

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. IPR2025-00957

U.S. Patent No. 11,937,172

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 11,937,172**

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. '172 PATENT.....	6
A. '172 Patent Specification	6
B. Prosecution History (EX1014).....	6
VI. PERSON OF ORDINARY SKILL	7
VII. CLAIM CONSTRUCTION	7
VIII. GROUNDS	7
A. Ground 1: Jain (EX1017)	7
1. Background	7
2. Analysis.....	9
B. Ground 2: Dua (EX1018).....	39
1. Background	39
2. Analysis.....	40
C. Secondary Considerations	70
IX. NO BASIS FOR DISCRETIONARY DENIAL	70
A. 35 U.S.C. § 325(d) Supports Institution.....	70
B. <i>Fintiv</i> Supports Institution.....	72
X. CONCLUSION.....	73

EXHIBIT LIST

Ex.	Description
EX1001	U.S. Patent No. 11,937,172 (“’172 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 ’172 Patent
EX1017	U.S. Pub. No. 2009/0069049 (“Jain”)
EX1018	U.S. Pub. No. 2006/0165060 (“Dua”)
EX1019	U.S. Pub. No. 2010/0082481

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

EX1034	Near Field Communication - Interface and Protocol (NFCIP-1), Standard ECMA-340 (December 2002)
EX1035	NFC Forum News Conference, NFC Forum (June 5, 2006)
EX1036	Dean A. Gratton, “Developing Practical Wireless Applications”, Elsevier Digital Press (2007)
EX1037	Jacki Katzman, “NFC Forum Unveils Technology Architecture and Announces Initial Specifications and Mandatory Tag Format Support”, NFC Forum, at 3 (June 5, 2006)
EX1038	Arumugam et al., “Consumer Electronics Application and Coverage Constraints Using Bluetooth and Proposed Bluetooth Evolution Technologies” (Aug. 2001)
EX1039	U.S. Pub. No. 2010/0082445
EX1040	Information Sciences Institute, RFC 793 Transmission Control Protocol (Sep. 1981), https://datatracker.ietf.org/doc/html/rfc793
EX1041	“Bluetooth Basics”, Bluetooth (Apr. 23, 2006), https://web.archive.org/web/20060423011921/http://www.bluetooth.com/Bluetooth/Learn/Basics/
EX1042	“iPhone Premieres This Friday Night at Apple Retail Stores”, Apple (Jun. 28, 2007), https://www.apple.com/newsroom/2007/06/28iPhone-Premieres-This-Friday-Night-at-Apple-Retail-Stores/

LIST OF CHALLENGED CLAIMS

Claim	Limitation
1[pre]	A method of operating a smartphone in performing at least one financial transaction; the method including a two-step process in establishing and using a capability in order to perform said at least one financial transaction; the method comprising:
1[a]	responsive to sensing at least one parameter by at least one sensor of the smartphone and responsive to determining that the at least one parameter that is sensed satisfies a criterion, performing a first step of said two-step process by enabling a mode to communicate by the smartphone information requesting an authorization to establish said capability;
1[b]	while the mode is enabled, and as a precursor to performing a second step of said two-step process, transmitting by the smartphone first data to a first device requesting the authorization to establish said capability to perform said at least one financial transaction; and
1[c]	receiving by the smartphone second data from the first device, comprising the authorization, responsive to said transmitting by the smartphone the first data; then
1[d]	performing the second step of said two-step process comprising performing a first transaction of said at least one financial transaction, responsive to detecting by the smartphone that a proximity condition is satisfied and responsive to sensing the at least one parameter and determining that the at least one parameter sensed satisfies the criterion;
1[e]	wherein said performing the second step of said two-step process comprises sensing that the proximity condition is satisfied relative to an access point maintained by a vendor at a point of purchase counter, by detecting a short-range signal that is transmitted by the access point, determining that a value of the at least one parameter that is sensed satisfies the criterion and then, responsive to having sensed that the proximity condition is satisfied relative to the access point and having determined that the value of the at least one parameter sensed satisfies

