ***authorization*** to engage in financial transactions, and requesting the same is thus ***requesting the authorization***, as claimed. *See* Jain, FIG. 9

124. Further, in my opinion, a POSITA would understand that Jain's request for activation code to the financial institution (step 920) is a request for authorization. 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 and enabling that card to perform financial transactions, requesting an activation code is ***requesting the authorization to establish said capability to perform said at least one financial transaction***.

(vi) 1[c]: ***receiving by the smartphone second data from the first device, comprising the authorization, responsive to said transmitting by the smartphone the first data; then***

125. In my opinion, Jain discloses this limitation. Jain discloses, after sending the request for an activation code, ***receiving by the smartphone*** an activation code from the financial institution, or ***first device***, where the activation code is ***second data ... comprising the authorization***. Specifically, in response to this request, step 924 requires the smartphone receiving a response from the financial institution with an activation code that is then checked against a stored activation code (retrieved at step 922). Jain ¶[0081]. If the activation codes match, the transaction card is activated by step 926. Jain ("the locally-stored activation code is

identified at step 922. If the locally stored information matches the provided information at decisional step 924, then at step 926, the transaction card is activated."). This "activation process may include activating the transaction card and/or financial account" (Jain ¶[0026]), which authorizes the transaction card to perform payments with the associated financial account by "signifying activation of the financial vehicle carried on the card" (Jain ¶[0071]). Thus, as also discussed above in connection with my analysis for limitation 1[b], receipt of a matching activation code that enables completion of Jain's activation process is (or at least renders obvious) the claimed "***authorization***."

126. 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]If 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 ***compris***[***es***] ***… 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 … second data … comprising … authorization***. EX1016 at 23-28.

127. 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.

(vii) 1[d][i]: *[then] performing the second step of said two-step process comprising performing a first transaction of said at least one financial transaction,*

128. In my opinion, Jain discloses this limitation. Jain discloses using the transaction card and smartphone to perform a contactless payment transaction with the financial institution. This constitutes the ***second step of said two-step process***. For instance, Jain discloses transacting with a nearby retail payment terminal POS 114 to pay for a product—***performing a first transaction of said at least one financial transaction***. *See* Jain ¶¶[0019], [0023]. The POS terminals may be contactless-enabled terminals at merchants accepting financial transactions using Mastercard, Visa, Amex, Discover, and other payment programs. Jain ¶[0028]. The intelligent transaction card converts the mobile device to a contactless payment device loaded with a financial vehicle (FV) such as a credit card or a debit card, to perform payment transactions with the POS 114 that accepts contactless payment transactions. Jain ¶[0029]. Jain describes this referencing FIG. 1, as also detailed in my analysis for limitations 1[d][ii]-[iii]:

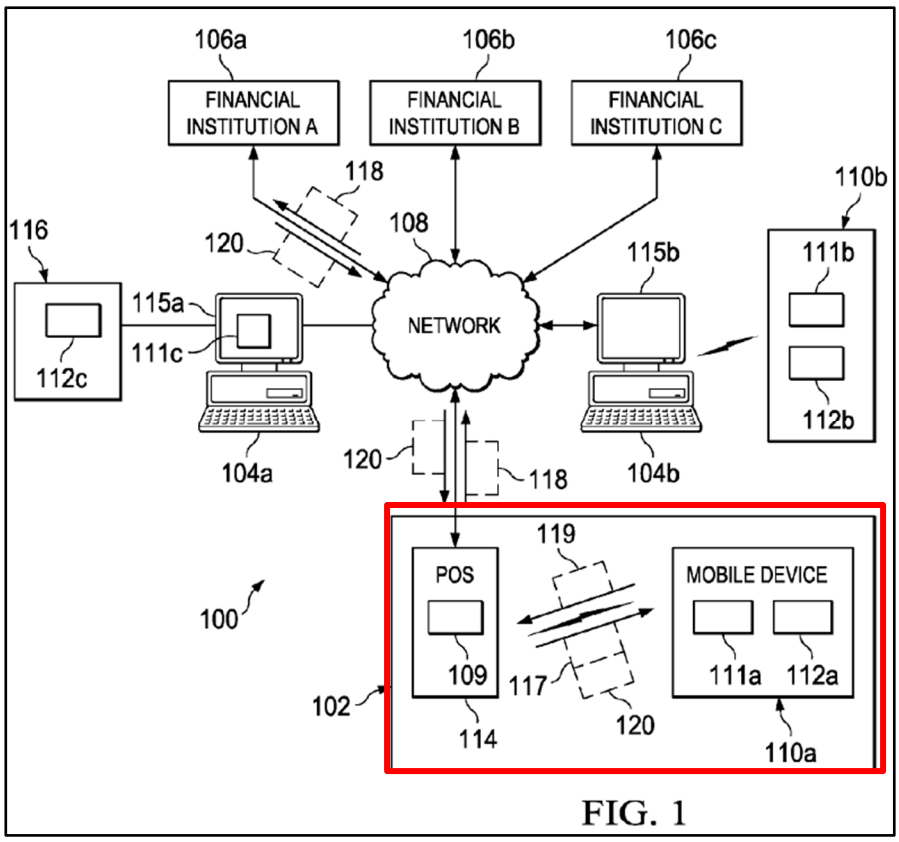


FIG. 1

(viii) 1[d][ii]: *responsive to detecting by the smartphone that a proximity condition is satisfied and*

129. In my opinion, Jain discloses this limitation. Jain discloses executing transactions with nearby POS devices using short range signals, such as near-field communication (NFC) or "proximity signals." *See* Jain ¶[0023]. In other words, executing transactions are ***responsive to detecting by the smartphone that a proximity condition is satisfied***. Specifically, the smartphone first "wirelessly receive[s] a request from the POS device 114 to execute a transaction and/or provide a response." Jain ¶[0023]. The smartphone then activates a "reader mode" of the transaction card "[i]n the event that the mobile device 110 is proximate (*e.g.*, 10 cm or less) a transmitting terminal" to the POS—***detecting by the smartphone that a***

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

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

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

132. Without a reaching a certain signal strength or otherwise satisfying a ***proximity condition***, both devices are sending unnecessary communication signals guaranteed to be lost. This wastes time and processing. Especially for

communications executing financial transactions, either device indiscriminately transmitting sensitive financial information without ensuring communication to the correct device is a security risk. Either device is sending communications that will likely to subject to errors, like packet loss, due to transmission past an effective range, increasing the risk of miscommunication. And devices trying to read wireless communications with weak signal strength are also likely to misinterpret noise or other small unintended wireless signals as communications.

133. 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.

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

135. Thus, for Jain's smartphone to communicate with the POS device using NFC, the smartphone has ***detected that a proximity condition is satisfied*** (*e.g.*, the device is within a range of "10 cm or less" to the POS device, *see* Jain ¶[0030]) by receiving and decoding a short-range NFC signal from the POS device.

136. The Patent Owner agrees with this mapping. In its infringement contentions in the district court litigation, Patent Owner also asserts use of short range communications—specifically, use of NFC—is sufficient to establish ***detecting by the smartphone that a proximity condition is satisfied***. *See* Exhibit 1016 at 29 and 180.

(ix) 1[d][iii]: *responsive to sensing the at least one parameter and determining that the at least one parameter sensed satisfies the criterion;*

137. In my opinion, Jain discloses this limitation. In its Infringement Contentions, Patent Owner argued that the Accused Products meet this limitation by performing a financial transaction after unlocking the phone using biometrics (*e.g.*, fingerprint or face recognition) in the same manner as in 1[a][i]. *See* EX1016 at 35-38. Under at least this interpretation, Jain discloses that the payment transaction with the financial institution is dependent on (***responsive to***) the transaction card being authorized (Fig. 7) and activated (Fig. 9), which includes the claimed ***sensing*** and ***determining***. Jain ¶¶[0073]-[0075], [0081]; *see also supra* Section V.A.1.a.iii.

138. In addition, it is my opinion that Jain discloses performing a financial transaction as responsive to sensing that the same parameter satisfies the criterion. For example, Jain discloses that during payment, the merchant terminal may "prompt the user to authorize a transaction such as by entering a PIN." Jain ¶[0029]. Authorization via a PIN involves, or at least obviously involves, the process of Jain

paragraph [0075] discussed above in connection with limitation 1[a][i]. At a minimum, a POSITA would find that ***sensing*** a user-entered PIN and ***determining*** if that PIN matches a previously-stored PIN—***criteria***—to be the simplest, most natural, and thus obvious way of implementing PIN authorization, since it does not require communication with any other devices and allows the POSITA to reuse aspects of the software that implements the user authentication of Fig. 7.

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

140. For instance, EX1020 discloses completing a transaction, providing a signature on the mobile device, and authenticating the signature by comparing it "with a signature that has been previously stored for authentication purposes." EX1020 ¶¶[0083]-[0084]; *see also* EX1020 FIG. 4:

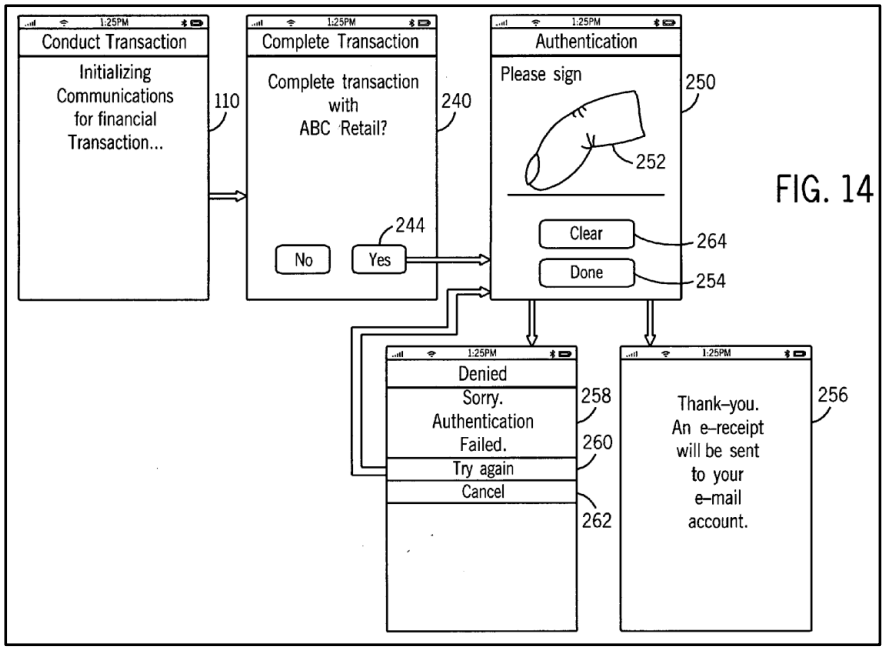


FIG. 14

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

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

142. Also, in my opinion, it would be obvious for a POSITA to authorize the transaction with user biometrics, instead of the disclosed PIN. Requiring biometric authentication before authorizing individual transactions was well known in the art. EX1020 ¶¶[0083]-[0084], [0088], FIG. 14 ("[T]he authentication screen 290 provides a menu 291 that lists various ways for authenticating a transaction … including biometric signatures such as fingerprints and retinal scans, for instance.");

EX1021 ¶[0052] ("Selecting 'Payment' may prompt a payment application 155 on the mobile device 100 to check the biometric sensor 160 for biometric input."). This is not unlike my prior analysis for limitation 1[a][i], where Jain contemplates using biometrics (*e.g.*, fingerprints) for its authorization process. Jain ¶[0075], Figure 7. That software and hardware can be reused here for individual transactions without further complicating the system or incurring any costs. Moreover, Jain recognizes biometrics as a good alternative to PINs. Jain ¶[0075].

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

144. In addition, a POSITA would further understand that two-factor authentication—PIN and biometric authentication—could be warranted here to provide additional security. A POSITA would also be familiar with two-factor authentication and would know how to perform both PIN and biometric authentication. *See, e.g.*, EX1028 Abstract; EX1029 Abstract; EX1030 Abstract.

The PIN authentication could be followed by the biometric authentication or vice versa. A POSITA would recognize the extreme sensitivity of financial information and transactions, and be motivated to incorporate heightened security measures.

145. As discussed in my analysis for limitation 1[a][i], it is my opinion that Jain discloses or at least renders obvious that implementing biometric authorization would entail the claimed ***sensing*** and ***determining***.

(x) 1[e][i]: ***wherein said performing the second step of said two-step process comprises sensing that the proximity condition is satisfied relative to an access point maintained by a vendor at a point of purchase counter, by detecting a short-range signal that is transmitted by the access point,***

146. In my opinion, Jain discloses this limitation. As set forth *supra* with respect to my analysis for limitation 1[d][ii], Jain discloses performing financial transactions with POS terminals through NFC, thereby requiring ***sensing that*** [***a***] ***proximity condition is satisfied relative to an access point maintained by a vendor at a point of purchase counter, by detecting a short-range signal that is transmitted by the access point***.

147. Specifically, Jain discloses that before performing a financial transaction, the smartphone must be sufficiently close to a POS device, which means a ***proximity condition*** [***must be***] ***satisfied***. Sufficient proximity is determined by detecting a "request" from a POS device transmitted via NFC—a ***short-range signal that is transmitted***.

148. In my opinion, Jain's POS device is the claimed ***access point***. Jain further discloses that the POS device may be a "merchant terminal"—an ***access point maintained by a vendor***). *See* Jain ¶[0029].

(xi) 1[e][ii]: *determining that a value of the at least one parameter that is sensed satisfies the criterion and then,*

149. In my opinion, Jain discloses this limitation. As already discussed in my analysis for limitation 1[d][iii], the second step of performing a financial transaction is responsive to claimed ***sensing*** and ***determining***.

(xii) 1[e][iii]: *responsive to having sensed that the proximity condition is satisfied relative to the access point and having determined that the value of the at least one parameter sensed satisfies the criterion, paying for a product by selectively sending information to at least one device;*

150. In my opinion, Jain discloses this limitation. As set forth in my analysis above, Jain's signature or fingerprint authentication constitutes ***determin*[*ing*] *that the value of … at least one parameter sensed satisfies the criterion***. *See* limitations 1[a][i], 1[d]. Jain's smartphone detecting a request from a POS device—signifying proximity—constitutes ***sens*[*ing*] *that the proximity condition is satisfied relative to the access point***. *See* limitations 1[d], 1[e][i]. Both authentication and proximity detection occurs prior to completing the transaction—***responsive to … sens*[*ing*] *that the proximity condition is satisfied … and … determin*[*ing*] *that the … parameter … satisf*[*ying*] *the criterion, paying for a product***.

