

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.,

Petitioner,

v.

TELCOM VENTURES LLC.,

Patent Owner.

Case No. IPR2025-00974

U.S. Patent No. 10,674,432

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 10,674,432**

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. MANDATORY NOTICES AND FEES	1
A. Real Party-In-Interest	1
B. Related Matters.....	1
C. Counsel and Service Information	2
D. Payment of Fees	2
E. Requirements for Inter Partes Review	2
III. GROUNDS	3
IV. STATE OF THE ART	3
V. '432 PATENT.....	5
A. Specification.....	5
B. Prosecution History	6
VI. PERSON OF ORDINARY SKILL	7
VII. CLAIM CONSTRUCTION	7
VIII. GROUNDS	7
A. Ground 1: Jain (EX1017)	7
B. Ground 2: Dua (EX1018).....	46
C. Secondary Considerations	77
IX. STIPULATION	78
X. CONCLUSION.....	79

EXHIBIT LIST

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

EX1020	U.S. Patent Appl. Pub. No. 2010/0082490 (“Rosenblatt”)
EX1021	U.S. Patent Appl. Pub. No. 2009/0307140 (“Mardikar”)
EX1022	“Product Overview”, Vivotech (Jun. 27, 2007), https://web.archive.org/web/20070627155330/ http://www.vivotech.com/products/vivo_pay/index.asp
EX1023	“Kyocera Wireless Mobile Phones Excel in Cellular South Wireless Wallet Consumer Trial”, Kyocera (Oct. 18, 2007), https://americas.kyocera.com/press-releases/press-releases_201503201874.htm
EX1024	U.S. Patent Appl. Pub. No. 2005/0137977
EX1025	U.S. Patent Appl. 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	Exhibit Intentionally Omitted
EX1032	Exhibit Intentionally Omitted
EX1033	Wall Street Journal, Vivotech (Aug. 12, 2005), https://web.archive.org/web/20060915080521if_/http://www.vivotech.com:80/newsroom/coverage/Videos/Wall_Street_Journal/Wall_Street_Journal.wmv
EX1034	Near Field Communication - Interface and Protocol (NFCIP-1), Standard ECMA-340 (December 2002)
EX1035	NFC Forum News Conference, NFC Forum (June 5, 2006)

EX1036	Dean A. Gratton, “Developing Practical Wireless Applications”, Elsevier Digital Press (2007)
EX1037	Jacki Katzman, “NFC Forum Unveils Technology Architecture and Announces Initial Specifications and Mandatory Tag Format Support”, NFC Forum, at 3 (June 5, 2006)
EX1038	Exhibit Intentionally Omitted
EX1039	U.S. Pub. No. 2010/0082445
EX1040	Exhibit Intentionally Omitted
EX1041	Exhibit Intentionally Omitted
EX1042	“iPhone Premieres This Friday Night at Apple Retail Stores”, Apple (Jun. 28, 2007), https://www.apple.com/newsroom/2007/06/28iPhone-Premieres-This-Friday-Night-at-Apple-Retail-Stores/
EX1043	“Review: Apple iPhone Bluetooth Headset”, Apple Insider (Jul. 30, 2007), https://appleinsider.com/articles/07/07/30/review_apple_iphone_bluetooth_headset
EX1044	“Eight Bluetooth Headsets Under the Microscope,” Treonauts (Aug. 12, 2005), https://blog.treonauts.com/2005/08/eight_bluetooth.html
EX1045	“Getting Base Stations Ready for LTE”, EETimes (April 17, 2007), https://www.eetimes.com/getting-base-stations-ready-for-lte/
EX1046	3rd Generation Partnership Project; Technical Specification Group Radio Access Network; LTE Physical Layer – General Description (Release 8), 3rd Generation Partnership Project, March 2007
EX1047	Near Field Communication - Interface and Protocol (NFCIP-1), Standard ECMA-340 (2nd Edition, December 2004)

LIST OF CHALLENGED CLAIMS

Claim	Limitation
1[pre]	A method of operating a smartphone in performing a plurality of financial transactions, the method comprising:
1[a][i]	responsive to at least one physiological parameter having been sensed by at least one sensor of the smartphone,
1[a][ii]	enabling a mode to communicate by the smartphone information requesting an authorization;
1[b]	while the mode is enabled, transmitting by the smartphone first data to a first device, the first data relating to a plurality of financial transactions to be conducted;
1[c]	receiving by the smartphone second data from the first device responsive to said transmitting by the smartphone the first data, the second data relating to the plurality of financial transactions to be conducted and differing from the first data;
1[d]	performing a first transaction of the plurality of financial transactions by:
1[e]	detecting by the smartphone that a proximity condition is satisfied between the smartphone and a first entity, wherein the first entity is distinct from the first device;
1[f]	establishing, using a first air interface, a wireless short-range communications link between the smartphone and the first entity, in response to the proximity condition having been satisfied between the smartphone and the first entity;
1[g]	receiving, using the first air interface, a short-range signal from the first entity; and
1[h]	responsive to receiving the short-range signal from the first entity, sending by the smartphone to the first entity over the first air interface, information associated with the second data received from the first device; and

Claim	Limitation
1[i]	independent of performing said first transaction, receiving by the smartphone a communications service from a wireless network, using a second air interface that differs from the first air interface,
1[j]	wherein said transmitting by the smartphone first data and said receiving by the smartphone second data are performed over an air interface that differs from the first air interface.
2[pre]	The method of claim 1,
2[a]	wherein establishing the wireless short-range communications link between the smartphone and the first entity is performed responsive to at least one physiological parameter having been sensed by at least one sensor of the smartphone.
3[pre]	The method of claim 1,
3[a]	wherein sending by the smartphone to the first entity, information associated with the second data, is performed responsive to at least one physiological parameter having been sensed by at least one sensor of the smartphone.
4[pre]	The method of claim 1,
4[a]	wherein sending by the smartphone to the first entity, information associated with the second data, is performed responsive to a value of at least one parameter associated with the smartphone.
5[pre]	The method of claim 1, wherein the method further comprises:
5[a]	performing a second transaction of the plurality of financial transactions by:
5[b]	detecting by the smartphone that a proximity condition is satisfied between the smartphone and a second entity, wherein the second entity is distinct from the first entity and is further distinct from the first device;
5[c]	establishing, using the first air interface, a wireless short-range communications link between the smartphone and the second entity, in

Claim	Limitation
	response to the proximity condition having been satisfied between the smartphone and the second entity;
5[d]	receiving, using the first air interface, a short-range signal from the second entity; and
5[e]	responsive to receiving the short-range signal from the second entity, sending by the smartphone to the second entity over the first air interface, information associated with the second data received from the first device.
6[pre]	The method of claim 1,
6[a]	wherein said transmitting by the smartphone first data to a first device includes transmitting by the smartphone data relating to a request to pay for a transaction; and
6[b]	wherein said receiving by the smartphone second data from the first device includes receiving by the smartphone data relating to an acknowledgement and/or authorization of enabling a mode/function to pay for a transaction.
7[pre]	The method of claim 1, comprising:
7[a]	transmitting by the smartphone third data to a second device; the second device being distinct from the first device and further being distinct from the first entity; and
7[b]	receiving by the smartphone fourth data from the second device relating to an acknowledgement and/or authorization of enabling a mode/function to pay for a financial transaction,
7[c]	wherein said transmitting by the smartphone third data to a second device and said receiving by the smartphone fourth data from the second device are performed over the air interface that differs from the first air interface.
8[pre]	The method of claim 1, wherein said operations further comprise:

Claim	Limitation
8[a]	responsive to performing a financial transaction, causing data to be transmitted selectively to a plurality of predetermined devices and further causing data to be received selectively from said plurality of predetermined devices.
9[pre]	The method of claim 1,
9[a]	wherein the second air interface comprises an Orthogonal Frequency Division Multiplexed and/or an Orthogonal Frequency Division Multiple Access (OFDM/OFDMA) technology.
10[pre]	A smartphone that is configured to perform operations associated with a plurality of financial transactions; the operations comprising:
10[a]	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;
10[b]	while the mode is enabled, transmitting first data to a first device as a precursor to performing the plurality of financial transactions; and
10[c]	receiving second data from the first device responsive to said transmitting the first data;
10[d]	performing a first financial transaction of the plurality of financial transactions by:
10[e]	detecting by the smartphone that a proximity condition is satisfied between the smartphone and a first entity, wherein the first entity is distinct from the first device;
10[f]	establishing, using a first air interface, a wireless short-range communications link between the smartphone and the first entity, in response to the proximity condition having been satisfied between the smartphone and the first entity;
10[g]	receiving, using the first air interface, a short-range signal from the first entity; and

Claim	Limitation
10[h]	responsive to receiving the short-range signal from the first entity, sending to the first entity over the first air interface, information based on the second data received from the first device; and
10[i]	independent of performing a transaction to pay for one or more items, receiving by the smartphone a communications service from a wireless network, using a second air interface that differs from the first air interface,
10[j]	wherein said transmitting first data and said receiving second data are performed over an air interface that differs from the first air interface.
11[pre]	The smartphone of claim 10,
11[a]	wherein establishing the wireless short-range communications link between the smartphone and the first entity is performed responsive to at least one physiological parameter having been sensed by at least one sensor of the smartphone.
12[pre]	The smartphone of claim 10,
12[a]	wherein sending by the smartphone to the first entity, information based on the second data, is performed responsive to at least one physiological parameter having been sensed by at least one sensor of the smartphone.
13[pre]	The smartphone of claim 10,
13[a]	wherein sending by the smartphone to the first entity, information based on the second data, is performed responsive to a value of at least one parameter associated with the smartphone.
14[pre]	The smartphone of claim 10, wherein the operations further comprise:
14[a]	performing a second financial transaction of the plurality of financial transactions by:
14[b]	detecting by the smartphone that a proximity condition is satisfied between the smartphone and a second entity; wherein the second entity is distinct from the first entity and is further distinct from the first device;

Claim	Limitation
14[c]	establishing, using the first air interface, a wireless short-range communications link between the smartphone and the second entity, in response to the proximity condition having been satisfied between the smartphone and the second entity;
14[d]	receiving, using the first air interface, a short-range signal from the second entity; and
14[e]	responsive to receiving the short-range signal from the second entity, sending by the smartphone to the second entity over the first air interface; information associated with the second data received from the first device.
15[pre]	The smartphone of claim 10,
15[a]	wherein said transmitting by the smartphone first data to a first device includes transmitting by the smartphone data relating to a request to pay for a transaction; and
15[b]	wherein said receiving by the smartphone second data from the first device includes receiving by the smartphone data relating to an acknowledgement and/or authorization of enabling a mode/function to pay for a transaction.
16[pre]	The smartphone of claim 10, wherein said operations further comprise:
16[a]	transmitting third data to a second device; the second device being distinct from the first device and further being distinct from the first entity; and
16[b]	receiving by the smartphone fourth data from the second device relating to an acknowledgement and/or authorization of enabling a mode/function to pay for a financial transaction;
16[c]	wherein said transmitting by the smartphone third data to a second device and said receiving by the smartphone fourth data from the second device are performed over the air interface that differs from the first air interface.

Claim	Limitation
17[pre]	The smartphone of claim 10, wherein said operations further comprise:
17[a]	responsive to performing a financial transaction, causing data to be transmitted selectively to a plurality of predetermined devices and further causing data to be received selectively from said plurality of predetermined devices.

I. INTRODUCTION

The '432 patent is directed to performing “financial transactions” using a “smartphone.” It does not disclose non-obvious technology for performing such transactions. Indeed, using existing cell-phone technology to conduct financial transactions was the subject of intense growth during the early 2000s, with pilot programs and commercial deployments by companies including Nokia, Motorola, Kyocera, and NTT. The technology was mature enough to be the subject of multiple patent publications from this timeframe, including the Jain and Dua references relied upon in this Petition.

II. MANDATORY NOTICES AND FEES

A. Real Party-In-Interest

The real parties-in-interest for Petitioner are Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.

B. Related Matters

The '432 patent was asserted against Petitioner in *Telcom Ventures LLC v. Samsung Electronics Co., Ltd., et al.*, Case No. 2:24-cv-00691-JRG (E.D. Tex., filed August 21, 2024).

Separately, the '432 patent was asserted against an unrelated defendant in *Telcom Ventures LLC v. Apple Inc.*, Case No. 1:24-cv-23837-JEM (S.D. Fla., filed Oct. 4, 2024).

The '432 patent is in the same family as U.S. Patents Nos. 9,462,411, 9,832,708, 10,219,199, 11,770,756, 11,924,743, 11,937,172, and 12,028,793, all also asserted against Petitioner. Petitioner is concurrently filing IPR petitions against these family members.

C. Counsel and Service Information

Electronic service may be made on the email addresses identified below and in the accompanying Power of Attorney.

LEAD COUNSEL	BACK-UP COUNSEL
James M. Glass (Reg. No. 46,729) jimglass@quinnemanuel.com QUINN EMANUEL URQUHART & SULLIVAN, LLP 51 Madison Avenue, 22 nd Floor New York, NY 10010 Tel: (212) 849-7000	Ognjen Zivojnovic (Reg. No. 69,516) ogizivojnovic@quinnemanuel.com Benjamin Kleinman (Reg. No. 66,856) benjaminkleinman@quinnemanuel.com QUINN EMANUEL URQUHART & SULLIVAN, LLP 50 California Street, 22nd Floor San Francisco, California 9411 Tel: (415) 875-6600

D. Payment of Fees

The Office is authorized to charge the fee required for this Petition (and any additional fees) to Deposit Account No. 50-5708.

E. Requirements for Inter Partes Review

Petitioner certifies that the '432 patent is available for *inter partes* review, that Petitioner is not barred or estopped, and that 35 U.S.C. §§315(a)-(b) is inapplicable.

III. GROUNDS

Ground	Basis	Reference	Claims
1	§103	Jain	1-17
2	§103	Dua	1-17

IV. STATE OF THE ART

Mobile phones could communicate using a variety of well-known wireless protocols prior to the alleged invention of the '432 patent in late 2008. EX1001 at 1:29-55. The market for mobile phones capable of cellular communications was well-established by the 1990s, with the Nokia 3210 released in 1999 selling over 160 million units. EX1002 ¶¶88. Manufacturers added other standardized wireless communication technology to mobile phones by the early 2000s. The first IEEE standard for Wi-Fi was published in 1997. By 2005, phones with both cellular and Wi-Fi capabilities, such as the 2005 Samsung SCH-i730, were common. *Id.* So too were phones with Bluetooth capabilities, including Nokia 6310 and Samsung SCH-i730. *Id.*

Near-Field Communication (NFC) was also common at that time, and used RFID technology (magnetic field induction) to allow short-range wireless communications between devices. EX1002 ¶¶89. Examples of mobile phones with integrated NFC capabilities include the 2004 Fujitsu F900ic, 2004 Nokia 3220 NFC Shell, and 2007 Nokia 6131 NFC. *Id.*

Manufacturers quickly deployed applications leveraging these capabilities, including 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 phones coupled with Osaifu-Keitai ("Wallet Mobile") software. EX1002 ¶¶90. This technology spread to the U.S., with mobile phone and payment companies teaming up to conduct pilot programs of mobile payment software, including a 2006 pilot by Nokia and MasterCard, a 2007 pilot by Motorola and Discover, and a 2007 pilot by Kyocera and MasterCard, with companies such as ViVOtech releasing full mobile payment solutions. *Id.*; EX1022:



As mobile phones evolved into smartphones and were increasingly used for sensitive activities (*e.g.*, financial transactions) and to store sensitive 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, 2003 Fujitsu F505i, 2004 Pantech GI100, and 2007 Toshiba G500 and G900. For example, mobile phones

used for payments in the 2007 Kyocera and MasterCard trial included fingerprint scanners and required biometric authentication. EX1002 ¶91; EX1023 (describing Kyocera trial of “mobile payment technology” from ViVOtech with “biometric security, with fingerprint scanners... for transactional security on the test handsets”).