Claim	Limitation
	the criterion, paying for a product by selectively sending information to at least one device;
1[f]	wherein said paying for a product by selectively sending information to at least one device comprises selectively and wirelessly transmitting information to the at least one device using unlicensed frequencies; and
1[g]	wherein said at least one parameter comprises a signal, a number, a word, a code, a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state.
2[pre]	The method of claim 1,
2[a]	wherein said enabling a mode to communicate by the smartphone information requesting an authorization comprises enabling a first function of the smartphone while disabling a second function of the smartphone responsive to the at least one parameter having been sensed by the at least one sensor of the smartphone and further responsive to having determined that the at least one parameter that is sensed satisfies the criterion; and
2[b]	then selectively communicating with the first device by using a communications capability of the first function, selectively establishing a master-slave relationship with the first device, and selectively requesting from the first device the authorization to establish the capability to conduct said at least one financial transaction.
3[pre]	The method of claim 2, further comprising:
3[a]	repeatedly sensing the at least one parameter and repeatedly deciding, based on comparing a value of the at least one parameter sensed to the criterion, whether or not to maintain enabled said first function while maintaining disabled said second function; and
3[b]	maintaining enabled said first function while maintaining disabled said second function responsive to deciding that said value of the at least one parameter continues to satisfy the criterion; or

Claim	Limitation
3[c]	disabling said first function and enabling said second function responsive to deciding that the value of the at least one parameter no longer satisfies the criterion.
4[pre]	The method of claim 1,
4[a]	wherein said transmitting by the smartphone first data to a first device is responsive to the at least one parameter having been sensed by the at least one sensor of the smartphone and is further responsive to having determined that the at least one parameter that is sensed satisfies the criterion; and
4[b]	wherein said receiving by the smartphone second data from the first device is responsive to said transmitting by the smartphone the first data and comprises receiving by the smartphone information relating to an acknowledgement and/or authorization to establish and use the capability to perform said at least one financial transaction.
5[pre]	The method of claim 1, further comprising:
5[a]	responsive to performing a financial transaction, causing data to be transmitted selectively to at least one device and further causing data to be received selectively from at least one device.
6[pre]	The method of claim 1,
6[a]	wherein said transmitting by the smartphone first data to a first device and receiving by the smartphone second data from the first device comprises wirelessly transmitting/receiving by the smartphone using unlicensed frequencies, licensed frequencies, a WiFi air interface protocol, an Orthogonal Frequency Division Multiplexing air interface protocol and/or an Orthogonal Frequency Division Multiple Access air interface protocol.
7[pre]	The method of claim 1,
7[a]	wherein said paying for a product further comprises deducting/withdrawing an amount of money from an account.

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

Claim	Limitation
9[e]	wherein said performing the second step of said two-step process comprises sensing that the proximity condition is satisfied relative to an access point maintained by a vendor at a point of purchase counter, by detecting a short-range signal that is transmitted by the access point, determining that a value of the at least one parameter that is sensed satisfies the criterion and then, responsive to having sensed that the proximity condition is satisfied relative to the access point and having determined that the value of the at least one parameter sensed satisfies the criterion, paying for a product by selectively sending information to at least one device;
9[f]	wherein said paying for a product by selectively sending information to at least one device comprises selectively and wirelessly transmitting information to the at least one device using unlicensed frequencies; and
9[g]	wherein said at least one parameter comprises a signal, a number, a word, a code, a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state.
10[pre]	The smartphone of claim 9,
10[a]	wherein said enabling a mode to communicate by the smartphone information requesting an authorization comprises enabling a first function of the smartphone while disabling a second function of the smartphone responsive to the at least one parameter having been sensed by the at least one sensor of the smartphone and further responsive to having determined that the at least one parameter that is sensed satisfies the criterion; and
10[b]	then selectively communicating with the first device by using a communications capability of the first function, selectively establishing a master-slave relationship with the first device, and selectively requesting from the first device the authorization to establish the capability to conduct said at least one financial transaction.
11[pre]	The smartphone of claim 10, wherein the operations further comprise:

Claim	Limitation
11[a]	repeatedly sensing the at least one parameter and repeatedly deciding, based on comparing a value of the at least one parameter sensed to the criterion, whether or not to maintain enabled said first function while maintaining disabled said second function; and
11[b]	maintaining enabled said first function while maintaining disabled said second function responsive to deciding that said value of the at least one parameter continues to satisfy the criterion; or
11[c]	disabling said first function and enabling said second function responsive to deciding that the value of the at least one parameter no longer satisfies the criterion.
12[pre]	The smartphone of claim 9,
12[a]	wherein said transmitting first data to a first device is responsive to the at least one parameter having been sensed by the at least one sensor of the smartphone and is further responsive to having determined that the at least one parameter that is sensed satisfies the criterion; and
12[b]	wherein said receiving by the smartphone second data from the first device is responsive to said transmitting by the smartphone the first data and comprises receiving by the smartphone information relating to an acknowledgement and/or authorization to establish and use t capability to perform said at least one financial transaction.
13[pre]	The smartphone of claim 9, wherein the operations further comprise:
13[a]	responsive to performing a financial transaction, causing data to be transmitted selectively to at least one device and further causing data to be received selectively from at least one device.
14[pre]	The smartphone of claim 9,
14[a]	wherein said transmitting first data to a first device and said receiving second data from the first device comprises wirelessly transmitting/receiving by the smartphone using unlicensed frequencies, licensed frequencies, a WiFi air interface protocol, an Orthogonal

Claim	Limitation
	Frequency Division Multiplexing air interface protocol and/or an Orthogonal Frequency Division Multiple Access air interface protocol.
15[pre]	The smartphone of claim 9,
15[a]	wherein said paying for a product further comprises deducting/withdrawing an amount of money from an account.
16[pre]	The smartphone of claim 9,
16[a]	wherein said using unlicensed frequencies comprises using unlicensed frequencies in a Time Division Duplex operation;
16[b]	wherein said selectively sending information to at least one device comprises selectively sending information to the access point maintained by the vendor at the point of purchase counter and to at least one other device that is predetermined; and/or
16[c]	wherein the operations further comprise selectively receiving information from the access point maintained by the vendor at the point of purchase counter and from at least one other device that is predetermined.

I. INTRODUCTION

The '172 patent is directed to performing a “financial transaction” using a “smartphone.” It does not, however, disclose any non-obvious technology for performing such a transaction. 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 prior art 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 '172 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 '172 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 '172 patent is in the same family as U.S. Patents Nos. 9,462,411, 9,832,708, 10,219,199, 10,674,432, 11,770,756, 11,924,743, and 12,028,793, all also asserted against Petitioner. Petitioner is in the process of 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 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 (any any additional fees) to Deposit Account No. 50-5708.

E. Requirements for Inter Partes Review

Petitioner certifies that the '172 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 (U.S. Pat. Appl. Pub. No. 2009/0069049)	1-16
2	§103	Dua (U.S. Pat. Appl. Pub. No. 2006/0165060)	1-16

IV. STATE OF THE ART

As the '172 patent recognizes, mobile phones could communicate using a variety of wireless protocols and frequencies that were well known prior to the alleged invention in late 2008. EX1001 at 1:35-61. Indeed, the market for mobile phones capable of cellular communications was well-established by the 1990s, with the Nokia 3210 released in 1999 eventually selling over 160 million units. EX1002 ¶85. Manufacturers added other standardized wireless communication technology to mobile phones by the early 2000s. The first IEEE standard for Wi-Fi (802.11) was published in 1997, and by 2005 phones with both cellular and Wi-Fi communication capabilities, such as the 2005 Samsung SCH-i730, were common. EX1002 ¶85. So too were phones with Bluetooth capabilities, such as the Nokia 6310 and, again, the Samsung SCH-i730. EX1002 ¶85.