151. In my opinion, Jain further discloses ***paying for a product by selectively sending information to at least one device***. Jain's smartphone, in response to a request from the POS device, generates a transaction response 119. Jain ¶¶[0027], [0029]. The transaction response 119, which identifies ***information*** associated with a payment account, is ***sen***[***t***] to the nearby POS 114—***at least one device***[1]. Jain ¶¶[0027], [0029]. But the transaction response 119 is only sent—***selectively sen***[***t***]—if the user authorizes the purchase. Jain ¶¶[0027], [0029].

(xiii) 1[f]: ***wherein said paying for a product by selectively sending information to at least one device comprises selectively and wirelessly transmitting information to the at least one device using unlicensed frequencies; and***

152. In my opinion, Jain discloses this limitation. Jain explains that the contactless payment transaction is executed by ***transmitting information*** from the smartphone to the POS device—***at least one device***—"using short range signals such as NFC (*e.g.*, ISO 18092/ECMA 340), ISO 14443 type A/B, ISO 15693, Felica, MiFARE, Bluetooth, Ultra-wideband (UWB), Radio Frequency Identifier (RFID),

[1] According to Patent Owner's infringement contentions, the claimed ***access point*** and claimed ***at least one device*** can be one and the same device. EX1016 at 43, 53 (pointing to "the point-of-sale device" or "terminal" for both limitations).

contactless signals, proximity signals, and/or other signals compatible with retail payment terminals (*e.g.*, POS 114)." Jain ¶[0023].

153. NFC only 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.

154. Patent Owner agrees. In its Infringement Contentions, Patent Owner alleges that "the wireless short-range communications link used by NFC is based upon the unlicensed 13.56 MHz frequency." EX1016 at 57.

155. 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.

(xiv) 1[g]: ***wherein said at least one parameter comprises a signal, a number, a word, a code, 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.***

156. In my opinion, Jain discloses this limitation. As discussed in my analysis for limitation 1[a][i], Jain's use of a PIN or biometric information, such as a fingerprint, for user authentication constitutes ***at least one parameter***. Jain ¶[0075], claim 10.

157. A PIN is a ***number***—a personal identification ***number***. Jain ¶[0075].

158. It is my understanding that biometric information, such as a fingerprint or other biometric signature for user authentication, is a ***physiological state***. Patent Owner acknowledged this in its infringement contentions. *E.g.*, EX1016 at 9-10, 58-59, 160-161, and 209-210.

(b) Claim 2

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

159. As addressed in Sections V.B.1.a, it is my opinion that Jain discloses limitation 2[pre].

(ii) 2[a]: *wherein said enabling a mode to communicate by the smartphone information requesting an authorization comprises enabling a first function of the smartphone while disabling a second function of the smartphone responsive to the at least one parameter having been sensed by the at least one sensor of the smartphone and further responsive to having determined that the at least one parameter that is sensed satisfies the criterion;*

160. In my opinion, Jain discloses this limitation. As discussed with limitations 1[a]-[b], after the bootstrapping/authentication process, Jain's smartphone ***enabl*[*es*] cellular ***communication*** with a financial institution to request activation of the transaction card. *See* Jain ¶¶[0072]-[0075]. This requires ***enabling a first function of the smartphone***. Specifically, the smartphone in step 714 will "turn antenna on an update host device signature in plug-in" and begin the activation process using the smartphone's radio technology. Jain at FIG. 7A. Thus, successful

authentication as part of "automatically bootstrapping" (Jain ¶[0072]) allows engaging in cellular radio communication to request from a financial institution activation of the transaction card 112.

161. While ***enabling*** the smartphone's antenna for the activation process, payment transactions are disabled—***while disabling a second function of the smartphone***. Payment transactions are disabled because the transaction card has not yet been activated. Jain ¶[0081]. Specifically, after the bootstrapping/authentication, per FIG. 7, the process for activating the transaction card begins, per FIG. 9. This includes communicating with a financial institution "using cellular radio technology of the host device." Jain ¶¶[0065], [0072], [0081]. As described by Jain, ***disabling*** payment transactions prior to activation reduces the risk of fraud. Activation first requires authentication and authorization, if authentication or authorization fails, then the associated financial institution is notified, preventing unauthorized transactions. Jain ¶[0075].

162. In my opinion, to the extent Patent Owner argues that ***disabling a second function of the smartphone*** is not explicitly disclosed, it would be obvious to a POSITA. While the smartphone is still in the process of activating the transaction card, a POSITA would have a reasonable expectation that the payment function of the smartphone must be disabled due to an inactive card. An activated card is an authorized card. And an inactive card is a card without authorization from

a financial institution to perform financial transactions. Therefore, any attempted payments or transactions with an inactive transaction card should fail. *See* Jain ¶¶[0019], [0023].

163. Moreover, Patent Owner agrees with the mapping discussed above. In its infringement contentions, Patent Owner alleges that this limitation is met through unlocking the smartphone or application. To Patent Owner, "unlocking the [] smartphone or application" is ***enabling a first function***. And unlocking the smartphone application also means ***disabling*** "locking the Samsung smartphone or application." Specifically, Patent owner recites "***enabling a first function*** (unlocking the [] smartphone or application) ***while disabling a second function*** (locking the Samsung smartphone or application)." EX1016 at 64-65.

164. In my opinion, that reasoning applies here. Jain discloses the limitation by turning on the antenna for requesting authorization. Jain turning on its antenna to perform cellular communications after user authentication is ***enabl***[***ing***] ***a first function***. And turning the antenna on also means ***disabling*** the antenna being off and disabling the lack of cellular communications when the user is not authenticated. In other words, Jain would also meet this limitation by ***enabling a first function*** (turning its antenna on to perform cellular communications when the user is authenticated) ***while disabling a second function*** (turning its antenna off and disabling cellular communications when the user is not authenticated).

165. The ***enabling*** and ***disabling*** occurs after Jain's bootstrapping/authorization process, thereby being ***responsive to having determined that the at least one parameter that is sensed satisfies the criterion*** as discussed in my analysis for limitation 1[a]-[b]. This is because, as is further described with limitation 1[b], the bootstrapping/authorization process (FIG. 7) must have fully completed prior to turning on the antenna and updating the host device signature to enable cellular communication (step 714). Jain FIG. 7.

(iii) 2[b]: ***and then selectively communicating with the first device by using a communications capability of the first function, selectively establishing a master-slave relationship with the first device, and selectively requesting from the first device the authorization to establish the capability to conduct said at least one financial transaction.***

166. In my opinion, Jain discloses this limitation. As explained in my analysis for limitation [b], Jain's smartphone with a transaction card ***selectively communicate[s]*** with the financial institution—***then selectively communicating with the first device***. The smartphone communicates with the financial institution using the smartphone's cellular radio enabled for activation—***using a communications capability of the first function***. And the communication is to request the financial institution to authorize the financial account associated with the card so that the smartphone may perform payments with that associated account—

selectively requesting from the first device the authorization to establish the capability to conduct said at least one financial transaction.

167. In my opinion, Jain discloses or at least renders obvious that the smartphone ***establishes a master-slave relationship with the*** financial—***first device***. According to the '172 patent, a first wireless communications device acts as a "master" and a second wireless communications device acts as a "slave" if "the second wireless communications device is configured to enable a mode/function thereof" only "responsive to receiving an authorization from the first wireless communications device." EX1001 at 5:57-63.

168. Jain discloses such a master-slave relationship where the financial institution is the ***master*** and the smartphone and transaction card is the ***slave***. This occurs when the smartphone is activated to perform financial transactions (***selectively communicating with the first device by using a communications capability of the first function***) after receiving activation authorization by the financial institution—***selectively requesting from the first device the authorization to establish the capability to conduct said at least one financial transaction***. This was described with limitations 1[b]-1[c]. The ***master-slave relationship*** is because the financial institution controls operational aspects of the smartphone and transaction card related to performing financial transactions. This includes controlling financial instruments (*e.g.*, credit cards, debit cards, etc.) that are

associated with the financial institution from the smartphone's wallet, protecting the financial institution against attempted fraud, and removing expired cards. *See* Jain ¶¶[0028], [0075]. These wallet control operations protect the financial institutions interests by ensuring the financial institution may not be left on the hook for fraudulent transactions and also protect users from any bad actors attempting to mimic their financial instruments.

(c) Claim 3

(i) 3[pre]: *The method of claim 2, further comprising:*

169. As addressed in Sections V.B.1.b, it is my opinion that Jain discloses limitation 3[pre].

(ii) 3[a]: *repeatedly sensing the at least one parameter and repeatedly deciding, based on comparing a value of the at least one parameter sensed to the criterion, whether or not to maintain enabled said first function while maintaining disabled said second function; and*

170. In my opinion, Jain discloses this limitation. As discussed in 1[a][ii], Jain's smartphone bootstrapping/authentication process enables a mode to communicate by the smartphone information requesting activation during the activation process—***first function***—of the smartphone and transaction card with the financial institution, and that payment services—***second function***—can only be performed after activation is successful. *See* Jain ¶¶[0072]-[0075]. As is discussed with limitation 1[a][i], this determination is based on authenticating a user using a

PIN or biometrics (*e.g.*, fingerprint). *See* Jain ¶¶[0072], [0075], Fig. 7B at steps 734-742.

171. In my opinion, a POSITA would find it obvious to repeatedly perform authentication and repeatedly check for a PIN or biometrics. This is because a POSITA would have a reasonable expectation that the smartphone and transaction cards remain bootstrapped, and the user remains authenticated (Fig. 7) as the rightful owner of the device as discussed with limitation 1[a][ii]. Jain ¶¶[0072], [0081].

172. Therefore, it would be an obvious security measure to repeatedly perform the user authentication process, such as prompting for a PIN or biometrics, when, for example, idleness causes the smartphone to re-lock to the home screen—***repeatedly sensing the at least one parameter and repeatedly deciding***. During unlocking of the phone, when the authentication process is re-executed, the smartphone would decide to continue—***whether or not to maintain enabled***—the activation process—***first function***. It would be obvious for other events to also cause the phone to repeat the authorization process to maintain security and re-challenge the user for a PIN number or biometrics, such as a network delay (*e.g.*, slow network connection or network timeout), a change to the smartphone with potential security implications (*e.g.*, it re-locks due to changing applications), or the smartphone losing battery or otherwise being shut off (*e.g.*, it re-locks due to being shut off).

173. Finally, as already discussed with limitation 2[a], payment services would remain disabled during activation—***while maintaining disabled said second function***.

174. Alternatively, and similar to Patent Owner's infringement contentions, Jain discloses this limitation by ***maintaining enabled a first function*** (maintaining its antenna on to perform cellular communications when the user is authenticated) ***while maintaining disabled the second function*** (maintaining its antenna off when the user is not authenticated). Patent Owner argued this limitation is met by "repeatedly deciding, based on comparing [the user's fingerprint,] . . . whether or not to maintain enabled the first function (unlocking the Samsung smartphone or application) while maintaining disabled the second function (locking the Samsung smartphone or application)." EX1016 at 86. Thus, the same applies to Jain's smartphone repeatedly deciding, based on verifying the user's PIN or biometrics still match the baseline, whether or not to ***maintain enabled the first function*** (maintaining its antenna on for cellular communications) ***while maintaining disabled the second function*** (maintaining its antenna off for cellular communications).

(iii) 3[b]: *maintaining enabled said first function while maintaining disabled said second function responsive to deciding that said value of the at least one parameter continues to satisfy the criterion; or*

175. In my opinion, Jain discloses this limitation. As discussed with limitations 2[a] and 3[a], Jain ***maintain[s] enabled*** the activation process—***first function***—while ***maintain[s] disabled*** the card's payment services—***second function***—based on deciding that the smartphone user is still authorized (*e.g.*, a PIN or user biometrics remain valid) during activation.

176. Alternatively, as discussed with limitations 2[a] and 3[a] above, Patent Owner's own mapping for its infringement contentions apply here. Patent Owner asserts that "maintaining enabled the first function (unlocking the Samsung smartphone or application) while maintaining disabled the second function (locking the Samsung smartphone or application)." EX1016 (Patent Owner Infringement Contentions) at 94. Similarly, Jain ***maintain[s] enabled the first function*** (maintaining the smartphone's antenna on for cellular communications) ***while maintaining disabled the second function*** (maintaining smartphone's antenna off for cellular communications) based on deciding that the smartphone user is still authorized (*e.g.*, a PIN or user biometrics remain valid).

(iv) 3[c]: *disabling said first function and enabling said second function responsive to deciding that the value of the at least one parameter no longer satisfies the criterion.*

177. In my opinion, Jain discloses this limitation. Limitation 3[c] is an alternative to limitation 3[b]: ***maintaining enabled … or disabling***. As discussed above, Jain discloses limitation 3[b].

178. Alternatively, similar to limitation 3[b], Patent Owner's mapping for its infringement contentions apply here. Jain discloses ***disabling said first function*** (turning off the smartphone's antenna for cellular communications) ***while maintaining disabled the second function*** (turning on the smartphone's antenna for cellular communications) based on deciding that the smartphone user is still authorized (*e.g.*, a PIN or user biometrics remain valid). *See* EX1016 at 94.

(d) Claim 4

(i) 4[pre]: *The method of claim 1,*

179. As addressed in Sections V.B.1.a, it is my opinion that Jain discloses limitation 4[pre].

(ii) 4[a]: *wherein said transmitting by the smartphone first data to a first device is responsive to the at least one parameter having been sensed by the at least one sensor of the smartphone and is further responsive to having determined that the at least one parameter that is sensed satisfies the criterion; and*

180. In my opinion, Jain discloses this limitation. As discussed with limitation 1[b], Jain's smartphone transmissions of "a request for the activation code" (step 920 in FIG. 9) is ***transmitting by the smartphone first data to a first device***.

181. In addition, as set forth above with respect to limitations 1[a] and 1[b], that ***transmitting*** takes place only after Jain's bootstrapping/authenticating process

of FIG. 7—***responsive to the … at least one parameter … satisf*[*ying*]*the criterion***.

The bootstrapping/authenticating process was further discussed with limitation 1[a].

(iii) 4[b]: ***wherein said receiving by the smartphone second data from the first device is responsive to said transmitting by the smartphone the first data and comprises receiving by the smartphone information relating to an acknowledgement and/or authorization to establish and use the capability to perform said at least one financial transaction.***

182. In my opinion, Jain discloses this limitation. As set forth for element 1[c], Jain's smartphone receives a response to its activation code requests of steps 920 of FIG. 9. And the receipt constitutes ***receiving by the smartphone second data responsive to said transmitting by the smartphone the first data***.