V. '432 PATENT

A. Specification

The specification assumes familiarity with “wireless communications device[s]” such as “a wireless/mobile phone, a Personal Digital Assistant (PDA), a smart phone,... etc.” EX1001 at 1:52-67, 3:9-13. It relies on long-established, generic concepts of computer systems such as “authorization” (5:42-44), “sensors” for detecting physiological input (mentioned only at 6:11-31), “short-range communications” (mentioned only at 8:28-32 and 8:53-62), “air interface[s]” (6:60-61, mentioning then-existing interfaces at 7:17-28), and “communications service[s]” (9:10). 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 1:31-32), and assumes that mobile phones could act as digital wallets. EX1001 at 1:42-44. It does not disclose or purport to disclose new or improved means of sensing (including physiological/biometric sensing) or proximity detection. EX1002 ¶38.

B. Prosecution History

On May 9, 2019, the Examiner rejected all claims on the ground of non-statutory obviousness-type double patenting as not patentably distinct from claims of U.S. Patent 10,219,199. EX1009 at 70. Applicant amended the claims and argued this rendered the rejections moot. EX1009 at 148, 154.

On December 17, 2019, the Examiner issued a final rejection, reiterating the requirement for terminal disclaimer. EX1009 at 168. The Examiner also rejected all claims as obvious in view of the combination of Dua with U.S. Patent Publication 2004/0143550. EX1009 at 169. Applicant submitted a request for continued examination and amended the claims again. Applicant argued that Dua did not teach “enabling a mode to communicate... responsive to at least one physiological parameter” in the newly-amended claim. EX1009 at 253. Applicant also submitted a terminal disclaimer disclaiming the terminal part of the term of the ’432 patent that would extend beyond the term of the ’199 patent. EX1009 at 262.

On April 22, 2020 the Examiner noted that Applicant authorized cancelling 16 claims. EX1009 at 278. The Examiner allowed the remaining claims. The Examiner found that the closest prior art of record was Dua, but found that the only limitation that Dua did not teach or suggest is “enabling a mode to communicate... responsive to at least one physiological parameter.” EX1009 at 275-277.

As discussed below for Ground 2 based on Dua, Petitioner respectfully disagrees with the Examiner. Dua expressly teaches enabling a mode to communicate using PIN codes, and that biometrics, including fingerprints, could be used instead of PIN codes. Dua ¶[0366].

VI. PERSON OF ORDINARY SKILL

A person of ordinary skill in the art at the time of the '432 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. More education can supplement for less practical experience, and vice versa. EX1002 ¶¶80-83.

Petitioner's expert, Dr. Almeroth, exceeded this level by the priority date. EX1002 ¶83.

VII. CLAIM CONSTRUCTION

No express constructions are required to find the '432 patent claims invalid. To the extent relevant, Petitioner addresses the plain meaning of certain terms in the analysis for the presented Grounds.

VIII. GROUNDS

A. Ground 1: Jain (EX1017)

1. Background

Filed September 5, 2008 (before the earliest effective filing date of the '432 patent), Jain is prior art under at least pre-AIA 35 U.S.C. §102(e). Jain discloses all

limitations of the '432 claims. Petitioner presents Jain as an obviousness reference in the event Patent Owner argues differences between Jain and the '432 claims.

Jain was not considered by the Examiner during prosecution of the '432 patent. *See* EX1002 ¶45.

While each limitation is addressed in detail in the sections below, given the repetitive and nonsequential nature of the claim language, here is a short, non-limiting overview of Ground 1:

Claim 1 can generally be broken down into a first step of requesting an authorization to engage in financial transactions and a second step of performing those transactions. EX1002 ¶92-97. This first step consists of (1) sensing a physiological parameter; (2) enabling a communications mode; and (3) while the mode is enabled, transmitting first data and receiving second data relating to financial transactions. Jain discloses the same sequence by (1) performing user authentication via biometrics (*e.g.*, Fig. 7B, steps 734-742); (2) if user is authorized, updating device signatures to enable cellular communication with a financial institution (*e.g.*, Fig. 7A, step 714); and (3) using cellular communications to request and receive an activation code from the financial institution (*e.g.*, Fig. 9, steps 920-926).

Claim 1 also requires a second step of performing the financial transaction, consisting of (1) detecting if the smartphone is in proximity of a first entity; (2)

establishing a short-range communications link if proximity condition is satisfied; (3) receiving a short-range signal and sending information associated with data related to the financial transaction. Again, Jain discloses the same sequence by detecting if the mobile device is sufficiently close to a POS terminal to receive a transaction request via a short-range NFC signal (*e.g.*, ¶[0023], [0027]) and transmitting a transaction response containing information associated with a payment account (*e.g.*, ¶[0027]).

2. Claim 1

(a) 1[pre]

Jain describes operating a “mobile device 110,” which can be a “*smartphone*,” with a “transaction card 112” attached thereto or incorporated therein to “wirelessly execut[e] transactions” with point-of-sale terminal 114. EX1002 ¶98; Jain ¶¶[0005], [0018], [0021], [0029], FIG 1 (annotated):

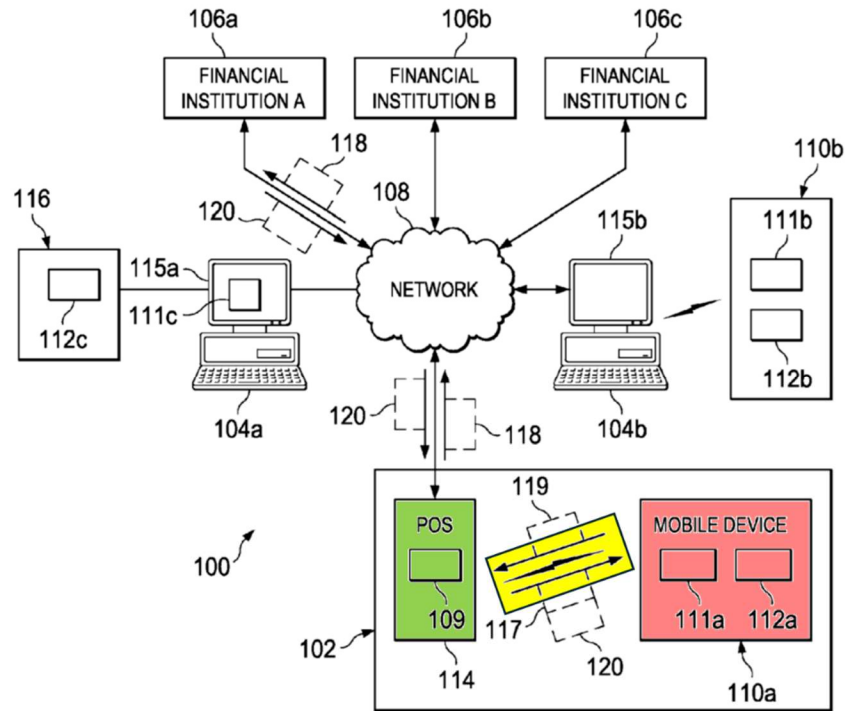


FIG. 1

For example, Figure 1 shows mobile device 110a with transaction card 112a and GUI 111a (red) wirelessly executing transactions with POS device 114 (green). Jain ¶[0019]. POS device 114 transmits transaction request 117 to mobile device 110 when in close proximity. Jain ¶[0027]. Mobile device 110 then sends transaction response 119 that identifies information associated with a payment account. Jain ¶[0027]. POS device 114 then sends transaction authorization request 118 to financial institution 106 (one of 106a, 106b, or 106c). Jain ¶[0027]. The financial institution transmits authorization response 120 to POS device 114, which then transmits it to mobile device 110. Jain ¶[0027]. This response may include a payment transaction receipt presentable to the user through the mobile device's GUI. Jain

¶[0027]. The exchange between device 110 and POS 114 uses short-range signals such as NFC or Bluetooth. Jain ¶[0023]. *See* EX1002 ¶99.

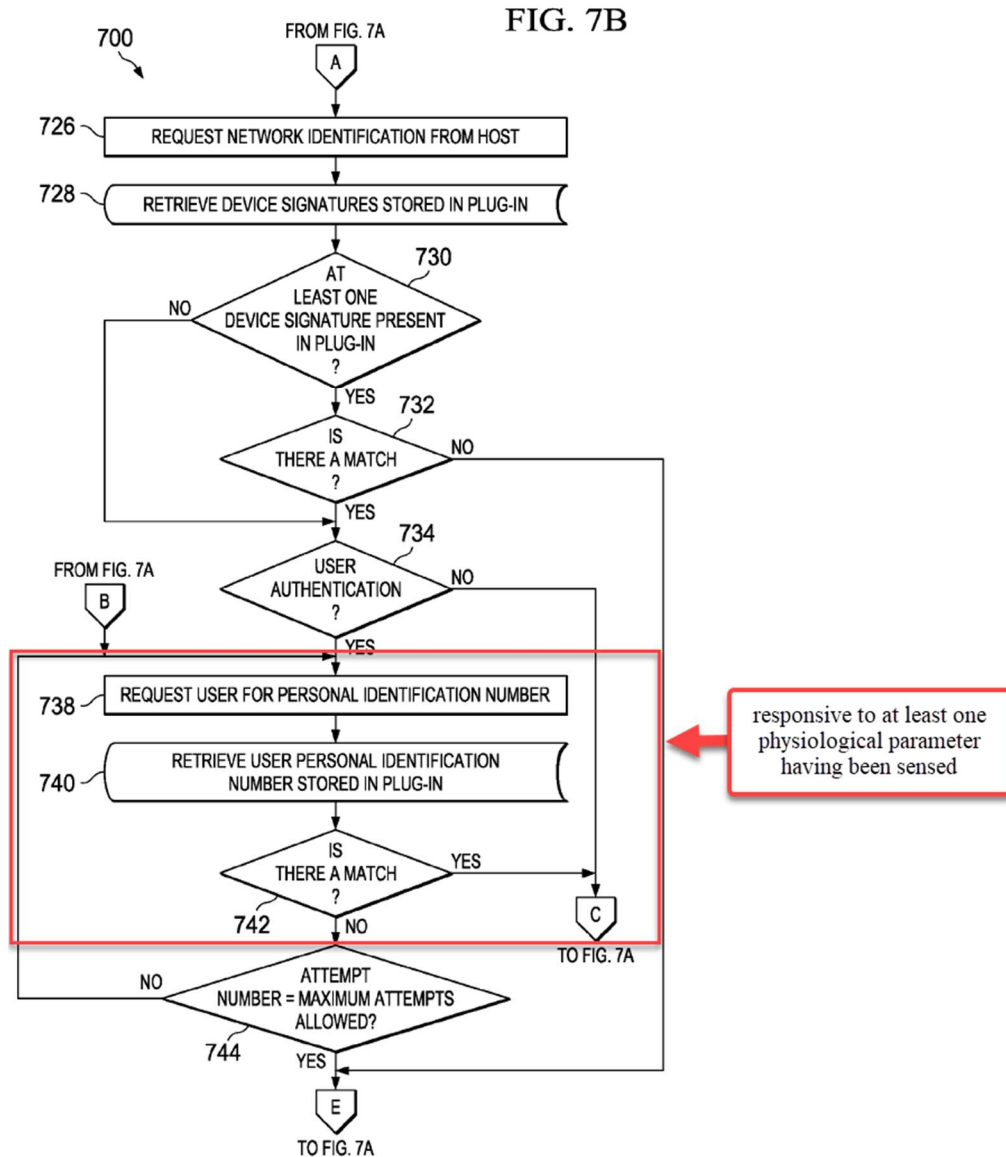
Jain interfaces mobile device 110 (*e.g.*, “smartphone” (¶[0018])) with transaction card 112 that “convert[s] mobile device 110 to a contactless payment device loaded with a financial vehicle (FV) that may be, for example, a credit card, debit card, gift card and/or other retail payment product” (¶[0029]). In such embodiments, transaction card 112 is part of mobile device 110. Jain ¶[0019], Fig. 1 (showing transaction card 112a within mobile device 110a); EX1002 ¶100.

If Patent Owner argues transaction card 112 cannot be considered part of mobile device 110, Jain at least renders obvious implementing the processes discussed herein using transaction card 112 integrated into mobile device 110. EX1002 ¶¶101-105. A POSITA would make this change because separability of the transaction card is not always advantageous (*e.g.*, smartphone vendor might find it commercially advantageous to provide transaction-card functionality with their smartphone and not allow interoperability with other devices). EX1002 ¶¶101-105. Also, integrating transaction card 112 with mobile device 110 allows the host device to achieve the benefits disclosed in Jain without incurring the cost of implementing an independent transaction card, and leveraging components of the mobile device 110. EX1002 ¶104. Finally, incorporating transaction card 112 into mobile device 110 protects against inadvertent loss of transaction card 112 (*e.g.*,

becoming detached from mobile device 110 without the user noticing). EX1002 ¶105.

(b) 1[a][i]

The claim begins with a prerequisite before requesting authorization to engage in financial transactions. Jain discloses this prerequisite in steps 734-742 of Fig. 7B. EX1002 ¶¶106-108. Specifically, Jain discloses an authentication process for “automatically bootstrapping” transaction card 112 to mobile device 110, which includes authenticating a user using biometrics (e.g. fingerprint) (*at least one physiological parameter*). Jain ¶¶[0072], [0075], Fig. 7B (annotated):



Jain teaches, at step 738, the smartphone receives a PIN via the smartphone's touch screen or keypad. Jain ¶¶[0022], [0075]. At step 740, the smartphone retrieves a locally-stored PIN. Jain ¶[0075]. At step 742, the smartphone determines whether the user-inputted PIN matches the locally-stored PIN. Jain ¶[0075], Fig. 7B.