Near Field Communication (NFC) was also common at that time, and used RFID technology (*i.e.*, magnetic field induction) to allow short-range wireless communications between devices in close proximity. EX1002 ¶¶86, 129, 132. Examples of mobile phones with integrated NFC capabilities include the 2004

Fujitsu F900ic, the 2004 Nokia 3220 NFC Shell, and the 2007 Nokia 6131 NFC.

EX1002 ¶86.

Manufacturers quickly deployed applications leveraging these additional smartphone 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 mobile phones coupled with Osaifu-Keitai ("Wallet Mobile") software. EX1002 ¶87. This technology soon spread to the United States, with mobile phone and payment companies teaming up to conduct pilot programs of their own mobile payment software, including a 2006 pilot by Nokia and MasterCard, a 2007 pilot program by Motorola and Discover, and a 2007 pilot by Kyocera and MasterCard, with companies such as ViVOtech releasing full mobile payment solutions. EX1002 ¶87; *see also* EX1022:



See also screenshots from EX1033:



As mobile phones evolved into smartphones and were increasingly used for sensitive activities (*e.g.*, financial transactions) and to store sensitive user data (*e.g.*, payment account information), mobile phone security received industry attention. EX1002 ¶88. 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. EX1002 ¶88. For example, the mobile phones used for mobile payments in the 2007 Kyocera and MasterCard trial included fingerprint scanners and required biometric authentication. EX1002 ¶88; *see also* EX1023 **Error! Hyperlink reference not valid.**(describing Kyocera trial of “mobile payment technology” from ViVOtech with “biometric security, with fingerprint scanners from Atrua Technologies for transactional security on the test handsets”).

V. '172 PATENT

A. '172 Patent Specification

The specification assumes familiarity with a “wireless communications device” such as “a wireless terminal, a wireless/mobile phone, a Personal Digital Assistant (PDA), a smart phone, a multi-media device including Global Positioning System (GPS) capability, etc.” EX1001 at 1:60-2:8, 3:17-21. It relies on long-established, generic concepts of computer systems such as “authorization” (5:48-50), “sensors” capable of detecting, inter alia, physiological input (mentioned only at 6:17-34), “short-range communications” (mentioned in the specification only at 8:29-34 and 8:56-65), “air interface[s]” (6:63-64, with a recitation of then-existing interfaces at 7:21-31), 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 1:39-40. It also assumes that mobile phones could act as digital wallets. EX1001 at 1:49-52. The specification does not disclose or purport to disclose new or improved means of sensing (including physiological/biometric sensing) or proximity detection. EX1002 ¶¶38-39.

B. Prosecution History (EX1014)

The Examiner allowed the claims of the '172 patent without any rejections. EX1002 ¶40.

VI. PERSON OF ORDINARY SKILL

A person of ordinary skill in the art at the time of the '172 patent ("POSITA") had at least a Bachelor of Science in electrical engineering, computer engineering, or similar fields and at least two years of practical experience in the field of secure wireless communication applications. More education can supplement for less practical experience, and vice versa. EX1002 ¶¶77-79.

Petitioner's expert, Dr. Almeroth, exceeded this level by the priority date. EX1002 ¶80.

VII. CLAIM CONSTRUCTION

No express constructions are required to find the '172 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

Jain is prior art under at least pre-AIA 35 U.S.C. § 102(e), having been filed Sep. 5, 2008 and thus before the earliest effective filing date of the '172 patent. Jain discloses all limitations of the '172 patent claims, but Petitioner presents Jain as an obviousness reference in the event Patent Owner argues there are differences between Jain and the '172 patent claims.