183. The response is ***information relating to an acknowledgement and/or authorization to establish and use the capability to perform said at least one financial transaction***. The received activation code is to activate the transaction card, thereby constituting ***information relating to an acknowledgement and/or authorization to establish***. Jain ¶[0081]. The transaction card is activated where the received activation code matches the locally-stored activation code information. Jain ¶[0081]. This "activating the transaction card and/or financial account" (Jain ¶[0026]) authorizes the transaction card to perform payments with the associated financial account by "signifying activation of the financial vehicle carried on the card" (Jain ¶[0071]). Because the transaction card becomes activated from the

response, which allows for performing transactions, the response is ***information relating to an acknowledgement and/or authorization to establish and use the capability to perform … financial transaction***[***s***].

(e) Claim 5

(i) 5[pre]: ***The method of claim 1, further comprising:***

184. As addressed in Section V.B.1.a, it is my opinion that Jain discloses limitation 5[pre].

(ii) 5[a]: ***responsive to performing a financial transaction, causing data to be transmitted selectively to at least one device and further causing data to be received selectively from at least one device.***

185. In my opinion, Jain discloses this limitation. As discussed for limitation 1[e][iii], Jain's smartphone executes transactions by sending transaction information to "contactless-enabled [POS] terminals currently being deployed by merchants"—***performing a transaction***. *See* Jain ¶¶[0019], [0023].

186. After completion of the transaction, the financial institution may also transmit transaction receipts to the smartphone—***responsive to performing a financial transaction, causing data to be transmitted selectively to at least one device***. Jain ¶[0046]. Specifically, "the financial institution 106 may transmit information to the mobile host device 110 in response to at least an event." "The event may include completing a transaction." Jain ¶[0046]. The transmitted

information is "transaction information (*e.g.*, transaction receipt[)] … ." Jain ¶[0046].

187. Further, the smartphone receives the transaction receipts sent by the financial institution after the financial transaction—***responsive to performing a financial transaction, … causing data to be received selectively from at least one device***. As previously stated, "the financial institution 106 may transmit information to the mobile host device 110 in response to at least an event." "The event may include completing a transaction." Jain ¶[0046]. The transmitted information is "transaction information (*e.g.*, transaction receipt[)] … ." Jain ¶[0046]. Jain FIG. 2 illustrates the financial institution wirelessly transmitting a transaction receipt to the smartphone using cellular radio technology. Jain ¶[0041].

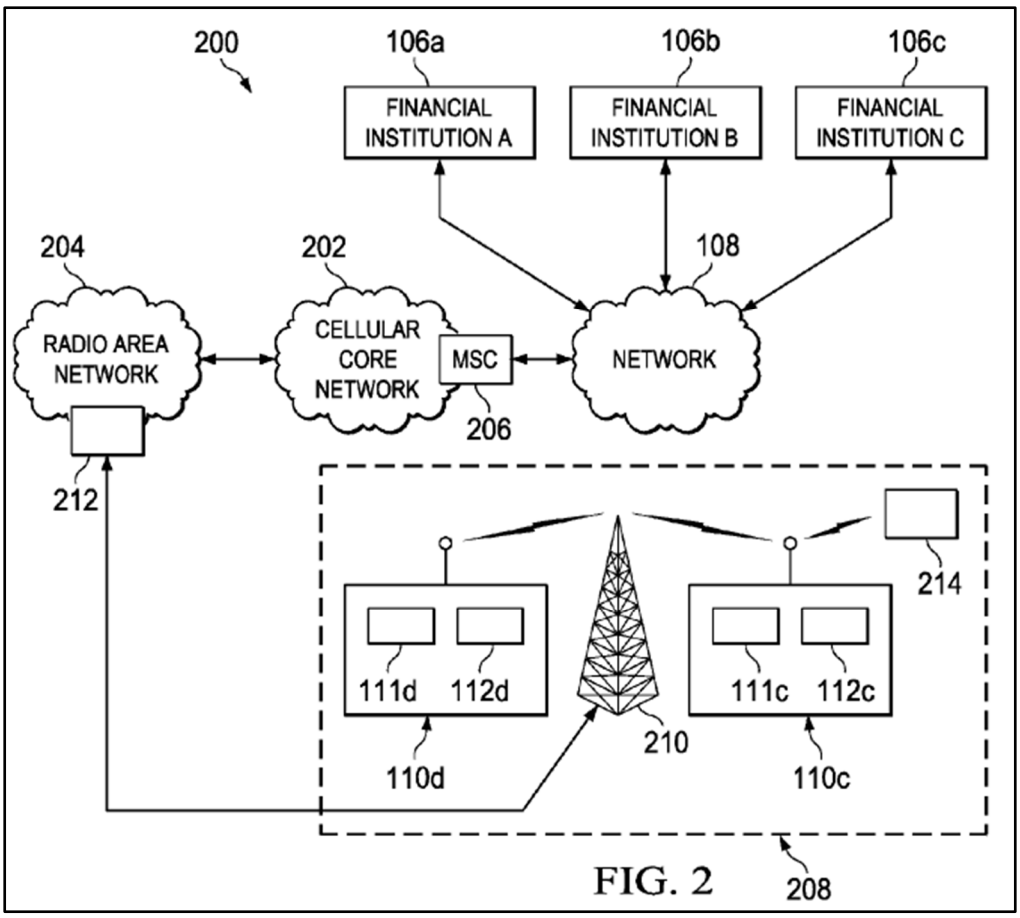


FIG. 2

The transaction receipt is "communicated information between the financial institutions 106 and the transaction card 112." Jain ¶[0041]. Therefore, the smartphone receives the transaction receipt from the financial institution—***causing data to be received selectively from at least one device***. Jain ¶¶[0041], [0046].

188. In my opinion, Patent Owner's theory in its Infringement Contentions also applies here. In its Infringement Contentions, the Patent Owner stated that the smartphone "includes causing data (transaction data) to be transmitted selectively to a device (base station) and further causing data (updated account information) to be received selectively from a device (base station)." EX1016 at 130. In my opinion,

this same theory applies here. Jain's smartphone also causes data (transaction data) to be transmitted selectively to a device (network 108, GSM core network 202, RAN 204, Base Station Controllers (BSC) 212, and/or Base Stations (BS) 210). *See* Jain ¶[0044], FIG. 2. In addition, Jain's smartphone also includes further causing data (updated account information) to be received selectively from the device (network 108, GSM core network 202, RAN 204, Base Station Controllers (BSC) 212, and/or Base Stations (BS) 210). *See* Jain ¶[0044]; Fig. 2.

(f) Claim 6

(i) 6[pre]: *The method of claim 1,*

189. As addressed in Sections V.B.1.a, it is my opinion that Jain discloses limitation 6[pre].

(ii) 6[a]: *wherein said transmitting by the smartphone first data to a first device and receiving by the smartphone 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.*

190. In my opinion, Jain discloses this limitation. As discussed with my analysis for limitations 1[b]-[c], Jain explains that the smartphone and transaction card wirelessly transmits a request for the activation code to a financial institution—***transmitting by the smartphone first data to a first device***. Jain ¶[0081]. And the

smartphone receives an activation code for the transaction card—***receiving by the smartphone second data from the first device***. Jain ¶[0081]. Jain's smartphone uses cellular radio technology for transmitting and receiving the request and activation code, respectively—***transmitting … and receiving … comprises wirelessly transmitting/receiving by the smartphone***. Jain ¶[0081].

191. The cellular radio technology used includes ***licensed frequencies*** may use GSM, CDMA, UMTS, and other modes. Jain ¶[0041]. Such cellular radio technology use ***licensed frequencies***. Cellular radio technology includes the 700MHz Band, 800 MHz Band, PCS Band, and AWS Band—698-806MHz, 806-849/851-896MHz, 1850-1910/1930-1990MHz, and 1710-1755/2110-2155MHz, respectively. But to the extent the cellular radio technology in Jain does not use licensed frequencies, the frequencies constitute ***unlicensed frequencies***. Because the limitation recites that several types of frequencies can satisfy the limitation—***unlicensed frequencies, licensed frequencies, a WiFi air interface protocol, … and/or an Orthogonal Frequency Division Multiple Access air interface protocol***—the limitation is still disclosed.

(g) Claim 7

(i) 7[pre]: *The method of claim 1,*

192. As addressed in Sections V.B.1.a, it is my opinion that Jain discloses limitation 7[pre].

(ii) 7[a]: *wherein said paying for a product further comprises deducting/withdrawing an amount of money from an account.*

193. In my opinion, Jain discloses this limitation. As discussed in my analysis for limitation 1[f], Jain's smartphone pays for products by sending transaction information to contactless-enabled POS terminals. The POS terminals are at merchants that accept financial transactions using various payment programs, including debit cards s at merchants accepting financial transactions using various payment programs including using credit cards, debit cards, and bank accounts. Jain ¶[0025]. Using such accounts to make payments in transactions, particularly where a debit card or bank account is used, causes ***deducting / withdrawing an amount of money from an account***.

194. In particular, when executing a transaction, the financial institution (*e.g.*, "credit card provider, a bank, an association (*e.g.*, VISA), a retail merchant[,] … a prepaid/gift card provider, an[d/or] internet bank" (Jain ¶[0039].)) "may identify an account number and associated verification information and determine funds available to the account holder." Jain ¶[0039]. Jain also explains that the merchant "POS 114 may receive an indication that a transaction amount has been accepted or declined for the identified account and/or request additional information from the transaction card." Jain ¶[0036].

(h) Claim 8

(i) 8[pre]: *The method of claim 7,*

195. As addressed in Sections V.B.1.g, it is my opinion that Jain discloses limitation 6[pre].

(ii) 8[a]: *wherein said using unlicensed frequencies comprises using unlicensed frequencies in a Time Division Duplex operation;*

196. In my opinion, Jain discloses this limitation. As discussed with limitations 1[e][iii] and 1[f], Jain explains that the contactless payment transaction is executed by transmitting information from the smartphone and transaction card to a POS device merchant terminal using short range signals operating in unlicensed frequencies such as NFC, Bluetooth, Felica, MiFARE, UWB, and RFID. Jain ¶[0023].

197. At least NFC and Bluetooth constitute ***using unlicensed frequencies in a Time Division Duplex operation***. As discussed with limitation 1[f], NFC and Bluetooth operate ***using unlicensed frequencies***. Further, "NFC systems can take place as [a] half … duplex system"—***Time Division Duplex operation***. EX1032 at 21. Patent Owner agrees with this mapping: "NFC, a short-range half duplex communication technology," uses ***Time Division Duplex Operations***. EX1016 at 144.

198. Bluetooth also uses ***Time Division Duplex operations***. Not unlike NFC, Bluetooth can operate on half-duplex. *See* EX1038 at 1.

(iii) 8[b] & 8[c]: ***wherein said selectively sending information to at least one device comprises selectively, sending information to the access point maintained by the vendor at the point of purchase counter and to at least one other device that is predetermined; and/or wherein the method further comprises selectively receiving information from the access point maintained by the vendor at the point of purchase counter and from at least one other device that is predetermined.***

199. In my opinion, Jain discloses this limitation. Limitation 8[b] includes two limitations that are alternates to each other—***wherein said selectively sending information … and/or wherein the method further comprises selectively receiving information … .*** Therefore, only one of the two limitations needs to be satisfied. But Jain discloses both limitations.

200. As discussed in my analysis for limitation 1[e][iii], Jain's smartphone executed transactions by sending transaction information to a merchant's contactless-enabled POS terminals—***sending information to the access point maintained by the vendor at the point of purchase counter***. *See* Jain ¶¶[0019], [0023], FIG. 1.

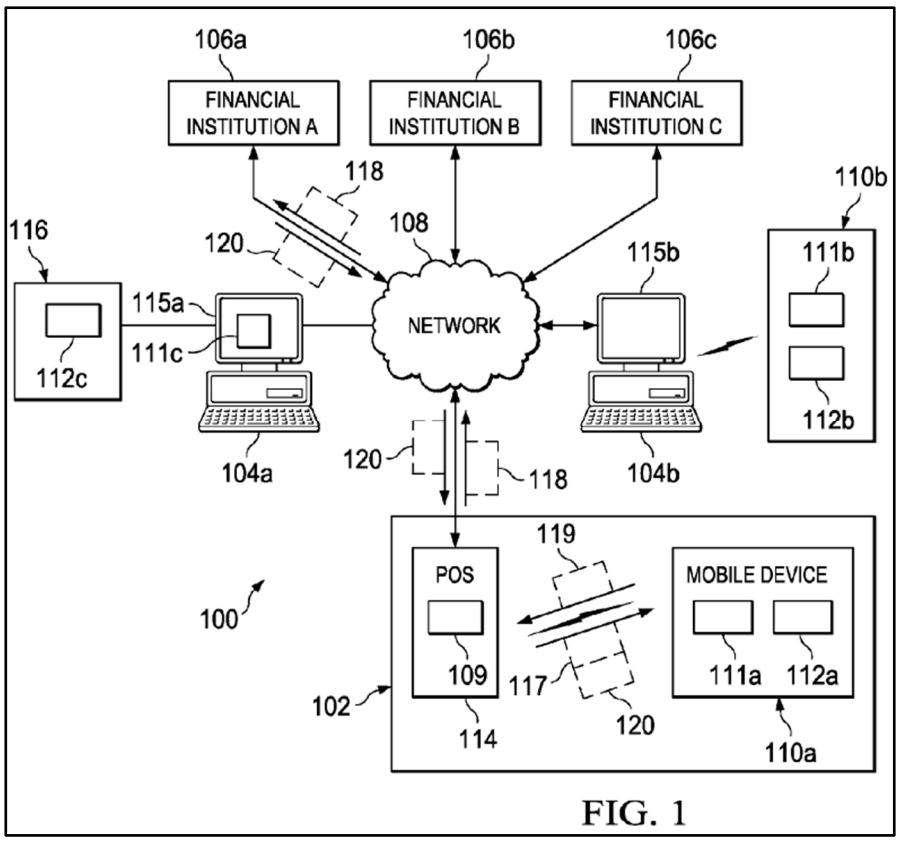


FIG. 1

201. After receiving the transaction information, the POS terminal sends a payment requests to a selected financial institution—***selectively sending information to at least one device***—to authorize the payment. Jain ¶[0027]. Specifically, "the POS device 114 may transmit a request 118 to authorize a transaction to the financial institution 106 [and] may include an account number, a transaction amount, user credentials, and/or other information." Jain ¶[0027].