Rather than “entering a PIN,” “the user may be authenticated using... biometric information (e.g., fingerprint)”—*i.e. one physiological parameter*. Jain

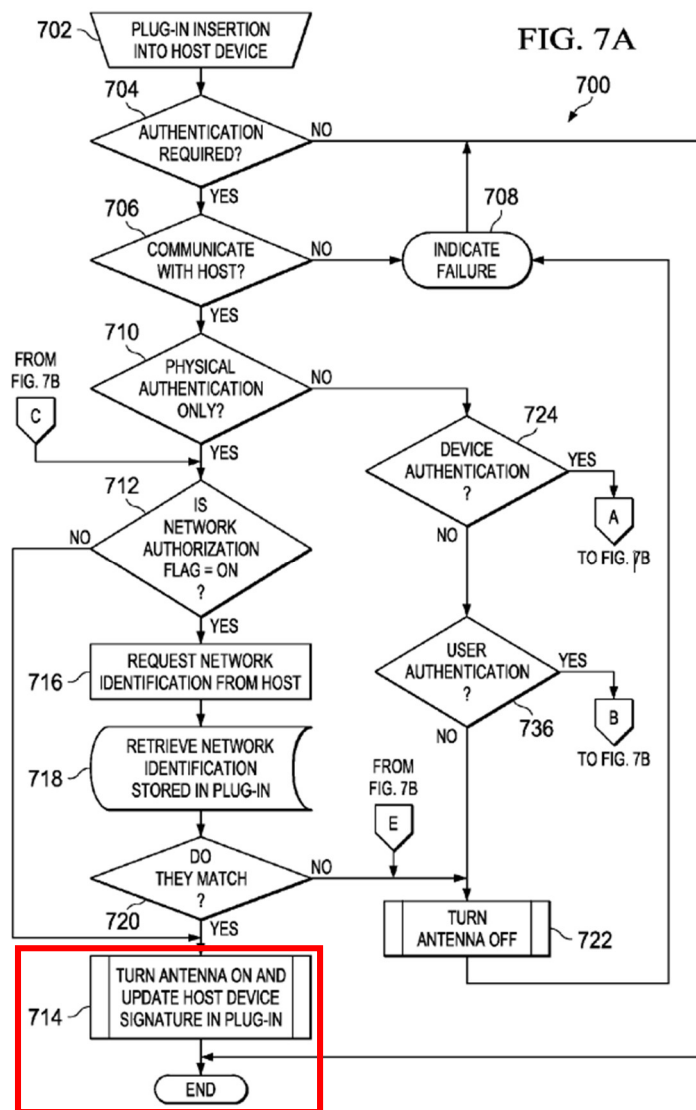
¶[0075]. Thus, Jain discloses performing steps 738, 740, and 742 in the context of biometric verification, where step 738 includes sensing “biometric information” using a biometric reader (*at least one sensor of the smartphone*), step 740 includes retrieving locally-stored biometric information, and step 742 includes determining if the sensed biometric information matches the stored biometric information. EX1002 ¶¶106-108.

Confirming this limitation is met, Patent Owner alleges in its infringement contentions that the use of biometric verification is itself sufficient to show *at least one physiological parameter having been sensed by at least one sensor of the smartphone*. EX1016 at 8-13; *see* EX1002 ¶109.

At a minimum, it would be obvious to implement Jain’s teaching of “authentication using... biometric information” in this manner, and a POSITA would be aware of such implementations. EX1002 ¶¶110-112; *see* EX1021 ¶¶[0040]-[0042]; EX1024 ¶¶[0009], [0025]; EX1025 ¶¶[0044], [0086]-[0092]; EX1026 at 28-29, 196; EX1027 at 1370-73. Biometric authentication is used to ensure a current user’s biometric information matches the biometric information of the device’s rightful owner. This entails first storing the owner’s biometric information during a setup stage and then comparing the stored biometric information to the current user’s information. EX1002 ¶110.

(c) 1[a][ii]

Limitation 1[a][ii] is a second prerequisite to requesting authorization: *enabling a mode to communicate*. Jain discloses this limitation. EX1002 ¶113-114. In response to authenticating the user in steps 738-744 of Fig. 7B, Jain process 700 returns to step 712 (label C in both figures) and proceeds to step 714: “turn antenna on and update host device signature in plug-in” (claimed *enabling*). Jain ¶¶[0072]-[0075] and Fig. 7A (annotated):



Once the host-device signature is updated (step 714) to match the host device, the transaction card completes the bootstrap operation and can communicate with the host; otherwise, the “host device is rejected [and] bootstrap is aborted.” Jain ¶[0065]. Only after bootstrapping/authentication (Figure 7) can activation (Figure 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 mobile device 110 to engage in the cellular communication with a financial institution as part of process 900 (*enable[s] a mode to communicate by the smartphone information*). EX1002 ¶¶113-114.

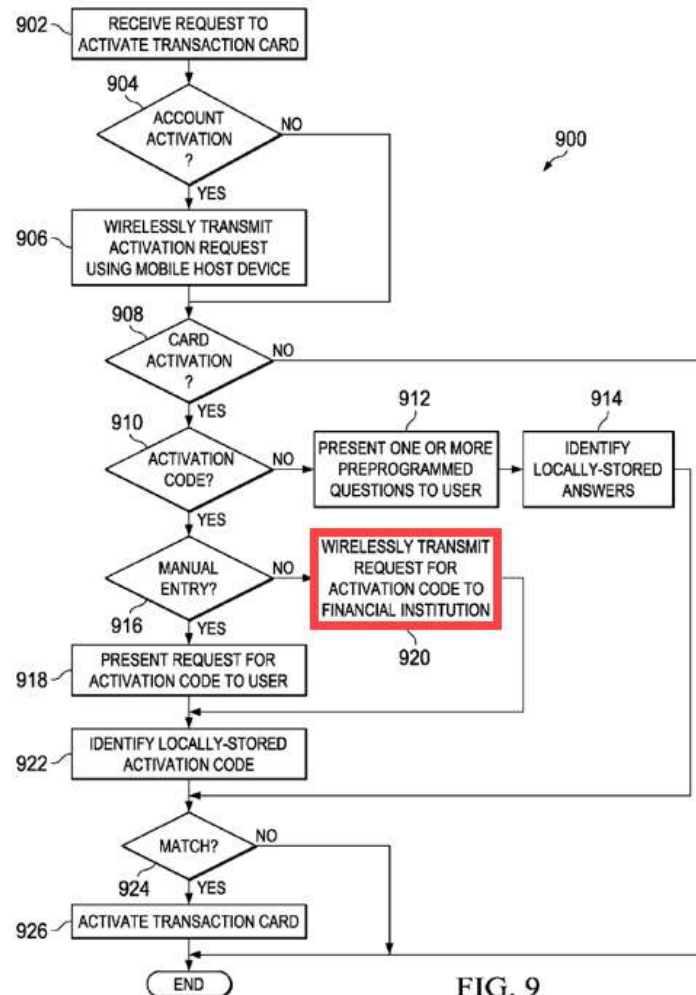
As explained below for limitations 1[b] and 1[c], process 900 entails “*requesting an authorization*” to perform financial transactions. EX1002 ¶¶115, 122-125.

(d) 1[b] and 1[c]

With the claimed *sensing* and *enabling* complete, claim 1 recites steps of *transmitting first data* and *receiving second data relating to the financial transactions to be conducted*.

After the user is authenticated by biometrics and the host device signature is updated to allow mobile device 110 with transaction card 112 to communicate with

a financial institution, Jain's mobile device 110 then performs "method 900 for activating a wireless transaction system" with the financial institution. Jain ¶[0080]. During step 920, smartphone 110 "wirelessly transmits a request for the activation code [request/] *an authorization*]" using the cellular radio technology" (*transmitting by the smartphone first data*) of the smartphone to the financial institution (*to a first device*). Jain ¶[0081], Fig. 9 (annotated below); EX1002 ¶¶117, 122-125.



In response to the step 924 request, mobile device 110 (*smartphone*) receives an activation code (*second data*) from the financial institution (*first device*). The

received activation code is checked against a stored activation code (retrieved at step 922). Jain ¶[0081]. If the activation codes match, “the transaction card is activated” at step 926. Jain ¶[0081]. This “activation process may include activating the transaction card and/or financial account” (Jain ¶[0026]), which allows the transaction card to perform payments with the associated financial account. Jain ¶[0071].

Thus, step 920 and 924 are performed to “activat[e] the transaction card and/or financial account.” Jain ¶[0026]; EX1002 ¶¶116-118. This activation, in turn, involves the financial institution signifying that the financial vehicle carried on the card is activated and allowing the card to wirelessly execute multiple financial transactions with a retail terminal. Jain ¶¶[0005], [0071]. Because the matching “activation code” allows the user to use the mobile device with the transaction card across multiple financial transactions, both the request for that activation code (*first data*) and the activation code itself (*second data*) relat[e] to a plurality of financial transactions. Because the first data is a request for activation code and the second data is the activation code, the *second data... differ[s] from the first data*. EX1002 ¶119.

Confirming this limitation is met, Patent Owner alleges in its infringement contentions that adding a financial card to a smartphone digital wallet and verifying it are sufficient to show 1[b] and 1[c]. EX1016 at 14-20; see EX1002 ¶120.

A POSITA would further understand that *receiving* the activation code *(second data) relat[es] to the plurality of financial transactions to be conducted* because the financial institution would not provide a matching activation code to a smartphone's request unless the smartphone is authorized to perform payment services with the financial institution. EX1002 ¶¶121-125. Indeed, Patent Owner asserts that receiving an issued credit card for conducting financial transactions is sufficient to establish “*receiving... second data relating to the plurality of financial transactions to be conducted .*” EX1016 at 14-20. This is supported by step 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; EX1002 ¶121.

(e) 1[d] and 1[e]

The next limitations relate to steps for performing the financial transactions. After enabling a mode to communicate and transmitting and receiving data relating to financial transactions, including authentication process 700 and activation process 900, Jain's mobile device 110 can execute contactless payment transactions with a nearby POS device (including *a first transaction of the plurality of financial transactions*, as discussed for limitations 1[e]-[j]) using short-range signals, such as NFC or “proximity signals.” Jain ¶¶[0023], [0029]; EX1002 ¶¶126-128. The mobile

device first “wirelessly receive[s] a request from the POS device 114 to execute a transaction and/or... provide a response.” Jain ¶[0023]. A POSITA would understand that Jain’s mobile device is only able to process the “request” if sufficiently close to POS device (*the first entity... distinct from the first device*) to actually receive and decode the short-range signal containing the request (*detecting by the smartphone that a proximity condition is satisfied*). EX1002 ¶¶126-128; EX1047 at §§10, 11, Figure 5; *see* EX1036 at 220.

Specifically, device 110’s transaction card 112 “may execute transactions with POS device 114 using short-range signals such as NFC (e.g., ISO 18092/ECMA 340),... Bluetooth,... proximity signals, and/or other signals compatible with retail payment terminals.” Jain ¶[0023]. Jain’s NFC and other short-range wireless protocols are only effective if an underlying signal of sufficient strength is detected such that the device and terminal can communicate using that protocol. EX1002 ¶¶128-32; EX1047 at §§10, 11, Figure 5; EX1035 at 4, 36; EX1036 at 220; EX1037 at 3. Signal strength rapidly deteriorates as distance increases. EX1002 ¶129; EX1035 at 4, 36; EX1037 at 3. Indeed, Jain recognizes that NFC communication may require a proximity of “10 cm or less.” Jain ¶[0030]. Accordingly, for Jain’s mobile device and the POS device to communicate over NFC, they must be sufficiently close, which a POSITA would understand corresponds to *detecting by the smartphone that a proximity condition is satisfied between the smartphone and*

a first entity (e.g., the mobile device and POS device are “10 cm or less” from each other). EX1002 ¶129.

Also, the claimed *detecting* occurs earlier in Jain’s NFC exchange, prior to sending payment information. Jain teaches that its NFC “wireless connection” is based on “ISO 18092/ECMA 340” standards. Jain ¶¶[0023], [0051], [0018]; EX1002 ¶130. The ECMA-340 Interface and Protocol Standard for NFC¹ explains that an NFC “transaction” requires an “initialization” (described in ECMA-340 §11) and then a “data exchange” (described in §12). EX1047 at §4.26, §10, Figure 5; EX1002 ¶131. ECMA-340 specifies two devices (“Initiator” and “Target”) and two communication modes (“Passive” and “Active”). EX1047 §1, §4.1, §4.7, §4.17,

¹ ECMA 340 is a well-known communications standard that defined NFC. EX1002 ¶131. This standard was publicly available and known to a POSITA even at the time of Jain’s filing, and thus predates the earliest priority date of the challenged patent. *Id.* Exhibit 1047 is a true and correct copy of the 2nd edition of “ECMA-340,” which was publicly available as of December 2004 and not updated again until June 2013. *Id.*; <https://ecma-international.org/publications-and-standards/standards/ecma-340/>. This version was also published as “ISO 18092” cited in Jain. *Id.* The disclosures of ECMA-340 referenced here are found in both the 1st edition (released December 2002) and the 2nd edition. *Id.*; compare EX1047 with EX1034.

§4.23, §7; EX1002 ¶132. But it does not matter whether Jain's POS device or mobile device is the "Initiator" or "Target," or what communication mode they use: every combination results in Jain's mobile device (*smartphone*) detecting a ***proximity condition has been satisfied*** and then establishing a short-range link used for subsequent communications. EX1002 ¶133. Specifically, in both modes, an "Initiator" device "shall activate its RF field" and a "Target" device then "shall be activated by the RF field of the Initiator." EX1047 §10. Then, the "Initiator" sends one or more commands (e.g., ALL_REQ, SENS_REQ, and/or ATR_REQ) and receives one or more responses (e.g., SENS_RES and/or ATR_RES). EX1047 §§11.2.1.16-.17, §11.2.1.23, §11.3.2, §§12.2-.3, Figures 13, 24-25; EX1002 ¶133. Thus, regardless of what mode is used and which of Jain's devices is the Initiator or Target, the Target device detects a sufficiently strong field from the Initiator (***proximity condition has been satisfied***), and the Initiator device detects that a Target is within its field by receiving a response to a command from the Target (***proximity condition has been satisfied***). EX1002 ¶133-135. This exchange of commands and responses results in selection of a particular "Target" and attributes/parameters for further communication with the same, thereby establishing a short-range link. EX1047 §7, §§11.2.1.24-25, §12, §12.1, Figures 22, 24-25; EX1002 ¶134-135. After this link is established, the Initiator and the Target communicate using ECMA-340's data exchange protocol. EX1047 Figures 5, 23,

and 24. This includes transmission of Jain's transaction request 117, transaction response 119, and authorization response 120. EX1002 ¶¶131-136.

Confirming this limitation is met, Patent Owner alleges in its infringement contentions that the use of NFC is itself sufficient to show *detecting by the smartphone that a proximity condition is satisfied*. EX1016 at 29-42; *see* EX1002 ¶¶137.

Also, it would be obvious to a POSITA that Jain's mobile device would first detect it is proximate to the POS terminal based on a signal from the POS device (*e.g.*, a "request," Jain ¶[0023], or earlier commands and responses exchanged as part of implementing ECMA-340) prior to communicating with that POS. EX1002 ¶¶130-138. To ensure communications would be successful and not wasted, and to avoid security risk of indiscriminately transmitting sensitive financial information, Jain's smartphone first needs to detect it is near the POS device prior to proceeding with a payment transaction. EX1002 ¶138. Otherwise, the NFC communication would fail. Such implementations were well-known to a POSITA. *Id.* For example, EX1020 leverages NFC to limit the range at which communication may take place. EX1020 ¶¶[0041], [0063]. In the context of Wi-Fi, EX1020 explicitly discloses using the ability to receive such signals as an indication of proximity. EX1020 ¶[0073] ("The [identifying information] may be used by the device 10 to indicate that the device is located within communication range of the hot spot 169."). A

POSITA would be motivated and able to use Jain's "request" or ECMA-340's commands and responses in the same manner. EX1002 ¶¶130-138.

(f) 1[f]

As described for 1[e], Jain discloses that before performing a financial transaction, the smartphone must be sufficiently close to POS 114 (*in response to the proximity condition having been satisfied between the smartphone and the first entity*); EX1002 ¶139. If that condition is met, Jain's smartphone sends transaction response 119 identifying information associated with a payment account to the nearby POS 114 (*entity*) using NFC. Jain ¶¶[0023], [0027], [0029]. Jain further discloses that communication using those protocols involves first establishing a wireless connection (*wireless short-range communications link*) between the mobile device (*smartphone*) and the POS device (*entity*). Jain ¶[0018], [0051].