202. Following the payment, the smartphone ***receiv***[***es***] a transaction receipt from the POS terminal—***information from the access point maintained by the vendor at the point of purchase counter***. Further, the receipt is sent by the financial institution that authorized the payment—***from … one other device that is***

predetermined. Jain ¶[0027]. Specifically, "in response to at least the transaction request 118, the financial institution 106 may transmit an authorization response 120 to the POS device 114 [and] the POS device 114 may transmit the response 120 to the transaction card 112." Jain ¶[0027].

(i) Claims 9-16

203. In my opinion, claims 9-16 are substantively identical to claims 1-8, and thereby disclosed by Jain. The only difference is that claims 9-16 are directed to "[a] smartphone that is configured to perform operations," whereas claims 1-8 are directed to "[a] method of operating a smartphone in performing at least one financial transaction." This distinction is immaterial since Dua discloses both methods and systems. Jain Title.

B. Ground 2: Dua (EX1018)

1. Background

204. 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 '172 Patent under at least pre-AIA 35 U.S.C. § 102(b).

205. 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.

206. 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:

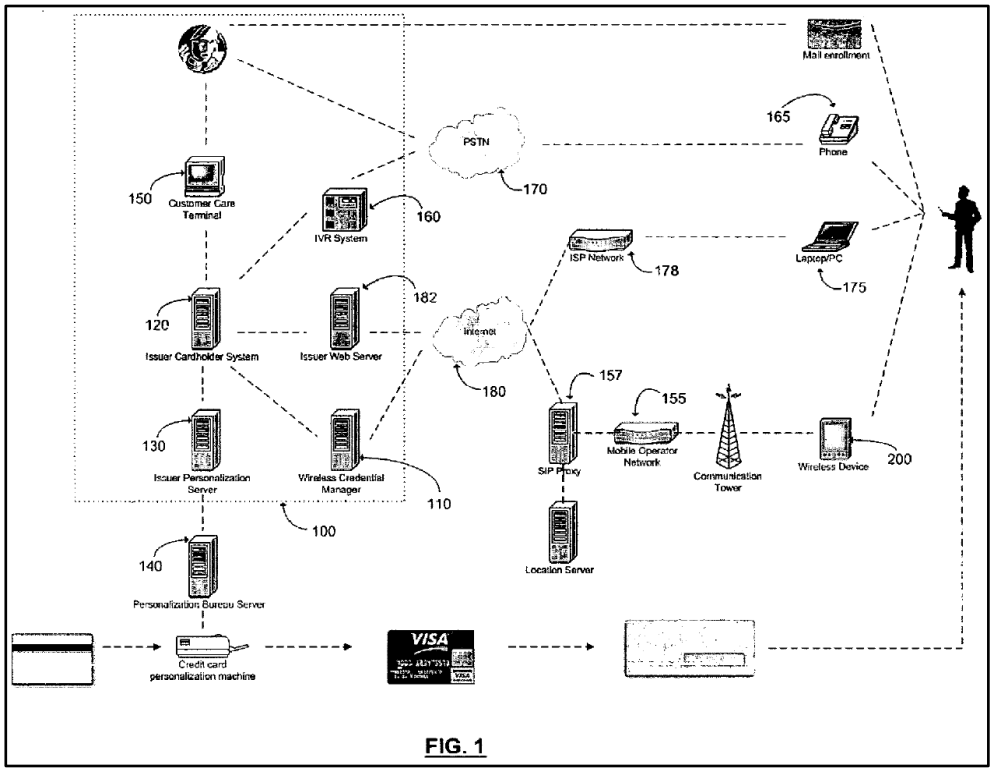


FIG. 1

207. Figure 1 shows a network by which a wireless credential manager "WCM 110 [can] … issu[e], cancel[], and manag[e] eletronic credentials [to] wireless device[]" 200. Dua ¶[0046]. An issuer can issue a physical credit card to a user, and the user "may also request a digital card for use with [a] wallet application on … [a] wireless device 200." Dua ¶[0055]. After the "issuer's system validat[es] the user's identity in real-time," such as by the user sending a "special code or PIN

mailed to the user," the "WCM … will transmit the credential to the wallet application." Dua ¶[0180]. The wallet application can store credentials on the wireless device or, for greater security, in an external wallet storage service accessible by the wallet application. Dua ¶¶[0041], [0287]-[0288], [0491]-[0492].

208. 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:

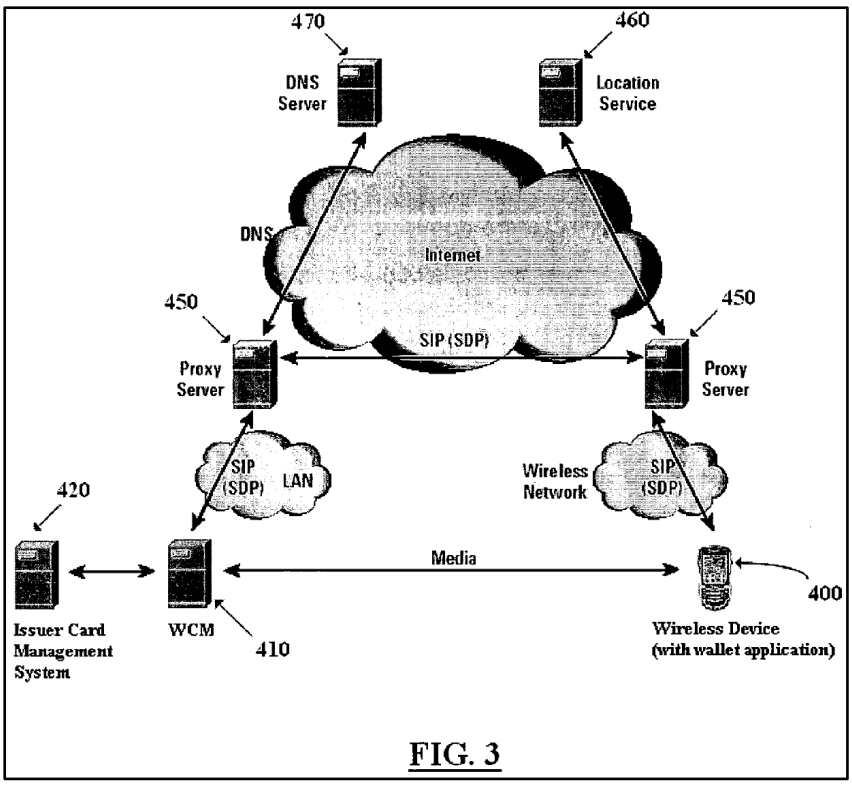


FIG. 3

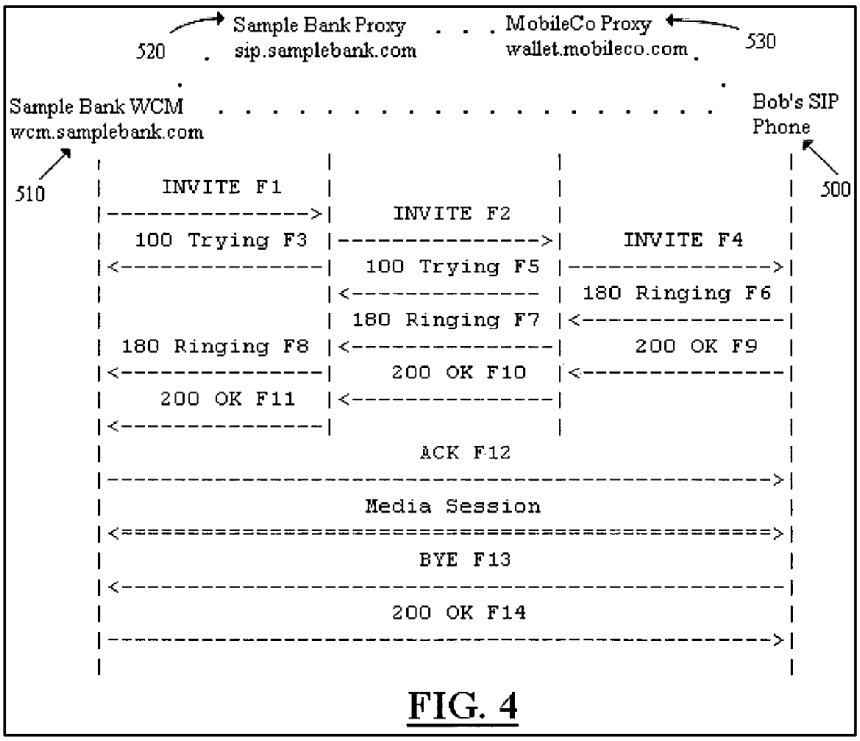


FIG. 4

209. 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].

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

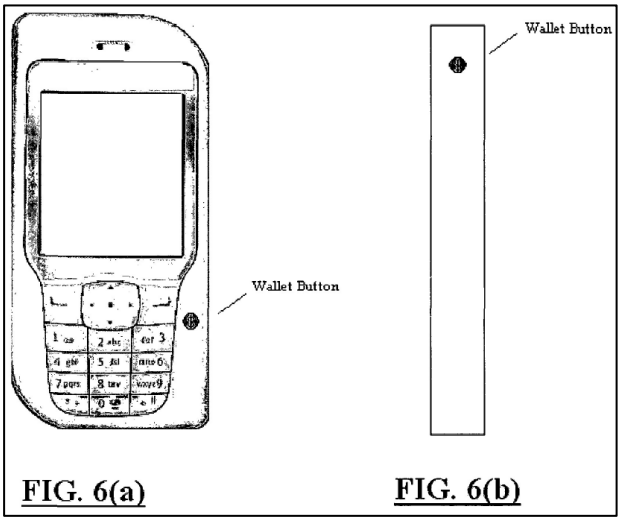


FIG. 6(a) FIG. 6(b)

211. 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][i]: *A method of operating a smartphone in performing at least one financial transaction;*

212. In my opinion, Dua discloses this limitation. Dua discloses a wireless device—***smartphone***. Dua Abstract, FIGS. 3, 5, 6(a)-8. The wireless device includes a "handheld device, such as a mobile telephone," "capable of wirelessly connecting to the internet" and phone applications like a "wallet application." Dua Abstract, ¶¶[0041], [0049], [0050], [0051], [0287]-[0288], FIGS. 3, 5, 6(a)-8. The wallet application can "conduct[] financial … transactions," and thus ***perform***[] ***at least one financial transaction***. Dua Abstract, ¶¶[0041], [0312]-[0313], [0333].

(ii) 1[pre][ii]: *the method including a two-step process in establishing and using a capability in order to perform said at least one financial transaction; the method comprising:*

213. In my opinion, Dua discloses this limitation. Dua discloses the ***two-step process*** [***of***] ***establishing and using***. The first ***establishing*** step is disclosed under two theories: (1) the issuer's "Wireless Credential Manager (WCM) 510 …

issu[ing] … a … [credit] [c]ard [to a] mobile device" ("**Card-Issuing Theory**") (Dua ¶[0128].); and (2) the wallet application "automatically authenticat[ing] itself" to an external wallet storage service for "access[ing] … stored credentials" ("**External-Storage-Authentication Theory**") (Dua ¶¶[0492], [0495].). The second ***using*** step is disclosed by a subsequent "authorized transaction … via … a short range wireless link with a point-of-sale … terminal." Dua Abstract.

214. The first "***establishing***" step is explained below with limitations 1[a][i], 1[a][ii], 1[b], and 1[c]. The second "***using***" step is explained below with limitations 1[d][i], 1[d][ii], and 1[d][iii].

> **(iii)** **1[a][i]:** ***responsive to sensing at least one parameter by at least one sensor of the smartphone and responsive to determining that the at least one parameter that is sensed satisfies a criterion,***
>
> **1[a][ii]:** ***performing a first step of said two-step process by enabling a mode to communicate information requesting an authorization to establish said capability;***

215. In my opinion, Dua discloses this limitation. Limitations 1[a][i] and 1[a][ii] are associated with the "***establishing***" step and those two theories. Under the first ***establishing*** step, limitations 1[a][i] and 1[a][ii] are disclosed by Dua under two theories—**Card-Issuing Theory** and **External-Storage-Authentication Theory**.

216. Under the **Card-Issuing Theory**, Dua discloses using PIN-entry to open the wallet application for the wallet application to be issued a credit card—***responsive to determining that the at least one parameter … satisfies a criterion, performing a first step of said two-step process***. Issuing a credit card to the wallet application requires the wallet application to first be opened. *See* Dua ¶¶[0128]-[0129], [0178], [0180], [0250]. And the "default security setting in the wallet application is that PIN-entry is required before the wallet application can be 'opened,'" or otherwise "allow the user access to the application," including to receive an issued a credit card. Dua ¶¶[0366], [0429]. In other words, after passing PIN-entry to open the wallet application, the wallet application can be issued a credit card.

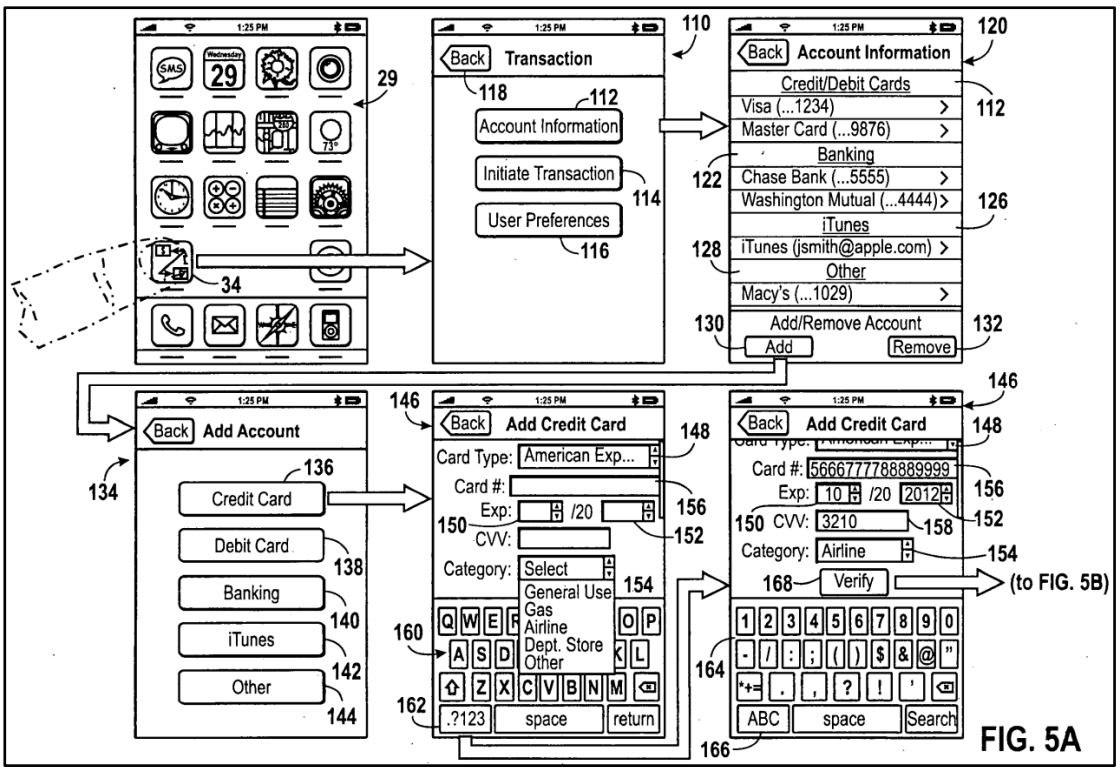
217. To the extent Patent Owner argues that Dua does not expressly mention PIN-entry to open the wallet application prior to card issuance, my opinion is that this is obvious to a POSITA. Using the wallet application requires authentication because "[d]ata in the wallet application is encrypted and protected with a special wallet PIN code … ." Dua ¶¶[0366], [0429]. Making significant changes in the wallet application, such as "access[ing] stored credentials and chang[ing] any application settings or preferences" requires user authentication. Dua ¶[0366]. Such significant changes includes adding a new credit card. A wallet application can hold multiple credit cards, amongst other confidential information. Dua ¶¶[0041],

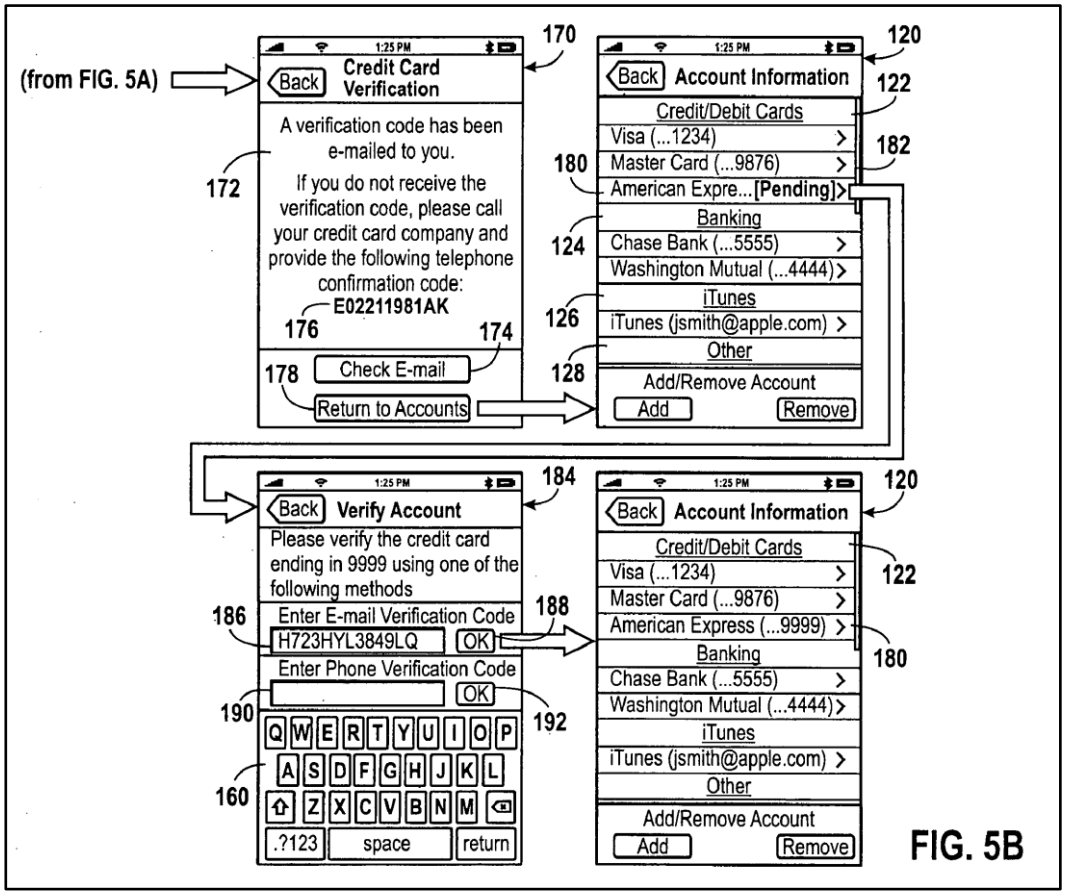
[0055], [0287]-[0288], [0334]. When the wallet application is opened, such as for credit card issuance, the wallet application allows the user to navigate and view the stored credentials. Dua ¶¶[0324]-[0332], [0334], [0366], [0378]. A similar security risk is that credit card issuance requires the wallet application to connect with, and accept data from, a remote server—usually a WCM. Dua ¶¶[0038], [0179]-[0180], FIGS. 3-4. But without requiring PIN-entry to open the wallet for credit card issuance, anyone could allow the wallet application to connect and accept data from an unknown remote server under the pretext of credit card issuance. To ensure security of the wallet application, a POSITA would retain Dua's "default" PIN-entry user authentication when opening the wallet application for credit card use. *See* Dua ¶[0366].

218. 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.

219. Additionally, a feature within a payment application to add an account or credit cards was well known to a POSITA. *See, e.g.*, EX1019 ¶¶[0136]-[0140], FIGS. 5A-B; EX1039 ¶[0117] ("The user then may be required to enter a personal identification number, a password, a security number, or the like in order to

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


Back
Transaction
Account Information
Initiate Transaction
User Preferences
Back
Account Information
Credit/Debit Cards
Visa (...1234)
Master Card (...9876)
Banking
Chase Bank (...5555)
Washington Mutual (...4444)
iTunes
iTunes (jsmith@apple.com)
Other
Macy's (...1029)
Add/Remove Account
Add
Remove
Back
Add Account
Credit Card
Debit Card
Banking
iTunes
Other
Back
Add Credit Card
Card Type: American Exp...
Card #:
Exp: /20
CVV:
Category: Select
General Use
Gas
Airline
Dept. Store
Other
Back
Add Credit Card
Card #: 5666777788889999
Exp: 10 /20 2012
CVV: 3210
Category: Airline
Verify
(to FIG. 5B)
FIG. 5A


(from FIG. 5A)
Back
Credit Card Verification
A verification code has been e-mailed to you.
If you do not receive the verification code, please call your credit card company and provide the following telephone confirmation code:
E02211981AK
Check E-mail
Return to Accounts
Back
Account Information
Credit/Debit Cards
Visa (...1234)
Master Card (...9876)
American Expre...[Pending]
Banking
Chase Bank (...5555)
Washington Mutual (...4444)
iTunes
iTunes (jsmith@apple.com)
Other
Add/Remove Account
Add
Remove
Back
Verify Account
Please verify the credit card ending in 9999 using one of the following methods
Enter E-mail Verification Code
H723HYL3849LQ
OK
Enter Phone Verification Code
OK
Back
Account Information
Credit/Debit Cards
Visa (...1234)
Master Card (...9876)
American Express (...9999)
Banking
Chase Bank (...5555)
Washington Mutual (...4444)
iTunes
iTunes (jsmith@apple.com)
Other
Add/Remove Account
Add
Remove
FIG. 5B

220. 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

221. Dua discloses that PIN-entry requires the wireless device receiving a PIN code after being typed in a PIN-entry or text-entry field by a keyboard or touchscreen keyboard—***sensing*** … ***by at least one sensor of the smartphone***. Dua ¶¶[0366], [0384], [0395], FIGS. 1, 3, 6(a), 8, 9. A POSITA would understand a touch screen or keypad as sensing touch, such as through a capacitive touch screen. *See also* EX1042. The entered PIN code validates the user's identity. For instance, a valid PIN code decrypts the wallet application's data or, as also understood by a

POSITA, matches a valid PIN code stored on the wallet application—***determining that the at least one parameter that is sensed satisfies a criterion***. Dua ¶¶[0050], [0366], [0399], [0429].

222. 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—***sensing … by at least one sensor of the smartphone***. 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 that the at least one parameter that is sensed satisfies a criterion***. Dua ¶¶[0050], [0366], [0399], [0429].

223. 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.

224. Following a PIN or fingerprint match, the wallet application is opened in order to be issued a credit card. *See* Dua ¶¶[0128]-[0129], [0178], [0180], [0250], [0366], [0429]. The steps taken for credit card issuance constitute ***performing a first step of said two-step process by enabling a mode to communicate information requesting an authorization to establish said capability***. Upon opening the wallet application for credit card issuance, the wireless device establishes a Session Initiation Protocol ("SIP") communication session is with the issuer's wireless credential manager to further establish a communication session—***enabling a mode to communicate***. Dua ¶¶[0046], [0104], [0128], [0178]. "The … SIP architecture … establish[es] direct communication between … WCM and wallet application … for … transferring … credentials, " such as "SIP['s] signaling functionality embedded in the Wireless Credential Manager (WCM) 510 is used to issue … a … MasterCard on [a] SIP-enabled mobile device 500 … ." Dua ¶¶[0128], [0178].

225. Through the SIP-established session, 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," different than the wallet PIN used to open the wallet application. Dua ¶[0180].

226. In response to the issuer's request, the wallet application responds with the "special code or PIN that was mailed to the user in advance of the issuance"—***information requesting an authorization to establish*** [***a***] ***capability***. The special code or PIN is "to ensure that the [user] … is in fact the person that requested the digital credential." Dua ¶[0180]. After receiving this message from the wallet application and "[s]ubsequent to … validating the user's identity[,] … the WCM 510 will transmit the credential to the wallet application." Dua ¶[0180]. This credential is the ***authorization***. And because the wallet application's response results in the credential—the ***authorization*** allowing financial transactions with the credit card and enabling the wireless device to execute those transactions—the message to the WCM with the PIN code constitutes ***information requesting an authorization to establish a capability*** to conduct financial transactions.

227. Under the **External-Storage-Authentication Theory**, one of Dua's disclosed embodiments allows wallet application to store credentials in an external wallet storage service. Dua ¶[0491]. "The external storage performs two basic

functions: storage and retrieval of information registered in the user's wallet application." Dua ¶[0491]. Retrieval of credentials from the external storage is only possible after sensing (a) a PIN code or fingerprint as part of opening the wallet; or (b) a reader key transmitted by a point-of-sale reader. Dua ¶¶[0353]-[0354], [0366], [0429]. Regardless, retrieval of credentials after sensing either a PIN code, fingerprint, or reader key constitutes ***responsive to determining that the at least one*** [***sensed***] ***parameter … satisfies a criterion, performing a first step of said two-step process by enabling a mode to communicate by the smartphone information requesting an authorization to establish said capability***.

228. Dua requiring PIN-entry or fingerprint scanning to open the wallet application—***sensing at least one parameter … and responsive to determining that the at least one parameter … satisfies a criterion***—is addressed above in connection with the **Card Issuing Theory**.

229. In addition, Dua discloses a reader key that causes ***sensing at least one parameter … and responsive to determining that the at least one parameter … satisfies a criterion***. A "[reader] key is transmitted from [a point-of-sale] reader to the wireless device." Dua ¶[0353]. "[A] key … received by the wallet application is used as a search string to locate a specific credential." Dua ¶[0353]. Upon matching the received reader key with a key in the wallet application registered with

a credential, the credential is automatically selected by the wallet application and transmitted for a financial transaction. *See* Dua ¶¶[0353]-[0354].

230. Following the selection of the credential, either by PIN, fingerprint, or reader key, the credentials are retrieved from external storage—***responsive to sensing at least one parameter … and … determining that the at least one parameter … satisfies a criterion, performing*** [***the***] ***first*** [***establishing***] ***step***. The wallet application retrieves credentials by setting up a communications session with the external storage—***enabling a mode to communicate***. A "real-time connection is initiated between the wallet application and the storage service" by "utiliz[ing] SIP." Dua ¶¶[0494]-[0495]. Through that real-time connection, the wireless device transmits a "username/password for the wallet application to automatically access the storage area." Dua ¶[0492]; *see also* Dua ¶[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[]… ." Dua ¶[0495]. Because the wireless device sending the "username/password" to the external storage causes the "credential … [to be] transmitted to the wireless device and … made available for use," the initial request with the "username/password" constitutes ***information requesting*** … ***authorization to establish*** [***the***] ***capability*** with the wireless device to conduct financial transactions.

(iv) 1[b]: ***while the mode is enabled, and as a precursor to performing a second step of said two-***

step process, transmitting by the smartphone first data to a first device requesting the authorization to establish said capability to perform said at least one financial transaction; and

231. In my opinion, Dua discloses this limitation. As discussed with limitations 1[pre][ii], 1[a][i], and 1[a][ii], the first ***establishing*** step is disclosed by Dua under the **Card-Issuing Theory** and **External-Storage-Authentication Theory**. Limitation 1[b] is also associated with the first ***establishing*** step and those two theories.

232. Under the **Card-Issuing Theory**, Dua's wireless device ***enable***[***s***] a ***mode to communicate*** through SIP communications with the wireless credential manager through SIP communications in order for the issuer to perform user authentication. This was discussed with limitations 1[a][i] and 1[a][ii]. Dua ¶¶[0046], [0104], [0128], [0178].

233. [***W***]***hile the mode is enabled***, 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].