Moreover, as addressed in more detail *supra* for 1[a], the NFC standard implemented by Jain teaches or renders obvious conducting a command/response exchange that concludes with the "Initiator" device selecting one or more "Target" devices and attributes/parameters for communication (*establishing a wireless short-range communications link*) after the "Initiator" and "Target" first detect RF signals from each other (*in response to at least the proximity condition having been satisfied*). EX1047 §7, §§11.2.1.24-25, §12, §12.1, Figures 22, 24-25; EX1002 ¶140. Once this *link* is established Jain's POS device (*entity*) and the mobile device

(*smartphone*) communicate using the “Data exchange protocol (DEP)” to exchange data “Requests” and “Responses,” including Jain’s transaction request 117, transaction response 119, and authorization response 120. EX1047 Figures 5, 23, and 24; EX1002 ¶140.

At a minimum, it would be obvious to a POSITA that Jain’s smartphone would first establish a NFC connection with the POS device (*establishing a wireless short-range communications link between the smartphone and the entity*) after detecting *the proximity condition having been satisfied* and prior to sending the transaction response 119 to POS 114 (*entity*) using NFC. EX1002 ¶¶141-148. To ensure communications would be successful and not wasted, and to avoid security risk of indiscriminately transmitting sensitive financial information, Jain’s smartphone needs to detect proximity and then establish a short-range communications link with the POS prior to proceeding with a payment transaction. EX1002 ¶146. Use of a link after detecting proximity further improves reliability and security, because once a link is established, Jain’s mobile device can receive confirmation of receipt of individual packets. *Id.* Such implementations of devices communicating via NFC establishing a connection prior to transmitting information were well-known to a POSITA. EX1019 ¶¶[0011], [0124], [0182]; EX1002 ¶146. For example, in Lin, “to facilitate the establishment of an NFC connection (e.g., typically 2-4 cm)” (*proximity condition having been satisfied*), an “RF field

generated by the payee device... may induce... transition to an active mode of operation, thus establishing an NFC connection between the two devices.” Lin ¶[0124]. “Accordingly, by way of this established NFC connection, the payment [information] may be transmitted to and received by the payor device.” *Id.*; EX1002 ¶147.

This wireless connection between Jain’s mobile device (*smartphone*, in red below) and a nearby POS device (*first entity*, green) uses protocols such as NFC, Bluetooth, or RFID (*a first air interface*, yellow). Jain ¶[0023]; EX1002 ¶148.

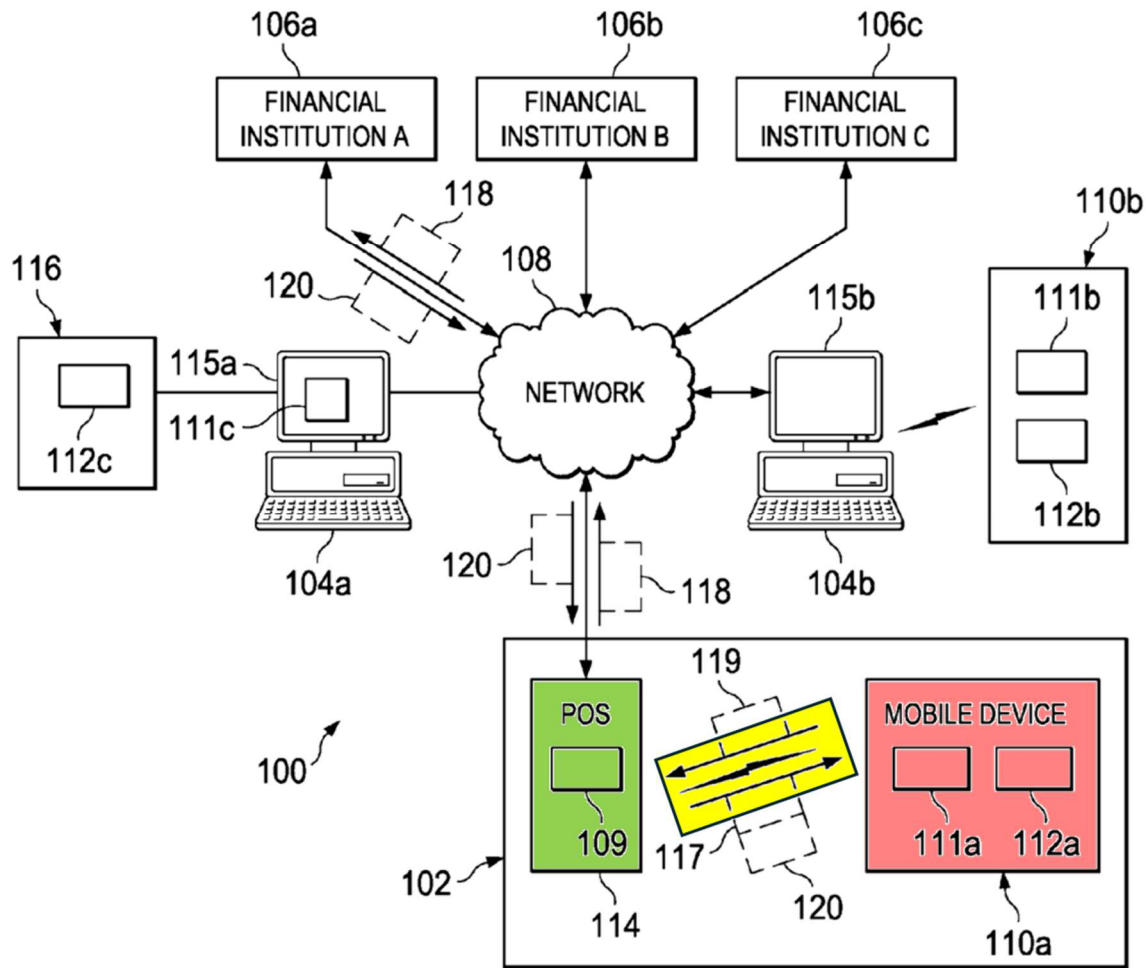


FIG. 1

Confirming this limitation is met, Patent Owner alleges in its infringement contentions that use of NFC is itself sufficient to show this limitation. EX1016 at 25-28. Thus, according to Patent Owner, the presence of NFC communication, as disclosed in Jain, demonstrates both the existence of *a wireless short-range communications link* and that this link is established *in response to the proximity condition having been satisfied between the smartphone and the first entity*. See EX1002 ¶149.

(g) 1[g]

Limitation 1[g]’s requirement of *receiving... a short-range signal from the first entity*, is addressed above in connection with 1[e] and 1[f], since Jain’s mobile device “wirelessly receive[s] a request from the POS device 114 to execute a transaction and/or... provide a response.” Jain ¶¶[0023], [0029]. This short-range signal is received wirelessly using NFC or other short-range protocols (*first air interface*). Jain ¶¶[0023], [0029]; EX1002 ¶150.

(h) 1[h]

Jain’s mobile device, in response to a request from the POS device (*responsive to receiving the short-range signal from the first entity*), generates transaction response 119 identifying information associated with a payment account, and may include an account number, a transaction amount, user credentials, and/or other information (*information*), and *send[s]* the transaction response 119 to the nearby POS 114 via NFC (*to the first entity over the first air interface*). Jain ¶¶[0023], [0027], [0029]; EX1002 ¶151. As explained above for 1[e], the activation code (*second data*) is sent as a verification to activate the financial account associated with the transaction card. Accordingly, the activation code (*second data*) received from the financial institution and used to activate the associated financial account is *associated with* the payment account information in the transaction response (*information*) because the transaction response (*information*) is based on

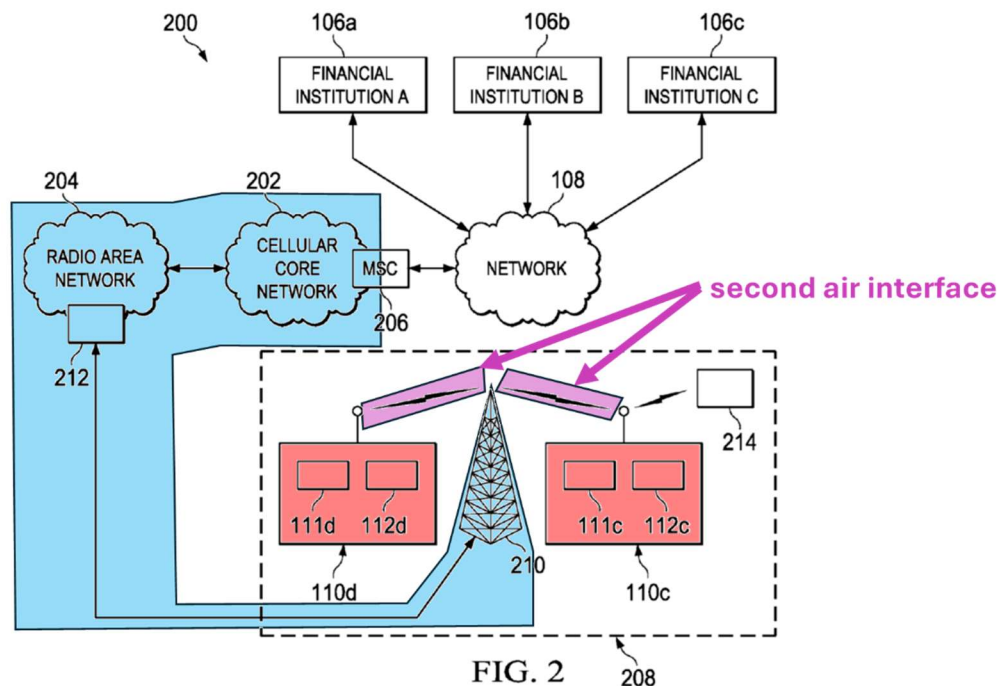
the same financial account activated and associated with the transaction card based on the activation code (*second data*). EX1002 ¶152.

A POSITA would find it obvious to receive payment account information itself from the financial institution and generate the transaction response based on that information. EX1002 ¶¶153-154. Receiving account information over a network rather than requiring that they be inputted or hard-coded in a local device was well known in the art. *Id.* For example, same as Jain, Chen teaches a mobile device that can hold account information (m-cards) and provide parts of that information (*e.g.*, an integer uniquely identifying the m-card) to a POS device via NFC. Chen ¶[0028], [0031], [0068]. Chen further teaches that this account information can be generated by the bank, not the mobile device. Chen ¶[0032]. Indeed, Jain itself discloses that the account information (also called “financial vehicle” or “FV” data) can be provisioned by “going to a third party wallet provider or directly to the [Financial Institution] website.” Jain at 13 (“Table 1,” row 3, column 4). A POSITA would be motivated to add receipt of actual account information (in lieu or in addition to the activation code) to Jain’s Figure 9 to simplify the authorization and activation process, since at that point the mobile device with transaction card is already communicating with the financial institution and receiving information (including the activation code) from the same. Further receiving Jain’s account information as part of the process would limit the number of steps a user has to take and how often

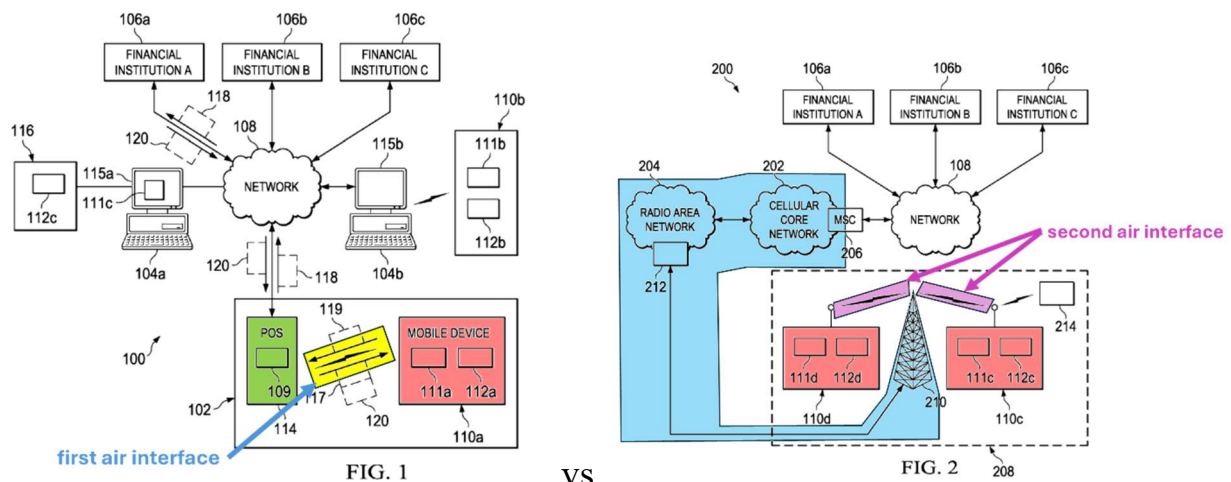
the mobile device has to initiate connections with the bank. This would be a minor and easy change to process 900—*e.g.*, adding one request and receipt at the end of the process—that would not otherwise interfere with Jain’s system. EX1002 ¶154.

(i) 1[i] and 1[j]

As described for 1[a][ii], Jain’s mobile device communicates with a financial institution using cellular radio technology. Jain ¶¶[0027], [0030], [0041]-[0048], [0065], [0072], [0081]; EX1002 ¶155. Annotated Figure 2 shows mobile device 110 (*smartphone*, in red) communicating via cellular radio technology (*the second air interface that differs from the first air interface*, in purple) to access the infrastructure providing cellular connectivity (*a communications service from a wireless network*, in blue).



This wireless network is separate from Jain's use of NFC or other proximity standards for communicating with a POS when engaging in a financial transaction, as shown in Figure 1. Jain ¶[0081]. An interface for cellular network (*second air interface*) differs from an interface for NFC or other proximity standards (*first air interface*). EX1002 ¶156; compare Jain ¶[0023] (Fig. 1) with Jain ¶[0041] (Fig. 2), as shown below:



compare FIG. 1 (NFC) (yellow) with FIG. 2 (cellular) (purple).

The mobile devices 110a, 110c, and 110d in Figs. 1 and 2 (red) are the same mobile device 110 having smartcard 112 discussed herein. Jain ¶[0017] (“Like reference symbols in the various drawings indicate like elements.”), ¶[0027] (discussing a mobile device that is in proximity-based communication with POS device 114..., and “[i]n some implementations, the financial institution 106 may transmit the authorization response 120 to the mobile device through a cellular core network (see FIG. 2)”). EX1002 ¶157.

Jain teaches that mobile device 110 can be cellular capable, which means that it receives cellular service (*communications service from a wireless network*) even during activation and before financial transactions are enabled. Jain ¶[0023]; EX1002 ¶158. Jain discloses, for example, that device 110 can make and receive voice calls over a cellular network. Jain ¶¶[0040], [0042]-[0043],[0056]. Thus, it is *independent of performing a financial transaction*. Jain ¶[0023]; EX1002 ¶158.

Further, as described for 1[a][ii], 1[b], and 1[c], the steps of *transmitting... first data and receiving... second data* are performed using cellular communications (*second air interface / an air interface that differs from the first air interface*). EX1002 ¶159.

3. Claim 2

(a) 2[pre]

Claim 1, *supra*. See EX1002 ¶160.