234. The response by the wireless device is to send "special code or PIN" to the wireless credential manager—***transmitting by the smartphone first data to a first device requesting the authorization to establish said capability to perform said at least one financial transaction***. *See also* Dua FIG. 3 (depiciting WCM 410 as a server communicating with the wireless device 400):

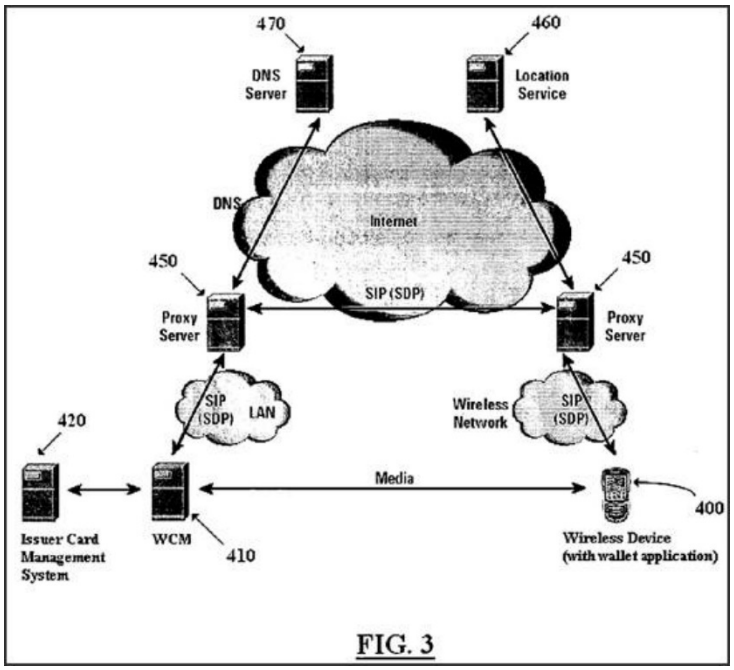


FIG. 3

As stated with limitations 1[a][i] and 1[a][ii], the response with the "special code or PIN" is for user authentication, "ensur[ing] that the [user] … is in fact the person that requested the digital credential." Dua ¶[0180]. And "[s]ubsequent to … validating the user's identity[,] … the WCM 510 will transmit the credential to the wallet application." Dua ¶[0180]. Because the wallet application's response with the "special code or PIN" results in the issued credit card that can be used in financial

transactions, the transmission of the PIN code is a ***request***[] ***t***[***o***] ***authoriz***[***e***] … ***establish***[***ing***] [***the***] ***capability to perform*** … ***financial transaction***[***s***].

235. The user authentication communications for card issuance is ***a precursor to performing a second*** [***transaction-execution***] ***step of said two-step process***, because having the transmitted credential is necessary to perform financial transactions with that credential.

236. Under the **External-Storage-Authentication Theory**, Dua's wireless device ***enable***[***s***] through SIP communications a ***mode to communicate*** for authenticating the wireless device to the external storage and retrieving credentials. Dua ¶[0492], [0494]-[0495]. This was discussed with limitations 1[a][i] and 1[a][ii].

237. [***W***]***hile the mode is enabled***, the wireless device authenticates itself to the external storage by transmitting a "username/password for the wallet application to automatically access the storage area"—***transmitting by the smartphone first data to a first device***. Dua ¶[0492]; *see also* Dua ¶[0495]. Accessing the external storage allows the wallet application to retrieve credentials stored there. 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[] … ." Dua ¶[0495]. Because transmitting the "username/password" for authentication causes retrieval and use of the credential,

the authentication and request for a credential is a ***request***[] ***t***[***o***] ***authoriz***[***e***] … ***establish***[***ing***] [***the***] ***capability to perform*** … [***a***] ***financial transaction***.

238. The wireless device's authentication and credential requests are ***a precursor to performing a second*** [***using***] ***step of said two-step process*** because financial transactions cannot occur prior to retrieving a credential.

(v) 1[c]: ***receiving by the smartphone second data from the first device, comprising the authorization, responsive to said transmitting by the smartphone the first data;***

239. In my opinion, Dua discloses this limitation. As discussed with limitations 1[pre][ii], 1[a][i], 1[a][ii], and 1[b], Dua discloses the first ***establishing*** step under the **Card-Issuing Theory** and **External-Storage-Authentication Theory**. Limitation 1[c] is associated with the "***establishing***" step and those two theories.

240. Under the **Card-Issuing Theory**, as previously discussed the wireless device's wallet application transmits a "special code or PIN" to the wireless credential manager—***transmitting by the smartphone the first data***. Dua ¶[0180]. After the wireless credential manager "validat[es] the user's identity," the wireless credential manager "transmit[s] the credential to the wallet application"—***receiving by the smartphone second data from the first device, comprising the authorization, responsive to said transmitting by the smartphone the first data***. Dua ¶[0180]. Upon receiving the issued credentials, the wireless device can use those credentials

in financial transactions, which means the credentials are authorization to perform financial transactions with the underlying account—***second data from the first device, comprising the authorization***.

241. Patent Owner agrees with this mapping. In the district court litigation, Patent Owner asserts in its infringement contentions that receiving an issued credit card for conducting financial transactions is sufficient to establish ***receiving*** … ***second data*** … ***comprising*** … ***authorization***. EX1016 at 23-28.

242. Under the **External-Storage-Authentication Theory**, as discussed with limitations 1[a][ii] and 1[b], the wireless device's wallet application transmits a "username/password" to the external storage in order for the "wallet application [to] automatically authenticate[] itself and gain[] access to the stored credentials"—***transmitting by the smartphone the first data***. Dua ¶¶[0492], [0495].

243. After obtaining access to the stored credentials, the wireless device retrieves and receives the credentials from the external storage—***receiving by the smartphone second data from the first device, comprising the authorization, responsive to said transmitting by the smartphone the first data***. Dua ¶¶[0491]-[0492], [0495]. The credentials ***compris***[***e***] ***the authorization*** because the credentials are necessary to engage in transactions using the underlying account.

(vi) 1[d][i]: ***then performing the second step of said two-step process comprising performing a first transaction of said at least one financial transaction,***

1[d][ii]: ***responsive to detecting by the smartphone that a proximity condition is satisfied and***

1[d][iii]: ***responsive to sensing the at least one parameter and determining that the at least one parameter sensed satisfies the criterion;***

244. In my opinion, Dua discloses this limitation. As discussed with limitation 1[b], the first ***establishing*** step under the **Card-Issuing Theory** and **External-Storage-Authentication Theory** occurs before the second ***using*** step—***then performing the second step***.

245. After receiving credentials, the wireless device makes proximity transactions with POS terminals—***second step … comprising performing a first transaction***. "Credentials … may [be] use[d] [by] the handheld device to conduct … [a] transaction … via … a short range wireless link with a point-of-sale terminal." Dua Abstract.

246. The "short range wireless link" used by the wireless device is implemented through short-range wireless communication protocols, like Near-Field-Communication ("NFC"). Because NFC is used for a proximity transaction, the transaction only occurs when the wireless device is in "close proximity" to the POS terminal. This requires detection of the NFC communications—***detecting by the smartphone that a proximity condition is satisfied***—such as the "reader key" being transmitted from the POS terminal. Dua Abstract, ¶¶[0016], [0318].

247. NFC and other short range wireless communication protocols require satisfying a proximity condition because such wireless communication protocols are only effective within a short range. The communication signals between the device and terminal must be strong enough to engage in communication with these protocols. The strength of the signal is dependent on distance between device and terminal, where signal strength increasingly attenuates with as the distance becomes greater.

248. Patent Owner agrees with this analysis. Patent Owner also asserted in its infringement contentions that use of short range communications—specifically, use of NFC—is sufficient to establish ***detecting by the smartphone that a proximity condition is satisfied***. EX1016 at 29. Thus, when Dua is able to communicate with the POS terminal using NFC, the wireless device has ***detected that a proximity condition is satisfied*** (*e.g.*, Dua at Abstract, ¶¶[0041], [0314]-[0315], [0382], [0395]) by receiving and decoding a short-range NFC signal from the POS device.

249. In addition, it is my opinion that a POSITA would find it obvious. A POSITA would find it obvious that Dua's wireless device would have to ***detect***[] ***by … that a proximity condition is satisfied*** based on the NFC signals from a POS terminal. Dua's wireless device establishes a peer-to-peer communication session with the POS terminal over NFC. *E.g.*, Dua ¶[0016], Claims 33, 36, 50. The peer-to-peer communication session potentially has to transfer a significant amount of

data, such as encryption keys, reader keys, and several credentials. Dua ¶[0359]. Dua contemplates the "user … hold[ing] the wireless device in front of the reader for a longer period of time while the processing … takes place." Dua ¶[0359].

250. 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.

251. 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.

252. **Card-Issuing Theory:** As discussed with limitations 1[a][i] and 1[a][ii], the first "***establishing***" step is "***responsive***" to sensing matching PIN or

fingerprint. Similarly, Dua discloses that transactions can be made after PIN-entry. The "default security setting in the wallet application is that PIN-entry is required before" (***responsive to***) "any credentials [are] transmitted to an external device," such as for a transaction with a point-of-sale reader. Dua Abstract, ¶[0366].

253. As discussed with limitations 1[a][i] and 1[a][ii], the wireless device receives a PIN code (***parameter***) through a PIN entry or text field, and typed in with a keyboard or touchscreen keyboard (***sensing … by at least one sensor of the smartphone***). Dua ¶¶[0366], [0384], [0395], FIGS. 1, 3, 6(a), 8, 9. The entered PIN code must be able to validate the user's identity, such as being able to decrypt wallet application's data or, to a POSITA, matching a validation PIN code stored on the wallet application (***determining that the at least one parameter that is sensed satisfies a criterion***). Dua ¶¶[0050], [0366], [0399], [0429].

254. PIN codes can be replaced with fingerprints (***parameter***) scanned by the "wireless device's embedded biometric technologies" (***sensing … by at least one sensor of the smartphone***). Dua ¶¶[0366], [0414], [0414]. To a POSITA, using a "fingerprint in lieu of a PIN code to authenticate a user to the wallet application" means determining if the scanned biometric data matches to the correct user's biometric data stored on the wireless device (***determining that the at least one parameter sensed satisfies the criterion***) or, as disclosed by Dua, if the scanned biometric data can decrypt the wallet application's data (***determining that the at***

least one parameter sensed satisfies the criterion). Dua ¶¶[0050], [0366], [0399], [0429].

255. **External-Storage-Authentication Theory:** As discussed with limitations 1[a][i] and 1[a][ii], the first "***establishing***" step is "***responsive***" to sensing a reader key registered with a credential. Because the first "***establishing***" step is authentication with external storage to retrieve a credential for a transaction, thereby occurring immediately prior to the transaction, the transaction is also "***responsive***" to sensing the same registered reader key (***sensing at least one parameter by at least one sensor of the smartphone and determining that the at least one parameter that is sensed satisfies a criterion***).

256. Finally, in its Infringement Contentions, Patent Owner argued that the Accused Products meet limitation 1[d][iii] by performing a financial transaction after unlocking the phone using biometrics (*e.g.*, fingerprint or face recognition) in the same manner as in 1[a][i]. *See* EX1016 at 35-38. Under at least this interpretation, Dua discloses that the payment transaction with the financial institution is dependent on (***responsive***) the credentials being retrieved from external storage, which includes the claimed ***sensing*** and ***determining***. Dua ¶¶[0050], [0366], [0399], [0429].

(vii) 1[e][i]: ***wherein said performing the second step of said two-step process comprises sensing that the proximity condition is satisfied relative to an access point maintained by a vendor at a point of***

> ***purchase counter, by detecting a short-range signal that is transmitted by the access point,***
>
> **1[e][ii]:** ***determining that a value of the at least one parameter that is sensed satisfies the criterion and then,***
>
> **1[e][iii]:** ***responsive to having sensed that the proximity condition is satisfied relative to the access point and having determined that the value of the at least one parameter sensed satisfies the criterion, paying for a product by selectively sending information to at least one device;***

257. In my opinion, Dua discloses this limitation. As discussed with limitations 1[d][i], 1[d][ii], and 1[d][iii], Dua's wireless device transmits credentials to POS terminals to perform a financial transaction—***performing the second step of said two-step process comprising performing a first transaction of said at least one financial transaction***. And transmitting credentials to the POS terminal only occurs after the wireless device verifies a PIN or fingerprint or receives a reader key registered to a credential, as discussed under the **Card-Issuing Theory** and **External-Storage-Authentication Theory**, respectively—***responsive to … determin*[***ing***] ***that a value of the at least one parameter that is sensed satisfies the criterion***.

258. Further, the transactions between the wireless device and POS terminal are a proximity transaction through a short range wireless communications. "Credentials are ultimately supplied to … a mobile telephone[,] … may [be] use[d] [by] the handheld device to conduct … [a] transaction … via … a short range

wireless link with a point-of-sale terminal." Dua Abstract. The short range wireless link between the wireless device and POS terminal is through NFC. Because NFC is used, the credential is only transmitted, and transaction only executed, once the wireless device becomes close enough to detect NFC communications from the "RFID reader[] installed at POS terminals in [the vendor's] stores"—***sensing that the proximity condition is satisfied relative to an access point maintained by a vendor at a point of purchase counter, by detecting a short-range signal that is transmitted by the access point***. Dua Abstract, ¶¶[0016], [0041], [0314]-[0315], [0318], [0354]; *see also* Dua ¶[0353]. *See also supra*, obviousness discussion for limitation 1[d][ii].

259. Only after satisfaction of all the requirements discussed above, the credentials are sent to the POS terminal, thereby executing the transaction—***selectively sending information to at least one device***. Dua Abstract.[2] And the executed transaction causes ***paying for … product***[***s***] like groceries or train tickets. *See* Dua ¶¶[0352]-[0353].

[2] According to Patent Owner's infringement contentions, the claimed ***access point*** and claimed ***at least one device*** can be one and the same device. EX1016 at 43, 53, 57 (pointing to "the point-of-sale device" or "terminal" for both limitations).

(viii) 1[f]: ***wherein said paying for a product by selectively sending information to at least one device comprises selectively and wirelessly transmitting information to the at least one device using unlicensed frequencies; and***

260. In my opinion, Dua discloses this limitation. As discussed with limitations 1[e][i], 1[e][ii], and 1[e][iii], Dua's wireless device transmits credential information to a POS terminal—***selectively sending information to at least one device***. *E.g.*, Dua Abstract, ¶[0353]. The transmitted credentials causes payment for products such as groceries and train tickets—***paying for a product***. Dua Abstract, ¶¶[0352]-[0353].

261. The wireless device uses short range wireless communication, such as NFC and Bluetooth, to transmit or otherwise communicate with the POS terminal—***wirelessly transmitting information to the at least one device using unlicensed frequencies***. Dua Abstract, ¶¶[0016], [0318].

262. NFC only 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.

263. Indeed, Patent Owner agrees. In its Infringement Contentions, Patent Owner alleges that "the wireless short-range communications link used by NFC is based upon the unlicensed 13.56 MHz frequency." EX1016 at 57.

264. 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.

(ix) 1[g]: ***wherein said at least one parameter comprises a signal, a number, a word, a code, 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.***

265. In my opinion, Dua discloses this limitation. As discussed with limitations 1[a][i] and 1[a][ii], Dua discloses several ***parameters***—a PIN code (***a number, a word,*** [***or***] ***a code***), fingerprint (***a physiological state***), and/or reader key (***a signal***).

(b) Claim 2

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

266. As addressed in Sections V.C.3.a, it is my opinion that Jain discloses limitation 2[pre].

(ii) 2[a]: ***wherein said enabling a mode to communicate by the smartphone information requesting an authorization comprises enabling a first function of the smartphone while disabling a second function of the smartphone responsive to the at least one parameter having been sensed by the at least one sensor of the smartphone and further responsive to having determined that the at least one parameter that is sensed satisfies the criterion;***

267. In my opinion, Dua discloses this limitation. As discussed with limitations 1[a][i] and 1[a][ii], Dua discloses ***enabling a mode*** … ***responsive to the*** … ***parameter having been sensed*** … ***and*** … ***determined*** … [***to***] ***satisf***[***y***] [***a***] ***criterion*** under the **Card-Issuing Theory** and **External-Storage-Authentication Theory**. Both theories also disclose ***enabling a first function*** … ***while disabling a second function***.

268. Under the **Card-Issuing Theory**, the "default security setting in the wallet application is that PIN-entry is required before the wallet application can be 'opened.'" Dua ¶¶[0366], [0429]. And the "wireless device … could use a fingerprint in lieu of a PIN code … ." Dua ¶[0366]. Once the PIN or fingerprint is received, the PIN-entry or fingerprint-scanning function for opening the wallet is disabled.

269. Patent Owner agrees with this mapping. Patent Owner in its infringement contentions contends that the "***enabling a first function***" and "***disabling a second function of the smartphone***" limitations are met "unlocking the Samsung smartphone or application" and "locking the Samsung smartphone or application," respectively. EX1016 at 65. Dua has the same disclosure, where PIN-entry or fingerprint scanning open the wallet application.

270. Under the **External-Storage-Authentication Theory**, Dua's wireless device can receive a reader key from the POS terminal—***at least one parameter***

having been sensed by the at least one sensor of the smartphone—as discussed with limitations 1[a][i] and 1[a][ii]. Dua ¶[0353]. "[A] key … received by the wallet application is used as a search string to locate a specific credential." Dua ¶[0353]. Where the reader key locates a key registered to a credential—***determined that the … parameter … satisfies the criterion***—the wallet application automatically selects that credential to transmit for a financial transaction. *See* Dua ¶[0353]; *see also* Dua ¶[0354].

271. As stated with limitations 1[a][i] and 1[a][ii], Dua's wireless device can store credentials in external storage. Dua ¶[0491]. And upon receiving a reader key that matches up with a key registered to a credential—***responsive to having determined that the at least one parameter that is sensed satisfies the criterion***—the wireless device must retrieve that credential from external storage for later transmission as part of a financial transaction. Dua ¶¶[0492], [0494]. To retrieve the credential, Dua sets up "real-time connection is initiated between the wallet application and the storage service" by "utiliz[ing] SIP"—***enabling a first function of the smartphone***. Dua ¶¶[0494]-[0495]. The "real-time connection" also 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"—***enabling a first function of the smartphone***. Dua ¶¶[0493], [0495].

272. Receiving a reader key registered with a credential also causes several features of the wallet application to be PIN-less—***while disabling a second function of the smartphone***. The wallet application is automatically launched without a PIN entry. Dua ¶¶[0353], [0392]. The corresponding credential is automatically selected without a PIN entry. Dua ¶¶[0353], [0355], [0392]. And the credential is ready for transmission without PIN entry. Dua ¶¶[0354], [0384], [0392].

(iii) 2[b]: ***and then selectively communicating with the first device by using a communications capability of the first function, selectively establishing a master-slave relationship with the first device, and selectively requesting from the first device the authorization to establish the capability to conduct said at least one financial transaction.***

273. In my opinion, Dua discloses this limitation. Dua discloses ***then selectively communicating with the first device by using a communications capability of the first function, selectively establishing a master-slave relationship with the first device, and selectively requesting from the first device the authorization to establish the capability to conduct said at least one financial transaction*** under the **Card-Issuing Theory** and **External-Storage-Authentication Theory**.

274. Under the **Card-Issuing Theory**, Dua discloses that finding a matching PIN or fingerprint causes the wallet application to launch and prompt the user for an issuer PIN to transmit to the WCM to request credential issuance—***then selectively***

communicating with the first device. Dua ¶[0180]. The credential issuance request is a ***communicat*[*ion*] … [*that*] *us*[*es*] [*the*] *communications capability of the first function*** because the communication is through the unlocked wallet application. *See* Dua ¶[0180].

275. The communications channel between the wireless device and WCM ***establish*[*es*] *a master-slave relationship***. As the '172 patent specification explains, a first wireless communications device acts as a "master" and a second wireless communications device acts as a "slave" where "the second wireless communications device is configured to enable a mode/function thereof" only "responsive to receiving an authorization from the first wireless communications device." '172 patent at 5:57-63. Dua discloses such a relationship between the wireless device and WCM. The wireless device is responsive to the WCM validating the issuer PIN sent by the wallet application, and the WCM issuing the credential to wallet application. Dua ¶[0180].

276. Under the **External-Storage-Authentication Theory**, Dua discloses that receiving a reader key registered to credential causes the wallet application to automatically launch, and authenticate itself to and retrieve a credential from an external storage unit—***then selectively communicating with the first device***. Dua ¶¶[0353], [0355], [0384], [0392], [0491]. To retrieve the credential, Dua sets up "real-time connection is initiated between the wallet application and the storage

service" by "utiliz[ing] SIP," which includes "encrypt[ion] [for] all messages between the wallet application and the storage service," and "[n]ew communication keys … dynamically generated for each communication session"—***using a communications capability of the first function***. Dua ¶¶[0493]-[0495].

277. Through the communication session, the wireless device "automatically authenticates itself" to the external storage by providing a "username/password" previously established with the external storage. Dua ¶¶[0492], [0495]. The wireless device's authentication and credential request ***establish***[***es***] ***a master-slave relationship*** with the external storage. As the '172 patent specification explains, a first wireless communications device acts as a "master" and a second wireless communications device acts as a "slave" where "the second wireless communications device is configured to enable a mode/function thereof" only "responsive to receiving an authorization from the first wireless communications device." '172 patent at 5:57-63. Dua discloses such a relationship between the wireless device and external storage. Dua ¶[0180]. Tthe wireless device is responsive to the external storage's authentication of the wallet application and transmission of credentials back to the wallet application.

278. Alternatively, it is my opinion that Dua discloses this ***master-slave relationship*** because the wireless device establishes real-time control over a device of limited capability, such as external storage. Generally, a master-slave relationship

occurs when one device follows, serves, executes, or is otherwise responsive to the commands of a second device. In this case, the external storage serves the credential-retrieval commands of the wireless device. In service of the wireless device, "[t]he external storage performs two basic functions: storage and retrieval of information registered in the user's wallet application." Dua ¶[0491]. Those two functions—"storage and retrieval"—are provided to the wireless device when the wireless device authenticates itself to the external storage. Those functions and authentication allow the wireless device to issue commands requesting credentials from the external storage. Dua ¶¶[0491], [0495].

279. The authentication and credential request to the external storage constitutes a ***request***[] **…** [***for***] ***the authorization to establish the capability to conduct …*** [***a***] ***financial transaction***. This is because the request causes the external storage to transmit back the credential and allows use of that credential. Dua ¶[0495]. Specifically, after the request, the external storage's "credential information is securely transmitted to the wireless device and temporarily made available for use by the wireless device[] … ." Dua ¶[0495].

(c) Claim 3

(i) 3[pre]: *The method of claim 2, further comprising:*

280. As addressed in Sections V.C.3.b, it is my opinion that Jain discloses limitation 3[pre].

(ii) **3[a]-[c]:** ***repeatedly sensing the at least one parameter and repeatedly deciding, based on comparing a value of the at least one parameter sensed to the criterion, whether or not to maintain enabled said first function while maintaining disabled said second function; and***

maintaining enabled said first function while maintaining disabled said second function responsive to deciding that said value of the at least one parameter continues to satisfy the criterion; or

disabling said first function and enabling said second function responsive to deciding that the value of the at least one parameter no longer satisfies the criterion.

281. In my opinion, Dua discloses this limitation. Under the **Card-Issuing Theory** and **External-Storage-Authentication Theory**, Dua discloses under the ***repeatedly sensing the … parameter***, ***repeatedly deciding, based on … the … parameter***[**,**] … ***whether … to maintain enabled said first function while maintaining disabled said second function***, and then ***enabling*** and ***disabling*** as decided.

282. Under the **Card-Issuing Theory**, as discussed with limitation 2[a], Dua's PIN/fingerprint entry to unlock the wallet application and disable the locked function on the wallet application constitutes ***enabling a first function*** and ***disabling a second function of the smartphone***. This is similar to Patent Owner's infringement read. EX1016 at 65.

283. Further, in my opinion, a POSITA would find that Dua renders as obvious ***repeatedly sensing*** a PIN/fingerprint entry and ***repeatedly deciding*** … ***whether*** … ***to maintain enabled*** the unlocked wallet application ***while maintaining disabled*** the lock function on the wallet application. As contemplated or disclosed by Dua, the wireless device could end up being lost, stolen, or otherwise ending up in possession of someone other than the rightful owner. Dua ¶[0451]. This creates a security risk. *See* Dua ¶[0451]. For instance, if the device were lost or taken while a sensitive functionality, including transaction related functionality, was enabled, then the device could be misused. An un-authenticated user could use the wallet application with that functionality. For example, enabled functionality might remain enabled so long as someone (anyone) continued to use the device before it could enter sleep mode. If, however, the device repeatedly prompted the user to re-authenticate in order to maintain the enabled functionality, that risk is reduced.

284. Under the **External-Storage-Authentication Theory**, as discussed with limitations 2[a] and 2[b], Dua's wireless device repeatedly checks for a reader key—***repeatedly sensing the … parameter***. A wireless device can receive a reader key from a POS terminal at any time. *See, e.g.*, Dua ¶[0380], 42:21-25. And the wireless device can concurrently "receiv[e] and process[] multiple incoming reader keys," which means the wireless device checks for reader keys during and after receiving a reader key. Dua ¶[0364].

285. Every time a reader "key … [is] received by the wallet application," the reader key "is used as a search string to locate a specific credential"—***repeatedly deciding, based on comparing a value of the at least one parameter sensed to the criterion***. Dua ¶[0353].

286. Similarly, the wireless device determines when the reader key can no longer be detected—***repeatedly deciding, based on comparing a value of the at least one parameter sensed to the criterion***. A reader key cannot be detected when the wireless device is not nearby the POS terminal. Dua ¶¶[0353]-[0354], [0370]. POS terminals broadcast the reader key to the wireless device, (Dua ¶¶[0353]-[0354], [0370].) and use a "short range wireless link" through short-range wireless communication protocols to communicate to the wireless device. Dua Abstract, ¶¶[0016], [0318].

287. In my opinion, it is obvious to a POSITA to cause, when the registered reader key is no longer detected, the wireless device to perform the following—***responsive to deciding that the value of the … parameter no longer satisfies the criterion*** and ***repeatedly deciding, based on comparing a … parameter … the criterion, whether or not to maintain enabled said first function while maintaining disabled said second function***. **First**, the wireless cuts the real-time, encrypted connection with the external storage and delete any retrieved credentials—***disabling said first function***. And **Second**, the wireless device re-enables PIN entry to launch

the wallet application, to access the credentials, and/or to use credentials—***enabling*** [***the***] ***second function***.

288. Dua already discloses this functionality with a wallet button. Like the reader key, the wallet button opens the wallet application and transmits credentials. Dua ¶¶[0383]-[0384], [0395]; *see also* Dua ¶¶[0399], [0402], [0416]. The wireless device repeatedly checks if the wallet button is pressed. *See* Dua ¶[0386]. When the wireless device no longer detects a pressed wallet button, RF communications for transmitting credentials during a transaction are disabled. Dua ¶[0386]. Moreover, the retrieved credentials are deleted from the wireless device because credentials retrieved from external storage are only held temporarily for a transaction. Dua ¶[0495]. Further, "disabl[ing] RF communications" causes the wallet "application [to] shutdown or go into its normal dormant state." *See* Dua ¶[0383]. A POSITA would understand that this will cut off a real-time connection between the wallet application and external storage.

289. In my opinion, a POSITA would be motivated to apply this system to reader keys. This reduces security risk—risk of inadvertent credential transmission. And Dua recognizes the problem of inadvertent credential transmission. Dua ¶[0383]. Applying this system to reader keys would mean that RF communications to transmit a credential would be disabled when the wireless device no longer detects a registered reader key. Disabling RF communications also means deleting the

credentials retrieved from the external storage because credentials retrieved from the external storage are only held temporarily for a transaction. Dua ¶[0495]. And disabling RF communications causes the wallet application to shut down or transition into its normal dormant state. In turn, this re-enables PIN-entry. The "default security setting in the wallet application is that PIN-entry is required before the wallet application can be 'opened' and any credentials transmitted to an external device." Dua ¶[0366].

(d) Claim 4

(i) 4[pre]: *The method of claim 1,*

290. As addressed in Sections V.C.3.a, it is my opinion that Jain discloses limitation 4[pre].

(ii) 4[a]: *wherein said transmitting by the smartphone first data to a first device is responsive to the at least one parameter having been sensed by the at least one sensor of the smartphone and is further responsive to having determined that the at least one parameter that is sensed satisfies the criterion; and*

291. In my opinion, Dua discloses this limitation. The analysis for limitations 1[a][i] and 1[a][ii] discuss sensing a ***parameter*** … ***by*** … [***a***] ***sensor of the smartphone and*** … ***determin***[***ing***] ***that the*** … ***parameter*** … ***satisfies*** [***a***] ***criterion***. The analysis for limitation 1[b] discuss how the ***transmi***[***ssion***] ***by the smartphone first data to a first device***, under the **Card-Issuance Theory** and **External-Storage-Authentication Theory**, immediately follows (*i.e.*, ***responsive***

to) the ***parameter … sensed … by …*** [***a***] ***sensor of the smartphone and …*** ***determin***[***ing***] ***that the … parameter … satisfies*** [***a***] ***criterion***.

(iii) 4[b]: ***wherein said receiving by the smartphone second data from the first device is responsive to said transmitting by the smartphone the first data and comprises receiving by the smartphone information relating to an acknowledgement and/or authorization to establish and use the capability to perform said at least one financial transaction.***

292. In my opinion, Dua discloses this limitation. The analysis for limitation 1[b] discusses ***transmi***[***ssion***] ***by the smartphone the first data***. The analysis for limitation 1[c] discusses how the ***rece***[***ption***] ***by the smartphone second data from the first device***, under the **Card-Issuance Theory** and **External-Storage-Authentication Theory**, immediately follows (*i.e.*, ***responsive to***) ***transmitting by the smartphone the first data***.