(b) 2[a]

According to Patent Owner, limitation 2[a] does not impose any new requirement over limitation 1[a][i]: the same sensing of *the* at least one physiological parameter as a prerequisite to *enabling* a mode to communicate is also a prerequisite to then performing a first transaction and establishing the wireless short-range communications link between the smartphone and POS device. Compare Ex1016 at 47-53 with Ex1016 at 8-13 (pointing to the same “fingerprint unlock,” “facial

recognition,” “iris authentication,” and similar security functionality and associated evidence for both limitations); *see* EX1002 ¶161.

Even if the claims require an additional transaction-specific *sensing*, Jain discloses or renders this limitation obvious. EX1002 ¶¶162-169. In Jain, performance of a financial transaction is responsive to checking the same parameter used during the user authentication portion of process 700. 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]. Jain further discloses that this “PIN request” is presented and user information is received via GUI 111 of device 110. Jain ¶[0023]-[0025]. Authorization via PIN involves or obviously involves the process of Jain ¶[0075], discussed above for 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 to be a simple and obvious way of implementing PIN authorization: it does not require communication with any other devices and allows the POSITA to reuse aspects of software that implements the user authentication of Fig. 7. EX1002 ¶163. Such processes were well known in the art, including from Jain’s Fig. 7. *Id.* Further, it would have been obvious to a POSITA that this transaction-specific *sensing* would occur before establishing the wireless short-range link for a transaction. For example, as a security setting, the

NFC-capability of Jain's device could be turned off until PIN authentication, the same way PIN authentication enables a mode to communicate in limitation 1[a]. *Id.*

Also, it would be obvious for a POSITA to replace the disclosed PIN with user biometrics to authorize the transaction. EX1002 ¶167. Jain already contemplates using biometrics (e.g., fingerprints) for its user authorization process (Jain ¶[0075], Figure 7), and reusing that software and hardware for individual transactions would not further complicate the system or incur material costs. *Id.* Jain recognizes that biometrics are a good alternative to PINs. Jain ¶[0075]. A POSITA would recognize the advantages of biometrics over PINs, including that biometrics cannot be forgotten or obtained by a bad actor via, e.g., phishing, and that use of biometrics for authorizing individual transactions would thus improve system security. *Id.* Alternatively, a POSITA would also be familiar with two-factor authentication and would know how to retain PIN authentication while augmenting it with biometric authentication, and appreciate that the cost of doing so is warranted because of the extra security it provides for financial transactions. EX1002 at ¶¶168-169. Requiring biometric authentication before authorizing individual transactions was well known in the art. EX1002 at ¶169; e.g., Rosenblatt, [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.”); Mardikar, [0052] (“Selecting ‘Payment’ may

prompt a payment application 155 on the mobile device 100 to check the biometric sensor 160 for biometric input.”). Also, for the reasons discussed above for 1[a], Jain discloses or at least renders obvious that implementing biometric authorization would entail the claimed *sensing*.

4. Claim 3

(a) 3[pre]

Claim 1, *supra*. See EX1002 ¶170.

(b) 3[a]

According to Patent Owner, limitation 3[a] does not impose any new requirement over limitation 1[a][i]: the same sensing of *the* at least one physiological parameter as a prerequisite to *enabling* a mode to communicate is also a prerequisite to sending by the smartphone to the first entity information associated with the second data. Compare Ex1016 at 54-59 with Ex1016 at 8-13; see EX1002 ¶171.

Even if the claims require an additional transaction-specific *sensing*, Jain discloses or renders this limitation obvious. See 2[a], *supra*; EX1002 ¶172.

5. Claim 4

(a) 4[pre]

Claim 1, *supra*. See EX1002 ¶173.

(b) 4[a]

According to Patent Owner, limitation 4[a] does not impose any new requirement over limitation 1[a][i]. *Compare* Ex1016 at 60-67 with Ex1016 at 8-13; *see supra* limitations 1[a][i] and 3; EX1002 ¶174.

Even if the claims require an additional transaction-specific *sensing*, Jain discloses or renders this limitation obvious. *See* 2[a], *supra*; EX1002 ¶175.

Further, Jain’s authentication process using biometrics involves determining whether the sensed biometric matches the locally-stored value (*performed responsive to a value of at least one parameter associated with the smartphone*). EX1002 ¶176. At step 738 of Figure 7B, the smartphone receives a PIN via the device’s touch screen or keypad. Jain ¶¶[0022], [0075]. At step 740, the smartphone retrieves a locally stored PIN. Jain ¶[0075]. Then, at step 742, the mobile device determines whether the user-inputted PIN matches the locally-stored PIN. Jain ¶[0075], Fig. 7B. Jain discloses that rather than “entering a PIN... the user may be authenticated using... biometric information (e.g., fingerprint).” Jain ¶[0075]. Further, Claim 4’s “parameter associated with the smartphone” is broader than, and does not necessarily need to be, the “physiological parameter” from Claim 1. Accordingly, Claim 4 is met from Jain’s authentication process determining whether the user-inputted PIN matches the locally-stored PIN. EX1002 ¶176.

6. Claim 5

(a) 5[pre]

Claim 1, *supra*. Claim 5 largely involves repeating some of the same steps of Claim 1, but using a different POS device (*second entity*) for a *second transaction*. See EX1002 ¶177.

(b) 5[a]

Jain teaches a plurality of transactions. Jain Abstract, ¶[0005], ¶[0018]. Accordingly, Jain teaches *performing a second transaction of the plurality of financial transactions*. See EX1002 ¶178.

(c) 5[b]

Jain's method can be used to execute payment transactions at any capable retail payment terminal (e.g., POS 114) that accepts contactless payment transactions (Jain ¶[0029]) including, for example, cash registers (¶[0036]), contactless-enabled terminals (¶[0029]), or mobile device (¶[0047]). Thus, a user can complete a first transaction with a first POS device (e.g., cash register at a first store) and then complete a second transaction with a second POS device (e.g., cash register at a second store). Any such second POS device (*second entity*) is *distinct from* the first POS device (*first entity*) and also distinct from the financial institution (*first device*). EX1002 ¶179.

Jain's system will repeat the same process for performing a financial transaction with the second POS device (*second entity*). Jain ¶[0023]. Thus, Jain's

system with respect to the second POS device (*second entity*) will *detect by the smartphone that a proximity condition is satisfied* the same as discussed for limitation 1[e] for the first POS device. EX1002 ¶180.

(d) 5[c]

Jain's system with respect to the second POS device (*second entity*) will *establish, using the first air interface, a wireless short-range communications link between the smartphone and the second entity, in response to the proximity condition having been satisfied between the smartphone and the second entity* the same as discussed for limitation 1[f] for the first POS device. EX1002 ¶181.

(e) 5[d]

Jain's system with respect to the second POS device (*second entity*) will *receive, using the first air interface, a short-range signal from the second entity* the same as discussed for limitation 1[g] for the first POS device. EX1002 ¶182.

(f) 5[e]

Jain's system with respect to the second POS device (*second entity*) will *send by the smartphone to the second entity over the first air interface, information associated with the second data received from the first device responsive to receiving the short-range signal from the second entity* the same as discussed for limitation 1[h] for the first POS device. EX1002 ¶183.

7. **Claim 6**

(a) 6[pre]

Claim 1, *supra*. See EX1002 ¶184.

(b) 6[a]

As explained for limitation 1[b], during Jain’s step 920, smartphone 110 “wirelessly transmits a request for the activation code using the cellular radio technology” (*data relating to a request to pay for a transaction*). Jain ¶[0081]. Because the request for and receipt of the activation code are fundamental steps for activating the transaction card and allowing the transaction card to perform payments with the associated financial account (Jain ¶¶[0071], [0080]-[0081]), they are prerequisites to payment transactions and thus *relat[e] to a request to pay*. EX1002 ¶185.

Confirming this limitation is met, Patent Owner alleges in its infringement contentions that adding and verifying payment cards on a mobile phone digital wallet is itself sufficient to show this limitation. EX1016 at 77-81; *see* EX1002 ¶186.

(c) 6[b]

As explained for limitation 1[c], in response to the request of step 924, mobile device 110 receives an activation code from the financial institution, which is checked against a stored activation code, and if they match, the transaction card is activated (*data relating to an acknowledgement and/or authorization of enabling*

a mode/function to pay for a transaction). Jain ¶¶[0081], [0026], [0071]; EX1002 ¶187.

8. Claim 7

(a) 7[pre]

Claim 1, *supra*. See EX1002 ¶188.

(b) 7[a]

Jain's system expressly includes multiple financial institutions. See EX1002 ¶189. Jain teaches that POS 114 can wirelessly receive encrypted transaction information from the transaction card 112 and electronically send the information to one or more of the financial institutions 106. Jain ¶[0036]. Figure 1 illustrates the multiple financial institutions. Any one of the financial institutions that is not the first device can be *the second device distinct from the first device and further distinct from the first entity* (the POS device 114):

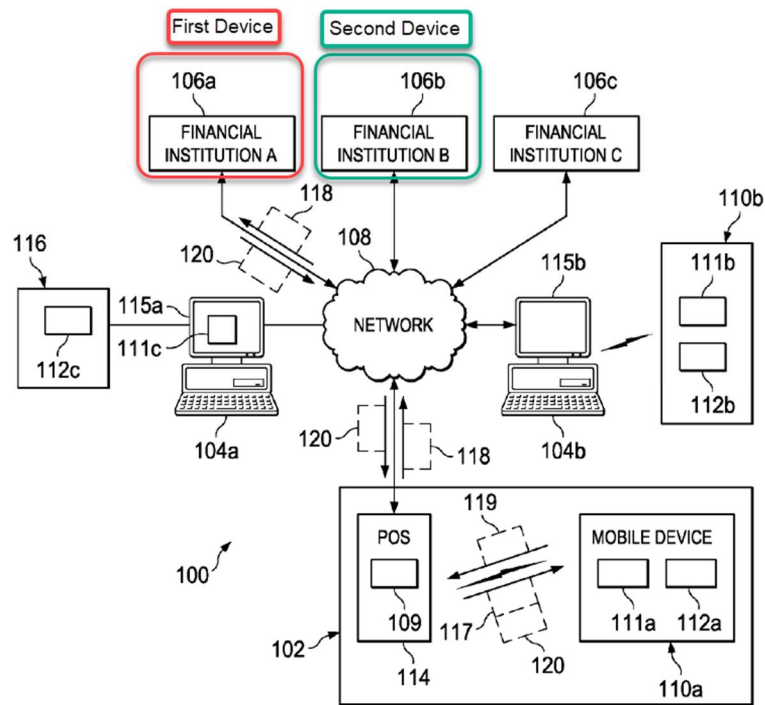


FIG. 1

Jain's system with respect to the second financial institution (*second device*) will *transmit by the smartphone third data to a second device* the same as discussed for limitation 1[b] for the first device. EX1002 ¶190.

(c) 7[b]

Jain's system with respect to the second financial institution (*second device*) will *receive by the smartphone fourth data from the second device relating to an acknowledgement and/or authorization of enabling a mode/function to pay for a financial transaction* the same as discussed for limitation 6[b] for the first device.

EX1002 ¶191.

(d) 7[c]

Jain's system with respect to the second financial institution (*second device*) will *transmit by the smartphone third data to a second device and receive by the smartphone fourth data from the second device over the air interface that differs from the first air interface*, the same discussed for limitation 1[j] for the first device. EX1002 ¶192.

9. Claim 8

(a) 8[pre]

Claim 1, *supra*. See EX1002 ¶193.

(b) 8[a]

Jain discloses *causing data to be transmitted selectively to a plurality of predetermined devices*. EX1002 ¶194. Jain's mobile device may transmit transaction history data in response to a request from the financial institutions to the mobile host device for transaction history. Jain ¶[0046]. This sending is *selective* because it occurs in response to the request from the financial institution. The financial institution requests this information using the cellular core network (together, *a plurality of predetermined devices*). Jain ¶[0046].

Jain further discloses *causing data to be received selectively from said plurality of predetermined devices* by explaining that the mobile device receives from the financial institution, either directly using the cellular core network or via POS device 114, a transaction receipt. Jain ¶[0041], [0046]; EX1002 ¶195. This

information is transmitted after payment is complete (*responsive to performing a financial transaction*). Jain ¶[0046] (“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.”).

In its infringement contentions, Patent Owner maps the plurality of predetermined devices to base stations. EX1016 at 95-96. Applying this theory, Jain’s system also causes data to be transmitted selectively to and selectively received from a plurality of predetermined devices (network 108, GSM core network 202, RAN 204, Base Station Controllers... 212, and/or Base Stations... 210). Jain ¶[0044], Fig. 2; EX1002 ¶196.

10. Claim 9

(a) 9[pre]

Claim 1, *supra*. See EX1002 ¶197.

(b) 9[a]

Limitation 9[a] lists specific protocols to be used for the *second air interface*. In Jain, the second air interface is implemented using cellular radio technology. Jain ¶[0081]. The specific cellular technology in Jain includes GSM, CDMA, UMTS, and other modes. Jain ¶[0041]. A POSITA would be motivated to use the most advanced and performant cellular technologies such as LTE and WiMAX (4G cellular technologies), well-known next-generation cellular technologies, in addition to the cellular technology mentioned in Jain to keep up with ever-evolving

technologies that allow for higher data rates and that, as of the priority date of the '432 patent, were known to POSITAs to be in line to displace older technologies in the near future. EX1002 ¶¶198-199; *see* EX1045, EX1046. WiMAX and LTE both use *Orthogonal Frequency Division Multiplexing* and *Orthogonal Frequency Division Multiple Access* air interface protocol. *Id.*

Jain also discloses “mobile device 110 [can] transmit packet data using its own connection to the external world (e.g., SMS, cellular, Wi-Fi).” Jain ¶[0053]; *see* Jain claim 13, 14. This includes using “WiFi technology” to “wirelessly interface” with financial institutions. Jain ¶[0068], Fig. 5. Accordingly, Jain discloses Wi-Fi as an alternative to “cellular” communications for implementing the *transmitting/receiving* to/from a financial institution, as taught in Jain’s Fig. 9. OFDM is the digital modulation scheme employed by Wi-Fi. EX1002 ¶200. Accordingly, the *second air interface* (Wi-Fi) *comprises an Orthogonal Frequency Division Multiplexed and/or an Orthogonal Frequency Division Multiple Access (OFDM/OFDMA) technology*. *Id.*

11. Claim 10

Claim 10 is substantively identical to claim 1, except:

(1) 10[b] further requires that transmitting first data to a first device is a *precursor to performing the plurality of financial transactions*. As explained for

limitation 1[b], the transmission of request for activation code (*first data*) occurs before performing the plurality of financial transactions.

(2) 10[c] does not require that *the second data relate to the plurality of financial transactions to be conducted and differing from the first data*” which is a requirement in 1[c].

(3) The information of 10[h] is *based on the second data received from the first device*, while the information of 1[h] is *associated with the second data*. But because the payment account information in the transaction response (*information*) is also *based on* activation of the financial account and the activation code received from the financial institution used to activate the associated financial account on the smartphone (*second data received from the first device*), 10[h] is also met as explained for limitation 1[h]. EX1002 ¶201.

Confirming this limitation is met, in its infringement contentions, Patent Owner’s support for each limitation of claim 1 is identical to the corresponding limitation in Claim 10. *Compare* EX1016 at 1-46 to EX1016 at 100-145; *see* EX1002 ¶¶202.

12. Claims 11-17

Claims 11-17 are substantively identical to claims 2-8, except claims 12 and 13 include the *based on* language as explained for 10[h]. EX1002 ¶203.

B. Ground 2: Dua (EX1018)

1. Background

Dua is prior art under at least pre-AIA 35 U.S.C. §102(b), having been published over a year before the earliest effective filing date of the '432 patent. Dua discloses all limitations of the '432 patent claims. Petitioner presents Dua as an obviousness reference in the event Patent Owner argues differences between Dua's disclosure and the '432 patent claims.

Dua was considered by the PTO Examiner during the prosecution of the patent application that issued as the '432 patent. The Examiner noted that the application was only allowed over Dua because the Examiner found Dua did not teach “enabling a mode to communicate... responsive to at least one physiological parameter.” EX1009 at 275-277. Applicant argued, and Examiner agreed, that Dua's paragraphs [0026], [0089], and [0495] do not teach or suggest this limitation. EX1009 at 253. As discussed below, the Examiner overlooked Dua's teachings for that limitation, or at least did not have the benefit of Petitioner's expert analysis on the disclosure and obviousness of this limitation. In portions of Dua outside those three cited paragraphs, Dua *does* disclose “biometric technologies” including using a “fingerprint in lieu of a PIN code to authenticate a user to the wallet application.” Dua ¶[0366]. Petitioner raises new arguments and expert analysis concerning the disclosures of Dua and its relationship to the challenged claims. For example,

Petitioner and its expert explain Dua’s disclosures of “biometric technologies,” which were seemingly overlooked. *See* EX1002 ¶¶39-45.

Below is a short, non-limiting overview of Ground 2:

As described in more detail in Section VIII.A.1 above, claim 1 requires first enabling a mode to communicate information requesting an authorization, and transmitting and receiving data relating to financial transactions.

Dua discloses this first step under two theories, the **Card-Issuing Theory** and the **External-Storage-Authentication Theory**. EX1002 ¶¶204-211. Under the **Card-Issuing Theory**, Dua discloses (1) performing PIN or biometric authentication to open a wallet application; (2) once opened, establishing a SIP communication session with a credit card issuer’s wireless credential manager (“WCM”); and (3) using the SIP communication session to receive credentials from the WCM. Under the **External-Storage-Authentication Theory**, Dua discloses (1) performing PIN or biometric authentication to open a wallet application or receiving a reader key; (2) establishing a SIP communication session with external storage; and (3) using the SIP communication session to retrieve credentials from the external storage.

After receiving/retrieving credentials under either theory, Dua then discloses the second step of performing the financial transaction by (1) requiring the user to authenticate via PIN or biometrics or requiring receipt of a reader key; (2) requiring

that the user device is sufficiently close to a point-of-sale terminal to engage in a transaction; and (3) transmitting the received/retrieved credentials to the point-of-sale terminal to perform the transaction.

2. Claim 1

(a) 1[pre]

Dua discloses a wireless device, which includes a *smartphone*. Dua Abstract, FIGS. 3, 5, 6(a)-8; EX1002 ¶212. 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” (*perform[] a plurality of financial transactions*). Dua Abstract, ¶¶[0041], [0312]-[0313], [0333].

(b) 1[a][i] and 1[a][ii]

The claim begins with two prerequisites: *sensing at least one physiological parameter* and *enabling a mode to communicate*. Dua discloses both prerequisites under both the **Card-Issuing Theory** and **External-Storage-Authentication Theory**. EX1002 ¶213.

Card-Issuing Theory: In Dua, the wallet application must be opened for the wallet application to be issued a credit card. Dua ¶¶[0128]-[0129], [0178], [0180], [0250]. Opening the wallet requires a PIN code or alternatively, fingerprints (*physiological parameter*) scanned by the “wireless device’s embedded biometric

technologies” (*sensing... by at least one sensor of the smartphone*). Dua ¶¶[0366], [0414]; EX1002 ¶214.

The “default security setting in the wallet application is that PIN-entry is required before the wallet application can be ‘opened’” or to “access... the application” to be issued a credit card. Dua ¶¶[0366], [0429]. This understanding is confirmed by additional disclosure in Dua. *See* EX1002 ¶215-218. **First**, using the wallet application requires authentication because “[d]ata in the wallet application is encrypted and protected with a special wallet PIN code.” Dua ¶[0429]. **Second**, Dua requires user authentication for making significant changes in the wallet application, such as “access[ing] stored credentials and chang[ing] any application settings or preferences.” Dua ¶[0366]. Adding a new credit card is such a change. **Third**, a wallet application can hold many credit cards and other confidential information. Dua ¶¶[0041], [0055], [0287]-[0288], [0334]. Regardless of how the wallet is opened, including for purposes of issuing an additional credit card, the wallet application allows the user to navigate and view the stored credentials and thus needs to be protected. Dua ¶¶[0324]-[0332], [0334], [0366], [0378]; EX1002 ¶¶215-218.

Further, a feature within a wallet/payment application to add an account or credit cards is well known to a POSITA. EX1002 ¶218; EX1019 ¶¶[0136]-[0140], Figs. 5A-B; EX1021 ¶[0047]; EX1039 ¶[0117]. A POSITA would be motivated to

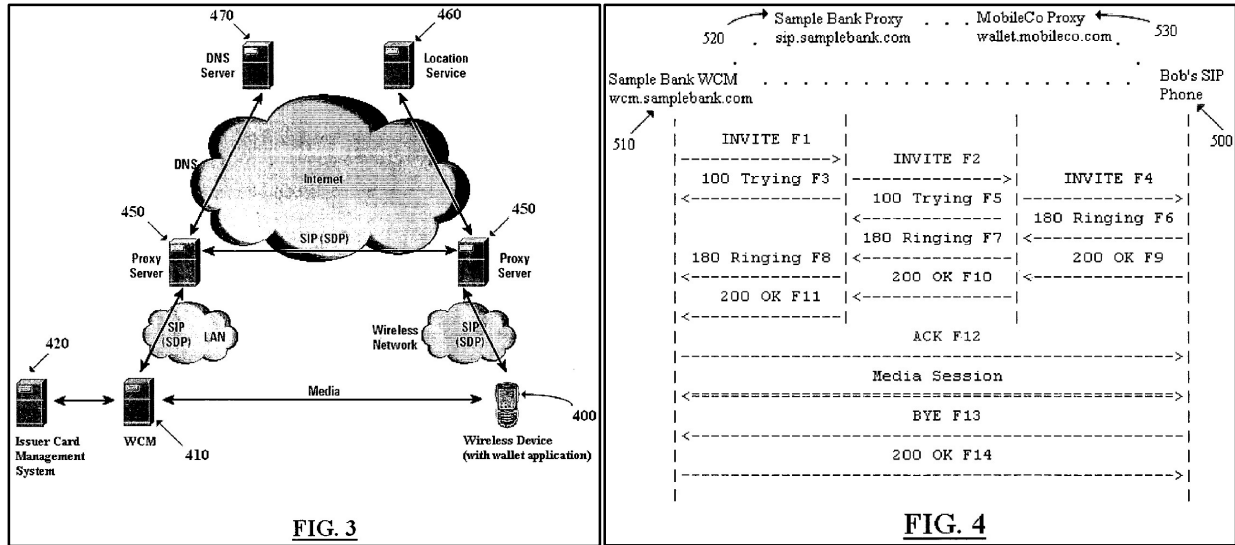
incorporate that feature in the wallet application because it improves utility regarding credit card management. EX1002 ¶219.

At a minimum, requiring PIN entry under these circumstances is obvious. EX1002 ¶¶216-221. To ensure security of other credentials, alongside allowing use of an encrypted wallet application and changes to the wallet application by an authenticated user, a POSITA would retain Dua’s “default” user authentication—PIN-entry—for credit card issuance. Dua ¶[0366]. It was well known to require such verification before permitting access to sensitive functionality. EX1019 ¶[0107], Fig. 10A, 10B; EX1002 ¶¶216-221.

Dua further teaches that PIN codes can be replaced with fingerprints (*physiological parameter*) scanned by the “wireless device’s embedded biometric technologies,” which involves biometric sensors (*sensing... by at least one sensor of the smartphone*). Dua ¶¶[0366], [0414]. Dua contemplates other biometric data, including “iris, voiceprints, facial recognition, and hand geometry.” Dua ¶[0534]. A POSITA would understand that using biometric data, like a “fingerprint[,] in lieu of a PIN code to authenticate a user to the wallet application,” involves determining if the scanned biometric data matches the biometric data stored on the wireless device or, as disclosed by Dua, determining if the scanned biometric data can decrypt the wallet application’s data. Dua ¶¶[0050], [0366], [0399], [0429]; EX1002 ¶222.

Confirming this limitation is met, Patent Owner alleges in its infringement contentions that use of biometric verification is itself sufficient to show *at least one physiological parameter having been sensed by at least one sensor of the smartphone*. EX1016 at 29-42; *see* EX1002 ¶223.

At a minimum, it would be obvious to implement Dua's teaching of "authentication using... biometric information" in this manner for the reasons explained above in connection with Jain's disclosure of limitation 1[a][i]. EX1002 ¶¶224-225. After matching PIN code or fingerprint is sensed, the wallet application is opened in order to be issued a credit card. The wallet application then establishes Session Initiation Protocol ("SIP") communication session between the wireless device and the issuer's wireless credential manager ("WCM") (*enabling a mode to communicate*). 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 SIP-enabled mobile device 500." Dua ¶¶[0128], [0178], Figs. 3 and 4:



Through the SIP session (*enabl[ed] mode to communicate information*), 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]. As explained below in more detail in connection with limitations 1[b] and 1[c], this process entails “*requesting an authorization*” to perform financial transactions. EX1002 ¶226.

External-Storage-Authentication Theory: A wallet application can store its 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 (*responsive to*) sensing a PIN code or fingerprint (*physiological parameter*) as part of opening the wallet. Dua ¶¶[0353]-[0354], [0366], [0429]; EX1002 ¶227.

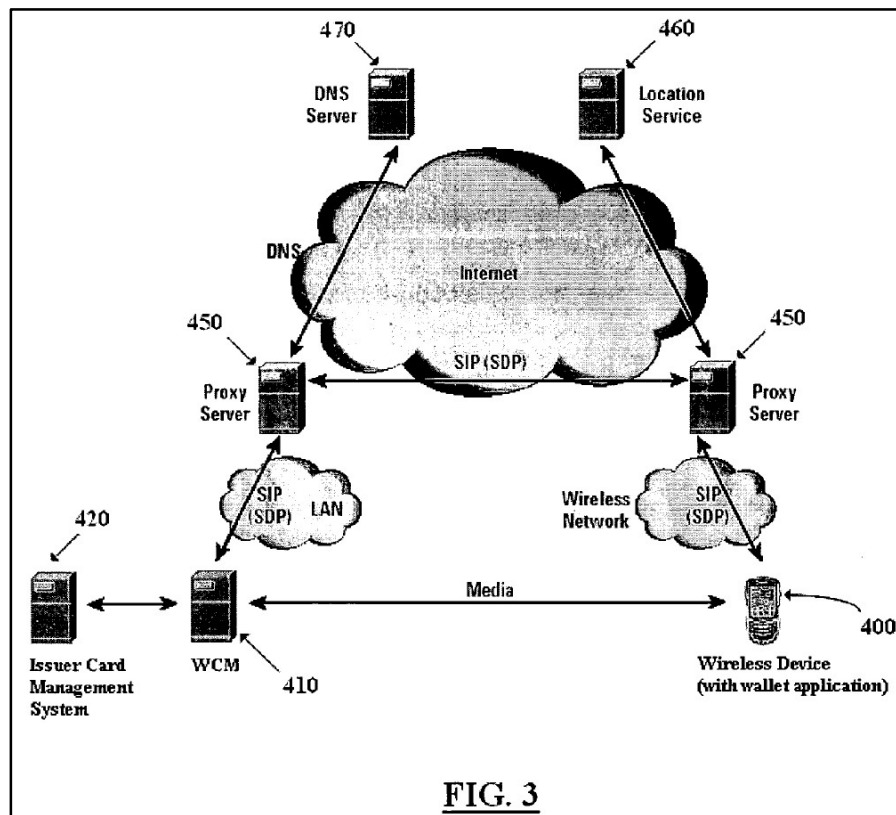
As addressed above in connection with the **Card Issuing Theory**, Dua's requirement that the user enter a PIN code or provide a fingerprint to open Dua's wallet discloses or at least renders obvious the claimed *sensing*. EX1002 ¶¶228-229. Retrieving the credential from external storage requires setting up a communications session between the wallet application and external storage. A "real-time connection is initiated between the wallet application and the storage service" by "utiliz[ing] SIP" (*enabling a mode to communicate*). 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], [0495]. As explained in connection with limitations 1[b] and 1[c], this process entails "*requesting an authorization*" to perform financial transactions.

(c) 1[b] and 1[c]

Claim 1 then recites the steps of transmitting first data and receiving second data relating to the financial transactions. Dua discloses these steps under both the **Card-Issuing Theory** and **External-Storage-Authentication Theory**. EX1002 ¶230.

Card-Issuing Theory: As discussed with limitation 1[a], the *mode to communicate* between the wireless device and WCM for user authentication that is *enabled* is SIP communications. Dua ¶¶[0046], [0104], [0128], [0178]; EX1002 ¶231. *While 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]. The wireless device’s wallet application then sends the “special code or PIN” (*first data*) to the WCM (*first device*) to allow “the issuer’s system [to] validat[e] the user’s identity in real-time.” Dua ¶[0180], FIG.3 (depicting WCM 410 as a server communicating with the wireless device 400):



“Subsequent to... validating the user’s identity[,]... the WCM 510 will transmit the credential to the wallet application” (*receiving... second data*). Dua ¶[0180]; EX1002 ¶232. The user holding the credential may then use the handheld device to conduct the authorized transaction or set of transactions. Dua Abstract, ¶[0026]. Because the exchange results in issuance of a credit card that can be used for a set of financial transactions, the transmission of the PIN code (*first data*) and the credentials (*second data differing from the first data*) *relate to a plurality of financial transactions to be conducted*. Further, with respect to limitation 1[a]’s requirement of *requesting an authorization*: because the exchange results in the issuance of a credit card, the transmission of the PIN code (*first data*) *request[s] an authorization* to perform financial transactions, and the credentials (*second data*) are an authorization to perform financial transactions (*authorization*), and enable the wireless device to execute those transactions. EX1002 ¶¶230-232.

External-Storage-Authentication Theory: As discussed with limitations 1[a][i] and 1[a][ii], the *mode to communicate* for authenticating the wireless device to the external wallet storage service and requesting/retrieving credentials is *enabled* by SIP communications. Dua ¶[0492], [0494]-[0495]; EX1002 ¶233. *While the mode is enabled*, the wireless device authenticates itself to the external storage by transmitting a “username/password for the wallet application” (*transmitting by the smartphone first data*) “to automatically access the storage area” (*first device*). Dua

¶[0492], ¶[0495]. Access to the storage area allows for requests to retrieve credentials. Dua ¶¶[0491]-[0492], [0495]. The wireless device then receives “credential information” (*second data*) that is “temporarily made available for use by the wireless device[.]” Dua ¶[0495]. The user holding the credential may then use the handheld device to conduct the authorized transaction or set of transactions. Dua Abstract, ¶[0026]. Because the exchange results in the receipt of credential information, the transmission of the username/password (*first data*), and the credentials (*second data differing from the first data*) *relate to a plurality of financial transactions to be conducted*. Further, with respect to limitation 1[a]’s requirement of *requesting an authorization*: because the exchange results in the receipt of credential information, the transmission of the username/password (*first data*) *request[s] an authorization to perform financial transactions*, and the credentials (*second data*) are an authorization to perform financial transactions (*authorization*). EX1002 ¶233.