293. Per the analysis for limitation 1[c], Dua discloses ***receiving … information relating to … authorization***. Limitation 1[c] recites ***receiving … second data … comprising … authorization***, thereby requiring ***receiving … information relating to … authorization***. Because Dua discloses limitation 1[c], Dua discloses ***receiving information relating to … authorization***.

294. Because Dua discloses ***receiving information relating to … authorization***, Dua discloses limitation 4[b]. Limitation 4[b] separates terms by ***and/or—receiving by the smartphone information relating to an***

acknowledgement and/or authorization to establish and use the capability to perform said at least one financial transaction.

(e) Claim 5

(i) 5[pre]: *The method of claim 1, further comprising:*

295. As addressed in Sections V.C.3.a, it is my opinion that Jain discloses limitation 5[pre].

(ii) 5[a]: *responsive to performing a financial transaction, causing data to be transmitted selectively to at least one device and further causing data to be received selectively from at least one device.*

296. In my opinion, Dua discloses this limitation. Dua's wireless device transmits a credential to a point-of-sale reader during a transaction—***responsive to performing a financial transaction, causing data to be transmitted selectively to at least one device***. Dua Abstract, ¶¶[0015]-[0016], [0041], [0293], [0314]-[0315], [0365].

297. Alternatively, the wireless device transmits multiple credentials to a point-of-sale reader. *See, e.g.*, Dua ¶[0359]. And each credential is a separate financial transaction—***performing a financial transaction***. *See* Dua ¶¶[0357]-[0360]. Credentials are sent sequentially. *See* Dua ¶¶[0357]-[0360]. Because later credentials are only sent after an earlier or first credential is sent, the later credentials

are ***transmitted*** to the POS terminal in ***respons***[***e***] ***to performing a financial transaction***.

298. Alternatively, Dua discloses, or POSITA would find it obvious, that communication protocols cause the wireless device to ***transmit***[] data to the POS in ***respons***[***e***] ***to performing a financial transaction***. Communication protocols used by the wireless device cause the wireless device to close the communication channel with the POS terminal after ***performing*** [***the***] ***financial transaction***.

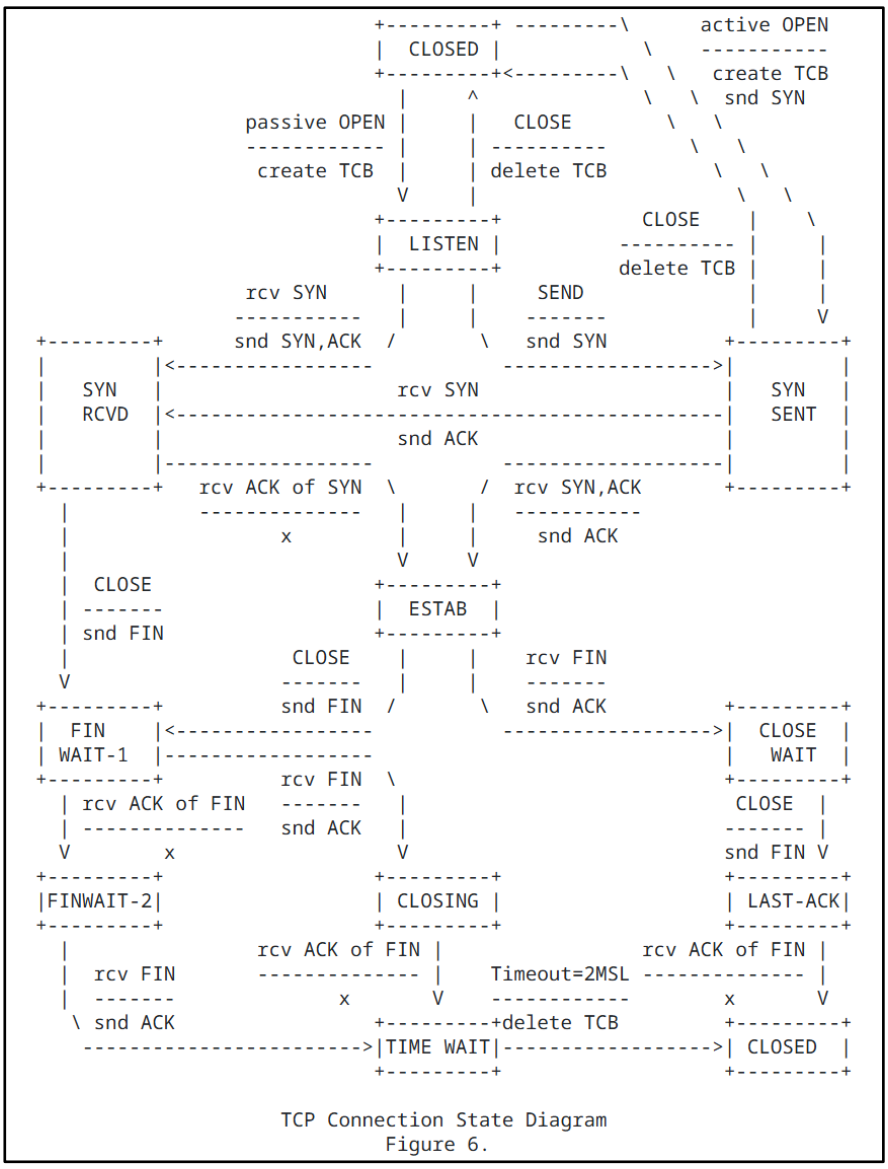
299. The wireless device sets up a "peer-to-peer communication session … through Near Field Communication." Dua Abstract, ¶[0016], Claim 38. Peer-to-peer communications utilize the "Transmission Control Protocol (TCP)," as TCP is a "host-to-host protocol." EX1040 at 1. And Dua discloses the use of TCP between the wireless device and POS terminal. *See* Dua ¶¶[0101], [0205], [0279], [0311], [0488].

300. Or Dua makes it obvious to use TCP between the wireless device and POS terminal. The communication session between the wireless device and POS terminal is "peer-to-peer" which fits how TCP is "intended for use as a highly reliable host-to-host protocol." Dua Abstract, ¶[0016], Claim 38. Dua also references how TCP is more useful where more data is being trafficked. *See* Dua ¶¶[0205], [0359]. This can be the case for the communications between the wireless

device and POS terminal, potentially requiring multiple reader keys, encryption keys, and credentials to be transferred between the two. *See* Dua ¶¶[0205], [0359].

301. After the wireless device completes the financial transaction, the wireless device sends a message to close the TCP peer-to-peer communication channel. *See* Dua ¶[0182], FIG. 4. TCP requires that "[w]hen two processes wish to communicate, their TCP's must first establish a connection (initialize the status information on each side. [And] [w]hen ... communication is complete, the connection is terminated or closed … ." EX1040 at 5. And "clearing of a connection … involves the exchange of segments, in this case carrying the FIN control flag." EX1040 at 12.

302. The connection closing is seen in the more fulsome description of the TCP model is provided in Figure 6, from EX1040.



TCP Connection State Diagram
Figure 6.

The states "FIN-WAIT-1", "FIN-WAIT-2", and "CLOSING" indicate messages from the remote host (*e.g.*, POS terminal) to close out the communication channel. *See* EX1040 at 21-22. "FIN-WAIT-1 … represents waiting for a connection termination request from the remote TCP, or an acknowledgment of the connection termination request previously sent." EX1040 at 21-22. "FIN-WAIT-2 … represents waiting for a connection termination request from the remote TCP."

EX1040 at 21-22. "CLOSING … represents waiting for a connection termination request acknowledgment from the remote TCP." EX1040 at 21-22.

303. Moreover, Dua implements a similar process with the communication channel between the wireless device and WCM. Dua ¶[0182], FIG. 4. When neither the wireless device or WCM has more data to transfer, the communication session is closed out, where the wireless device sends a "BYE" message to the WCM to close out the channel. Dua ¶[0182], FIG. 4.

304. Dua also discloses ***further causing data to be received selectively from at least one device***. After a transaction is complete, the POS terminal transmits to the wireless device an indication of a "successful transmission of credentials to [the POS] reader." Dua ¶¶[0364]-[0365]; *see also* Dua ¶¶[0015], [0041], [0293]. In other words, after a transaction is complete, the wireless device receives a message from the POS terminal indicating a "successful transmission of credentials"—***responsive to performing a financial transaction, … further causing data to be received selectively from at least one device***. Dua ¶¶[0364]-[0365]; *see also* Dua ¶¶[0015], [0041], [0293].

(f) Claim 6

(i) 6[pre]: *The method of claim 1,*

305. As addressed in Sections V.C.3.a, it is my opinion that Jain discloses limitation 6[pre].

(ii) **6[a]:** ***wherein said transmitting by the smartphone first data to a first device and receiving by the smartphone 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.***

306. In my opinion, Dua discloses this limitation. Limitations 1[b] and 1[c] discuss the transmission and reception of data between the wireless device and wireless credential manager in the **Card-Issuance Theory** or the wireless device and the external storage in the **External-Storage-Authentication Theory**—***transmitting by the smartphone first data to a first device and receiving by the smartphone second data from the first device***.

307. Dua's wireless device is capable of using a number of wireless communication channels and protocols. And transmission and reception of the data related to limitations 1[b] and 1[c] can occur across those various wireless communication channels and protocols. Dua ¶¶[0016], [0041], FIGS. 3, 8; *see also* Dua ¶[0494]. For instance, Wifi could be used—***using unlicensed frequencies … [and/or] a WiFi air interface protocol***, including Wifi. Dua ¶¶[0016], [0041], FIGS. 3, 8; *see also* Dua ¶[0494].

308. Because limitation 6[a] separates terms by "***and/or***," Dua discloses limitation 6[a]—***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.

(g) Claim 7

(i) 7[pre]: *The method of claim 1,*

309. As addressed in Sections V.C.3.a, it is my opinion that Jain discloses limitation 7[pre].

(ii) 7[a]: *wherein said paying for a product further comprises deducting/withdrawing an amount of money from an account.*

310. In my opinion, Dua discloses this limitation. As discussed with limitation 1[f], Dua discloses ***paying for a product*** with the smartphone's wallet application. For instance, Dua describes paying for groceries and train tickets through such as groceries and train tickets. Dua Abstract, ¶[0352].

311. Paying for the product requires ***deducting/withdrawing an amount of money from an account***. And any number of accounts or types of accounts could be used for the withdrawal, such as an account linked to a debit card credential in the wallet application that was used by the wireless device in the transaction. Dua ¶¶[0290], [0336], Claim 44.

(h) Claim 8

(i) 8[pre]: *The method of claim 7,*

312. As addressed in Sections V.C.3.g, it is my opinion that Jain discloses limitation 6[pre].

(ii) 8[a]: *wherein said using unlicensed frequencies comprises using unlicensed frequencies in a Time Division Duplex operation;*

313. In my opinion, Dua discloses this limitation. As discussed with limitation 7[a], Dua's wireless device is capable of using several wireless communication channels. For instance, the wireless device is capable of using Bluetooth and NFC—***using unlicensed frequencies***.

314. At least NFC and Bluetooth constitute ***using unlicensed frequencies in a Time Division Duplex operation***. As discussed with limitation 1[f], NFC and Bluetooth operate ***using unlicensed frequencies***. Further, "NFC systems can take place as [a] half … duplex system"—***Time Division Duplex operation***. EX1032 at 21. And Patent Owner agrees that "NFC, a short-range half duplex communication technology," uses ***Time Division Duplex Operations***. EX1016 at 144.

315. Bluetooth also uses ***Time Division Duplex operations***. Not unlike NFC, Bluetooth can operate on half-duplex. *See* EX1038 at 1.

(iii) 8[b]: *wherein said selectively sending information to at least one device comprises selectively, sending information to the access point maintained by the vendor at the point of purchase counter and to at least one other device that is predetermined; and/or*

316. In my opinion, Dua discloses this limitation. Because Dua discloses limitation 8[a] and 8[c], and because limitations 8[a], 8[b], and 8[c] are separated by "***and/or,***" Dua discloses claim 8. Also, limitation 8[b] mirrors limitation 1[e], further requiring that the ***selectively sending*** is to ***the access point*** of claim 1 and that ***selecting sending information … to at least one other device that is predetermined***. Dua discloses the wireless device sending credentials to a point-of-sale reader (***access point***), which is then forwarded to the issuer system (***at least one other device that is predetermined***). Dua Abstract, ¶¶[0009], [0015], [0041], [0293], [0365], Fig. 8.

(iv) 8[c]: ***wherein the method further comprises selectively receiving information from the access point maintained by the vendor at the point of purchase counter and from at least one other device that is predetermined.***

317. In my opinion, Dua discloses this limitation. As discussed with limitation 5[a], Dua discloses the wireless device receiving communications from the point-of-sale reader—***selectively receiving information from the access point maintained by the vendor at the point of purchase counter***. Dua Abstract, ¶¶[0009], [0015], [0041], [0293], [0365].

318. After completing the transaction, Dua's wireless device receives digital receipts of the transaction from a merchant's wireless credential manager—***selectively receiving information*** … ***from at least one other device that is***

predetermined. The wallet application "receiv[es] digital receipts from merchants." Dua ¶[0430]. A digital receipt is "record of payment transaction … during a … transaction using the wallet application." Dua ¶[0430]. The receipt can be "sen[t] … to the wallet application via a number of methods." Dua ¶[0432]. For instance, the merchant could use a "WCM deployed at the merchant's site to issue digital receipts to the wallet application." Dua ¶[0433]. Regardless, the wireless device receives a receipt associated with an underlying transaction from the merchant's WCM—***selectively receiving information … from at least one other device that is predetermined***.

(i) Claims 9-16

319. In my opinion, claims 9-16 are substantively identical to claims 1-8, and thereby disclosed by Dua. The only difference is that claims 9-16 are directed to "[a] smartphone that is configured to perform operations," whereas claims 1-8 are directed to "[a] method of operating a smartphone in performing at least one financial transaction." This distinction is immaterial since Dua discloses both methods and systems. Dua Title.

VI. Secondary Considerations of Non-Obviousness

320. 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.

321. In my opinion, there is a lack of commercial success for any product practicing the ’172 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.

322. In my opinion, there was no long-felt, unresolved need met by the ’172 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 ’172 patent. To the extent wide-scale deployment in the United States post-dated the ’172 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 ’172 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.

VII. Conclusion

323. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject

to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

* * *

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

Respectfully submitted,

Date: May 2, 2025

Kevin C. Almeroth, Ph.D.