Confirming this limitation is met by both theories, Patent Owner alleges in its infringement contentions that similar requesting and receiving issuance of a credit card meets the *transmitting* and *receiving* limitations. EX1016 at 23-28; *see* EX1002 ¶234.

(d) 1[d] and 1[e]

After receiving/retrieving credentials under either the **Card-Issuing Theory** or **External-Storage-Authentication Theory**, Dua discloses that the wireless device makes proximity transactions with point-of-sale readers (*performing a first transaction of the plurality of financial transactions*). EX1002 ¶235. “Credentials... may [be] use[d] [by] the handheld device to conduct... transactions... via... a short-range wireless link with a point-of-sale terminal.” Dua Abstract.

Because the short-range wireless link between the wireless device and point-of-sale reader includes NFC, the transaction occurs only if the wireless device (*smartphone*) is in “close proximity” to the point-of-sale reader (*first entity distinct from the first device*) and can thus detect its NFC communications (*detecting by the smartphone that a proximity condition is satisfied*). Dua Abstract, ¶¶[0016], [0318]. NFC and other short-range wireless communication protocols are only effective if there is an underlying signal of sufficient strength such that the device and the terminal can communicate using that protocol. EX1002 ¶236. Signal strength attenuates with increasing distance. *Id.* Thus, communicating with the POS terminal using NFC means the wireless device has *detected that a proximity condition is satisfied* (e.g., Dua Abstract, ¶¶[0041], [0314]-[0315], [0382], [0395]) by receiving and decoding a short-range NFC signal from the POS device.

Also, the claimed ***detecting*** occurs earlier in Dua's NFC exchange, prior to sending payment information. Dua teaches that its short-range communications protocol may be NFC. Dua ¶[0016]. Dua, like Jain, was filed after publication of the 2nd edition of the ECMA standard and before release of the 3rd edition. A POSITA would thus understand that Dua's references to NFC refer to implementing the ECMA 340 standard, 2nd edition. EX1002 ¶[237-240]. Moreover, as explained above in connection with Jain, regardless of what NFC mode is being used and which device in Dua is the Initiator and which device is the Target, both devices detect whether ***a proximity condition*** has been satisfy, establish a link, and then use that link to exchange data. This includes transmission of Dua's credential data. *Id.* At a minimum, it would have been obvious to implement Dua's NFC communications this way. *Id.* Dua tells a POSITA to look to "ISO/IEC 14443" RF proximity standard (Dua ¶[0013]), which would motivate a POSITA to also look to the standard for NFC, in addition to the benefits for implementing a standard discussed above in connection with Jain. EX1002 ¶[237-240].

Confirming this limitation is met, Patent Owner alleges in its infringement contentions that use of NFC is itself sufficient to show ***detecting by the smartphone that a proximity condition is satisfied***. EX1016 at 29-42; *see* EX1002 ¶[241].

It would be obvious to a POSITA that Dua's wireless device would first detect it is proximate to the POS terminal based on a signal from the POS terminal (*e.g.*,

“reader key,” Dua ¶[0318], or earlier commands and responses exchanged as part of implementing ECMA-340) prior to communicating with that POS. Dua’s wireless device has to establish a peer-to-peer communication session with the POS terminal over NFC. *E.g.*, Dua ¶[0016], Claims 33, 36, 50; EX1002 ¶¶242. Dua contemplates NFC communication sessions transferring a significant amount of data, such as encryption keys and several credentials, “requir[ing] the user to hold the wireless device in front of the reader for a longer period of time while the processing... takes place.” Dua ¶[0359]. As explained by Dua, the smartphone and POS communicate using short-range signals, such as near-field communication (NFC) or proximity signals. Dua Abstract, ¶¶[0016], [0041], [0314]-[0315], [0382], [0395]. Short-range signal communications are dependent on proximity between the two devices communicating. EX1002 ¶242. To ensure communications will be successful and not wasted, and to avoid security risk of indiscriminately transmitting sensitive financial information, Dua’s wireless device first needs to detect it is near the POS prior to proceeding with a payment transaction. *Id.* Otherwise, the NFC communication would fail. Indeed, such implementations were well-known to a POSITA. For example, EX1020 leverages NFC to limit the range at which communication may take place. EX1020 ¶[0041], [0063]. In the context of other wireless signals, specifically Wi-Fi, EX1020 explicitly discloses using the ability to receive such signals as an indication of proximity. EX1020 ¶[0073] (“The

[identifying information] may be used by the device 10 to indicate that the device is located within communication range of the hot spot 169.”). A POSITA would be motivated and able to use ECMA-340’s commands and responses in the same manner. EX1002 ¶242.

(e) 1[f]

As described for 1[e], Dua discloses that the wireless device makes proximity transactions with point-of-sale readers via short-range NFC after detecting that a proximity condition is satisfied. Dua Abstract, ¶¶[0016], [0318]; EX1002 ¶¶243-244. This limitation further requires that *in response* to that condition, *establishing a wireless short-range communications link between the smartphone and the entity*.

Dua further discloses that “[i]n personal environment transactions, credential data is transmitted from the wireless device to a merchant/organization using the short-range communication protocols.” Dua ¶[0320]. The wallet application supports “peer-to-peer connectivity... between the wireless device and the reader/POS terminal” (*entity*) using the short-range communication RF protocols” (*first air interface*). Dua ¶[0318]. Then, the POS device (*entity*) will “establish secure connectivity with the user’s wireless device” (*establishing a wireless short-range communications link between the smartphone and the entity*) and poll it for a list of payment methods. Dua ¶[0317]. Dua explains “one advantage of establishing

peer-to-peer connectivity with a POS terminal is that it allows for a bi-directional exchange of data.” Dua ¶[0319].

As addressed *supra* for 1[e], the NFC standard implemented by Dua teaches or renders obvious conducting a command/response exchange that concludes with the “Initiator” device selecting one or more “Target” devices and attributes/parameters for communication (*establishing a wireless short-range communications link*) after the “Initiator” and “Target” first detect RF signals from each other (*in response to at least the proximity condition having been satisfied*). EX1047 §7, §§11.2.1.24-25, §12, §12.1, Figures 22, 24-25; EX1002 ¶245. Once this *link* is established Dua’s POS terminal (*entity*) and the wireless device (*smartphone*) communicate using the “Data exchange protocol (DEP)” to exchange data “Requests” and “Responses,” including Dua’s bi-directional exchange of data like credentials and payment information. EX1047 Figures 5, 23, and 24; EX1002 ¶245.

It would be obvious to a POSITA that Dua’s smartphone would first establish a NFC connection with the POS device (*establishing a wireless short-range communications link between the smartphone and the entity*) after detecting *the proximity condition having been satisfied* and prior to sending credentials to the POS terminal (*entity*) using NFC. EX1002 ¶¶246-249. To ensure communications would be successful and not wasted, and to avoid the security risk of indiscriminately transmitting sensitive financial information, Dua’s smartphone needs to detect

proximity and then establish a short-range communications link with the POS prior to proceeding with a payment transaction with the POS device. *Id.* Use of a link after detecting proximity further improves reliability and security, because once a link is established, Dua's mobile device can receive confirmation of receipt of individual packets. *Id.* Dua recognizes in the context of short-range communications the benefit of "establishing peer-to-peer connectivity" prior to communicating information. Dua ¶¶[0317]-[0319]. Such implementations of devices communicating via NFC establishing a connection prior to transmitting information were well-known to a POSITA. EX1019 ¶¶[0011], [0124], [0182]; EX1002 ¶¶246-249. For example, in Lin, "to facilitate the establishment of an NFC connection (e.g., typically 2-4 cm)" (*proximity condition having been satisfied*), an "RF field generated by the payee device... may induce... transition to an active mode of operation, thus establishing an NFC connection between the two devices." Lin ¶[0124]. "Accordingly, by way of this established NFC connection, the payment [information] may be transmitted to and received by the payor device." Lin ¶[0124].

Confirming this limitation is met, Patent Owner alleges in its infringement contentions that use of NFC is itself sufficient to show *establishing, using a first air interface, a wireless short-range communications link between the smartphone and the first entity*. EX1016 at 28-32; *see* EX1002 ¶250.

(f) 1[g]

Limitation 1[g]’s requirement of *receiving... a short-range signal from the first entity* is addressed above for 1[e] and 1[f]. Dua explains that its system uses a credential-specific “reader key” that is programmed in all reader devices employed by an organization. Dua ¶[0353]. The reader key is transmitted from the reader to the wireless device during a proximity transaction, and receipt of the key initiates the automatic launch of the wallet application on the device and used to locate specific credentials for the transaction. Dua ¶[0353]. Accordingly, the wireless device *receive[s]* a reader key (*short-range signal*) transmitted from the reader (*first entity*) using the proximity protocol (*first air interface*). Dua ¶[0353]; EX1002 ¶251.

(g) 1[h]

Dua discloses that, after the reader key is received by the wireless device, it is transferred to the wallet application. Dua ¶[0353]. The reader key is then used as a search string to locate the appropriate credential that is transmitted back to the reader via the proximity protocol to perform the financial transaction. Dua ¶[0353]. Accordingly, the wireless device sends via NFC or other short-range wireless protocol (*over the first air interface*) credentials (*the second data* which is itself *information associated with the second data received from the first device*) to the point-of-sale terminal (*to the first entity*) to execute the financial transaction. Dua

Abstract; EX1002 ¶252. The executed transaction results in paying for a product, such as groceries or train tickets. Dua ¶¶[0352]-[0353]. This transmission of credentials is sent *responsive to receiving* the reader key from the POS reader in 1[f] (*short-range signal from the first entity*) because the receipt of the keys are required for establishing connectivity and for locating the credentials for the transaction. Dua ¶¶[0318], [0353]; EX1002 ¶252.

(h) 1[i] and 1[j]

Dua teaches that its wireless device is capable of wirelessly connecting to the Internet using network protocols, including GSM/GPRS, CDMA2000, W-CDMA, EDGE,... UMTS,... 802.11a, 802.11b, 802.11g (*receiving by the smartphone a communications service from a wireless network, using a second air interface*). Dua ¶[0041]; EX1002 ¶253. The wireless device will also have an SIP API framework embedded in or running on top of the operating system (*second air interface that differs from the first air interface*), which allows for multiple SIP-based applications, not just the wallet application (*independent of performing said first transaction*). EX1002 ¶253.

As discussed with limitations 1[a][b][c], for both **Card-Issuing Theory** and **External Device Theory**, the *transmitting* and *receiving* communications between the wireless device and either the WCM or the external wallet storage are *performed over* SIP communication via the cellular network (*second air interface*, annotated

below). Dua ¶¶[0046], [0104], [0128], [0178], [0492], [0494]-[0495]. In contrast, the financial transaction is performed using an NFC or other short-range wireless protocol (*first air interface*, annotated below). Dua Abstract, ¶¶[0016], [0318], Figure 8; EX1002 ¶254.

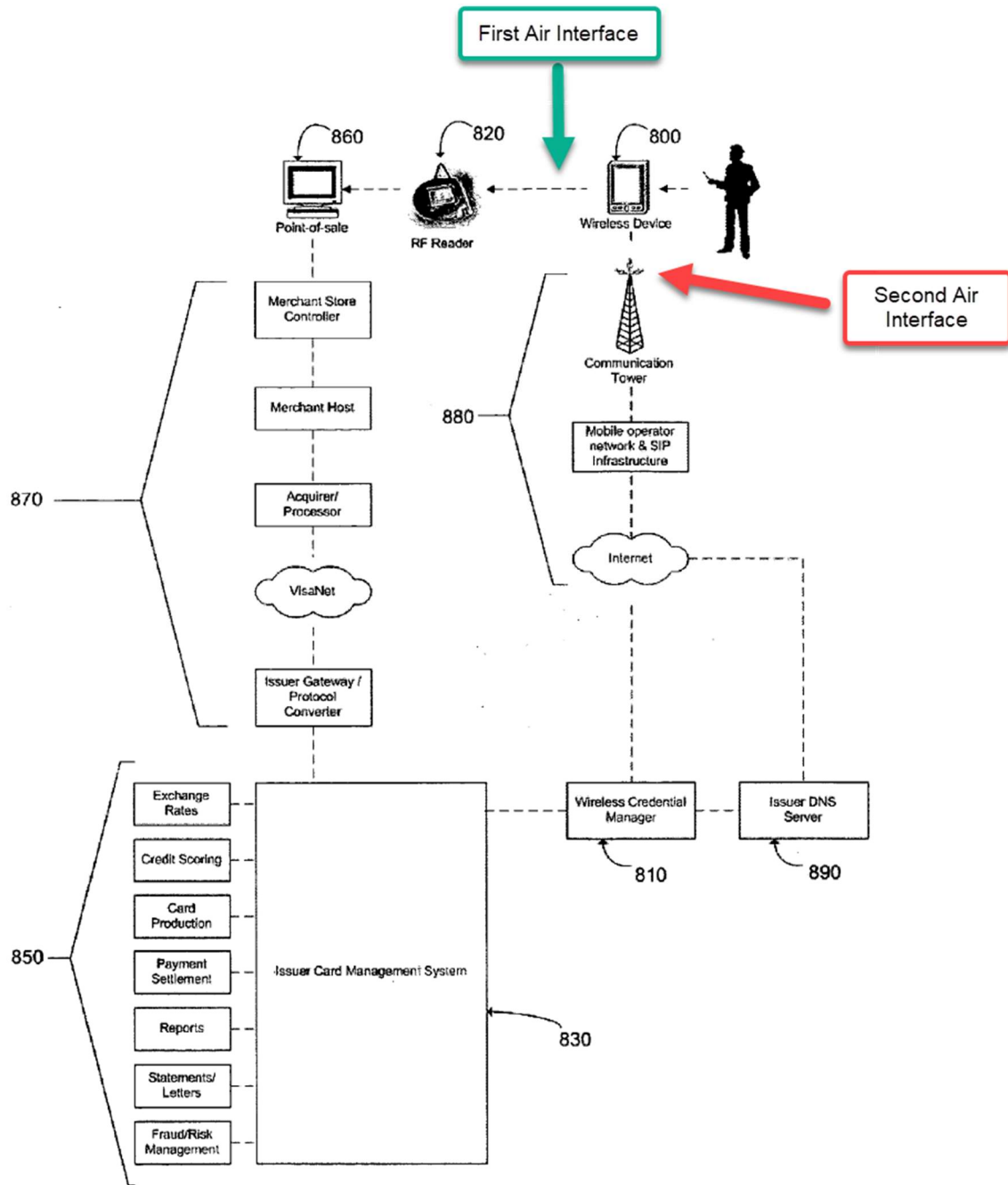


FIG. 8

3. Claim 2

(a) 2[pre]

Claim 1, *supra*. See EX1002 ¶255.

(b) 2[a]

According to Patent Owner, limitation 2[a] does not impose any new requirement over limitation 1[a][i]: the same sensing of the physiological parameter as a prerequisite to enabling a mode of communication is also a prerequisite to then performing the financial transaction. *Compare* Ex1016 at 8-14 *with* Ex1016 at 29-42; *see* EX1002 ¶256.

Even if the claims require an additional transaction-specific *sensing*, Dua discloses this limitation. EX1002 ¶257. Dua discloses that individual transactions, same as receiving or retrieving credentials, require opening the wallet application, which in turn is subject to 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]. Dua’s “default security setting” discloses or renders obvious the claimed *sensing* via PIN entry or fingerprint scanning for the reasons discussed above for limitation 1[a][i]. EX1002 ¶257.

4. Claim 3

(a) 3[pre]

Claim 1, *supra*. *See* EX1002 ¶258.

(b) 3[a]

According to Patent Owner, limitation 3[a] does not impose any new requirement over limitation 1[a][i]: the same sensing of *the* at least one physiological

parameter as a prerequisite to ***enabling*** a mode to communicate is also a prerequisite to sending by the smartphone to the first entity information associated with the second data. *Compare* Ex1016 at 54-59 *with* Ex1016 at 8-13; *see* EX1002 ¶259.

Even if the claims require an additional transaction-specific ***sensing***, Dua discloses or renders this limitation obvious. *See* 2[a], *supra*; EX1002 ¶260.

5. Claim 4

(a) 4[pre]

Claim 1, *supra*. *See* EX1002 ¶261.

(b) 4[a]

According to Patent Owner, limitation 4[a] does not impose any new requirement over limitation 1[a][i]. *Compare* Ex1016 at 60-67 *with* Ex1016 at 8-13; *see* 1[a][ii], 3[a], *supra*; *see* EX1002 ¶263.

Even if the claims require an additional transaction-specific ***sensing***, Dua discloses or renders this limitation obvious. *See* 2[a], *supra*; EX1002 ¶263. Further, Dua’s card-issuing and external-storage authentication processes using biometrics involves determining whether the sensed biometric matches the locally-stored value (***performed responsive to a value of at least one parameter associated with the smartphone***). Dua teaches that its card-issuing and external-storage authentication processes may use fingerprints scanned by the “wireless device’s embedded biometric technologies.” Dua ¶¶[0366], [0414]. Dua also contemplates other biometric data, including “iris, voiceprints, facial recognition, and hand geometry.”

Dua ¶[0534]. A POSITA would understand that using biometric data, like a “fingerprint[,] in lieu of a PIN code to authenticate a user to the wallet application,” involves determining if the scanned biometric data matches the biometric data stored on the wireless device or, as disclosed by Dua, determining if the scanned biometric data can decrypt the wallet application’s data” (*responsive to a value*). Dua ¶¶[0050], [0366], [0399], [0429]; EX1002 ¶263.

Further, Claim 4’s “parameter associated with the smartphone” is broader than, and does not necessarily need to be, the “physiological parameter” from Claim 1. Accordingly, Claim 4 is met from Dua’s PIN-entry for validating a user. For Dua’s PIN-entry, the wireless device receives a PIN code (*value of at least one parameter associated with the smartphone*) through a PIN-code entry or text field. Dua ¶¶[0366], [0384], [0395], FIGS. 1, 3, 6(a), 8, FIG. 9; EX1042; EX1002 ¶264. The entered PIN code is then used to decrypt data or otherwise matched against a validation PIN code stored on the wallet application, thereby validating the user’s identity. Dua ¶¶[0050], [0366], [0399], [0429]; EX1002 ¶264.

6. Claim 5

(a) 5[pre]

Claim 1, *supra*. See EX1002 ¶265. Claim 5 largely involves repeating some of the steps of Claim 1, but using a different POS terminal or reader (*second entity*) for a *second transaction*.

(b) 5[a]

Dua teaches a plurality of transactions. Dua Abstract (conducting a “set of transactions”). Accordingly, Dua teaches *performing a second transaction of the plurality of financial transactions*. See EX1002 ¶266.

(c) 5[b]

Dua notes that different merchants that have already implemented POS systems can easily add contactless RF readers to those existing POS systems to immediately accept contactless payments. Dua ¶[0013]. Any such capable RF reader is a second POS reader (*second entity*) *distinct from* the first POS reader (*first entity*) and also distinct from the WCM and the external wallet storage service (the alternative *first devices*). EX1002 ¶267. Dua’s system with respect to the second POS reader (*second entity*) will *detect by the smartphone that a proximity condition is satisfied* the same as discussed for limitation 1[e] for the first POS reader. *Id.*

(d) 5[c]

Dua’s system with respect to the second POS reader (*second entity*) will *establish, using the first air interface, a wireless short-range communications link between the smartphone and the second entity, in response to the proximity condition having been satisfied between the smartphone and the second entity* the same as discussed for limitation 1[f] for the first POS reader. EX1002 ¶268.

(e) 5[d]

Dua's system with respect to the second POS reader (*second entity*) will *receive, using the first air interface, a short-range signal from the second entity* the same as discussed for limitation 1[g] for the first POS reader. EX1002 ¶269.

(f) 5[e]

Dua's system with respect to the second POS reader (*second entity*) will *send by the smartphone to the second entity over the first air interface, information associated with the second data received from the first device responsive to receiving the short-range signal from the second entity* the same as discussed for limitation 1[h] for the first POS reader. The user holding the credential (*second data*) may use the handheld device to conduct a set of transactions. Dua Abstract, ¶[0026]; EX1002 ¶270.

7. Claim 6

(a) 6[pre]

Claim 1, *supra*. See EX1002 ¶271.

(b) 6[a]

As explained for 1[b]: for the **Card-Issuing Theory**, the wireless device's wallet application transmits a special code or PIN to the WCM to allow the issuer system to validate the user's identity for financial transactions; and for the **External-Storage-Authentication Theory**, the wireless device transmits a username/password for the wallet application to access the storage area to retrieve

credentials for financial transactions (both *data relating to a request to pay for a transaction*). Dua ¶[0081]. Because the special code or PIN for validating a user and the username/password to access the external storage are fundamental to receiving credentials for financial transactions, and allowing the wireless device to perform payments, they are prerequisites to payment transactions and thus *relat[e] to a request to pay*. Dua ¶¶[0180], [0492], [0495]; EX1002 ¶272.

(c) 6[b]

As explained for 1[c]: for the **Card-Issuing Theory**, subsequent to validating the user's identity, the WCM transmits the credential for financial transactions to the wallet application; and for the **External-Storage-Authentication Theory**, the wireless devices receives from the external wallet storage service credential information for financial transactions (both *data relating to an acknowledgement and/or authorization of enabling a mode/function to pay for a transaction*). Dua ¶[0081]; EX1002 ¶273.

8. Claim 7

(a) 7[pre]

Claim 1, *supra*. See EX1002 ¶274.

(b) 7[a]

For the **Card-Issuing Theory**, Dua's wallet application may store multiple electronic credentials (Dua ¶[0334]) which may be organized in a credential tree based on different issuers of credentials, *e.g.* Sample Bank, CapitalOne, Home

Depot, Gap, and ExxonMobil. Dua ¶[0345]. Dua teaches that financial institutions, government agencies, and other organizations who wish to securely deliver electronic credentials to a wireless device may use WCMs. Dua ¶[0218]. The embodiment shown in Figure 4 shows an issuer-specific WCM for “Sample Bank.” Accordingly, different issuers may use separate and specific WCMs. Any one of these other WCMs can be *the second device distinct from the first device and further distinct from the first entity*. EX1002 ¶275.

For the **External-Storage-Authentication Theory**, it would have been obvious to a POSITA that separate external storage service providers may be used for storing different credentials, personal information, and wallet settings. Dua ¶[0491]. It would be more secure to store this data in separate external storage providers because if one storage provider were compromised, the data in the other storage providers would still be safe. EX1002 ¶276. These other external storage services can be *the second device distinct from the first device and further distinct from the first entity*. *Id.*

Dua’s system with respect to this *second device* will *transmit by the smartphone third data to a second device* the same as discussed for limitation 1[b] for the first device. EX1002 ¶277.

(c) 7[b]

Dua's system with respect to this *second device* will *receive by the smartphone fourth data from the second device relating to an acknowledgement and/or authorization of enabling a mode/function to pay for a financial transaction* the same as discussed for limitation 6[b] for the first device. EX1002 ¶278.

(d) 7[c]

Dua's system with respect to this *second device* will *transmit by the smartphone third data to a second device and receive by the smartphone fourth data from the second device over the air interface that differs from the first air interface*, the same discussed for limitation 1[j] for the first device. EX1002 ¶279.

9. Claim 8

(a) 8[pre]

Claim 1, *supra*. See EX1002 ¶280.

(b) 8[a]

Dua discloses *causing data to be transmitted selectively to a plurality of predetermined devices*. After the transaction is authorized and approved, the retailer transaction processing system issues receipt requests for the transactions to the WCMs and concurrently sends approval messages to the POS. Dua ¶[0434]. Accordingly, *responsive to performing a financial transaction*, Dua's method *caus[es] data* (receipt requests and approval messages) *to be transmitted to a*

plurality of predetermined devices (WCMs and POS devices). EX1002 ¶281. This sending is *selective* because the retailer transaction processing system issues receipt requests to WCMs and approval messages to POS devices (*a plurality of predetermined devices*) that it interfaces with. Dua ¶[0434]; EX1002 ¶281.

Dua further discloses *causing data to be received selectively from said plurality of predetermined devices* by explaining that the wireless device receives digital receipts of the transaction from merchants' WCM. The wallet application can "receiv[e] digital receipts from merchants," which are a "record of payment transaction... during a... transaction using the wallet application." Dua ¶[0430]. This information is transmitted after payment is complete (*responsive to performing a financial transaction*). EX1002 ¶282.

In its infringement contentions, Patent Owner maps the plurality of predetermined devices to base stations. EX1016 at 95-96. Applying this theory, Dua's system also causes data to be transmitted selectively to and selectively received from a plurality of predetermined devices, *i.e.* base stations, because Dua's system controls and distributes credentials using the Internet. Dua Abstract; Figures 1, 3; EX1002 ¶283.

10. Claim 9

(a) 9[pre]

Claim 1, *supra*. See EX1002 ¶284.

(b) 9[a]

Limitation 9[a] lists specific protocols to be used for the *second air interface*. In Dua, transmission and reception of data can occur across a number of wireless communication channels and protocols, including Wi-Fi. Dua ¶¶[0016], [0041], [0494], FIGS. 3, 8. OFDM is the digital modulation scheme employed by Wi-Fi and LTE. EX1002 ¶¶285-286. Accordingly, the *second air interface* (Wi-Fi) *comprises an Orthogonal Frequency Division Multiplexed and/or an Orthogonal Frequency Division Multiple Access (OFDM/OFDMA) technology. Id.*

11. Claim 10

Claim 10 is substantively identical to claim 1, except:

(1) 10[b] further requires that transmitting first data to a first device is a *precursor to performing the plurality of financial transactions*. As explained for limitation 1[b], the transmission of the special code or PIN for the **Card-Issuing Theory** and the transmission of the username/password for the **External-Storage-Authentication Theory** (*first data*) occurs before performing the plurality of financial transactions.

(2) 10[c] does not require that *the second data relate to the plurality of financial transactions to be conducted and differing from the first data*” which is a requirement in 1[c].

(3) The information of 10[h] is *based on the second data received from the first device*, while the information of 1[h] is *associated with the second data*. But the payment credentials (*information*) is the same credentials received from the WCM or the external storage service provider (*second data*). Accordingly, the *information* is *based on the second data*, and 10[h] is met as explained for limitation 1[h]. EX1002 ¶287.

12. Claims 11-17

Claims 11-17 are substantively identical to claims 2-8, except claims 12 and 13 include the *based on* language as explained for 10[h]. EX1002 ¶288.

C. Secondary Considerations

Any secondary considerations weigh in favor of obviousness, and do not overcome the strong showing of obviousness. EX1002 ¶¶289-291. Patent Owner has never practiced the claimed invention, evidencing a lack of commercial success for any product practicing the '432 patent. EX1002 ¶290. Additionally, there was no long felt, unresolved need met by the '432 patent: to the extent wide-scale deployment of contactless payments with mobile devices was delayed in the U.S., it was because of industry and market barriers, not technical barriers. EX1002 ¶291. Further, the vast number of contactless payment systems, and trials of those systems before the '432 patent's priority date, indicates that many within the market observed

the desirability of such systems and were concurrently working towards implementing them. *See* Section IV; EX1002 ¶291.

IX. STIPULATION

Petitioner hereby stipulates that if the Board institutes *inter partes* review, Petitioner will not pursue in the district court litigation:

1. any ground raised or that could have reasonably been raised in the petition;
2. any ground that relies on a patent or printed publication as its primary reference; or
3. any ground that includes Jain or Dua in an obviousness combination.

Simply put, if the review is instituted, Petitioner does not at this time intend to present prior art invalidity based on patents or printed publication (beyond as evidence of operation of system prior art) in district court and instead intends to go to trial based on system prior art, including the system prior art described above in Section IV (“State of the Art”). However, district court litigation is still in its early stages, Petitioner has not yet received all documents responsive to subpoenas issued to the companies responsible for the prior art systems, and Patent Owner has not yet fully disclosed its validity contentions. As such, Petitioner cannot at this time exclude the possibility that it may rely on patents or printed publications that are not the basis of the Grounds set forth herein to address discrete gaps in its discovery into

prior art systems (*e.g.*, if Petitioner is unable to obtain discovery into how Kyocera implemented biometric verification, it may need to rely on printed publications to render those limitations obvious). But aside from this minor reservation of rights pertaining to secondary references, Petitioner intends to bifurcate its invalidity case: invalidity grounds based on patents and printed publications will be litigated in this IPR, and invalidity grounds based on prior art systems will be litigated in district court.

X. CONCLUSION

For the reasons above, *inter partes* review is requested.

Date: May 23, 2025

Respectfully submitted,

By: /s/ James Glass

James M. Glass

Counsel for Petitioner

CERTIFICATION UNDER 37 C.F.R. § 42.24

Under the provisions of 37 C.F.R. § 42.24, the undersigned hereby certifies that the word count for the foregoing Petition for *inter partes* review (excluding the table of contents, table of authorities, mandatory notices, certificate of service or word count, and appendix of exhibits or claim listing) totals 14,000 words, which is within the word limit allowed under 37 C.F.R. § 42.24(a)(i).

Date: May 23, 2025

/s/ James Glass

James Glass (Reg. No. 46729)

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 42.6(e), 42.105(a), the undersigned hereby certifies service on the PO of a copy of this Petition and its respective exhibits at the official correspondence address for the attorneys of record for the '432 patent as shown in USPTO PAIR via FedEx:

Carlson, Caspers, Vandenburg & Lindquist, P.A.
225 S. Sixth St.
Ste. 4200
Minneapolis, MN 55402
UNITED STATES

Courtesy copies were also sent via electronic mail to Patent Owner's counsel of record in the related district court proceeding:

Kirk T. Bradley (NC 26490)
Karlee N. Wroblewski (NC 55043)
Mary I. Riolo (NC 59644)
Alston & Bird LLP
1120 South Tryon Street, Suite 300
Charlotte, NC 28203
Telephone: (704) 444-1000
Email: kirk.bradley@alston.com
Email: karlee.wroblewski@alston.com
Email: mary.riolo@alston.com
Email: TelcomVentures@alston.com

Theodore Stevenson, III (TX 19196650)
Jacob W. Young (TX 24131943)
Alston & Bird LLP
2200 Ross Avenue, Suite 2300
Dallas, TX 75201
Telephone: (214) 922-3507
Email: ted.stevenson@alston.com
Email: jacob.young@alston.com

Email: apederson@carlsoncaspers.com

Date: May 23, 2025

/s/ James Glass

James Glass (Reg. No. 46729)