While each limitation is addressed in the “Analysis” section below in detail, given the repetitive and nonsequential nature of the ’172 patent’s claim language, below is a short, non-limiting overview of Ground 1:

’172 patent claim 1 requires a “first step” for “establishing a capability” to engage in a “financial transaction.” This “first step” consists of (1) determining if a parameter (*e.g.*, a signal, number, or physiological state) meets a criterion; (2) if the criterion is met, enabling a communications mode; and (3) using that communications mode to request and then receive authorization to establish the capability to engage in financial transactions. Jain discloses the same sequence by (1) performing user authentication via PIN or biometrics (*e.g.*, Fig. 7B, steps 734-742); (2) if user is authorized, updating device signatures to enable cellular communications with a financial institution (*e.g.*, Fig. 7A, step 714); and (3) using the cellular communications to request and receive an activation code from the financial institution (*e.g.*, Fig. 9, steps 920-926).

’172 patent claim 1 also requires a “second step” for then “using” the capability to engage in a financial transaction. This “second step” consists of (1) detecting if the smartphone is in proximity of an access point; (2) determining if the criterion is satisfied (according to Patent Owner, this criterion is satisfied by the claimed “first step” and no further determining is required); and (3) if both the criterion and the proximity condition are satisfied, performing the financial

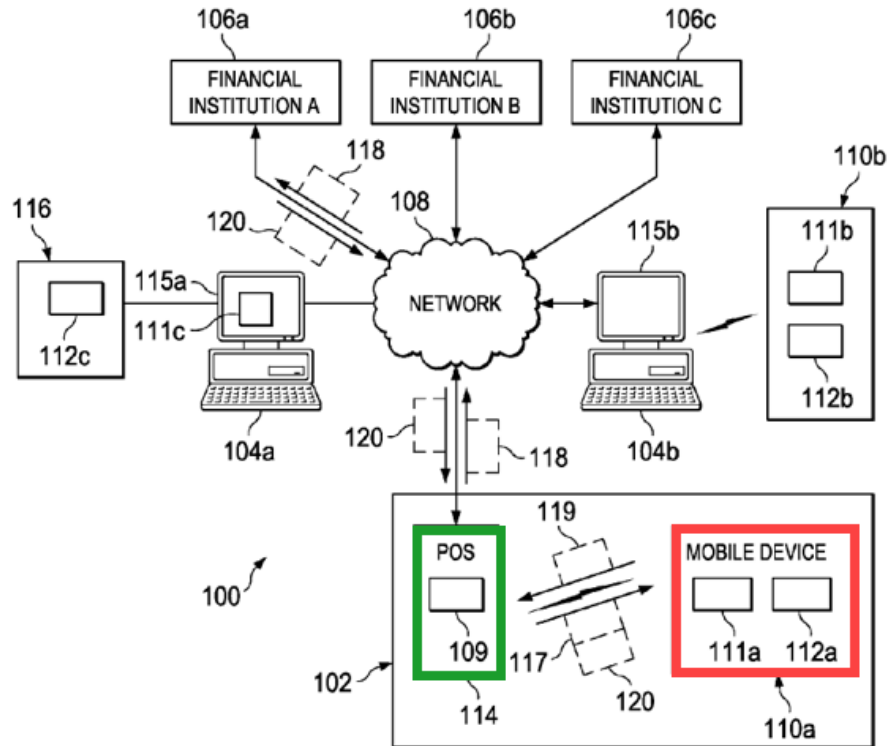
transaction by sending information to an access point. Again, Jain discloses the same sequence by (1) detecting if the mobile device is sufficiently close to a point of sale terminal to receive a transaction request via a short-range NFC signal (*e.g.*, ¶[0023], [0027]); (2) prompting the user to enter a PIN, either as part of the claimed first step (*e.g.*, Fig. 7B, steps 734-742) or again for individual transactions (*e.g.*, ¶[0029]); and (3) if both conditions are met, transmitting a transaction response containing information associated with a payment account (*e.g.*, ¶[0027]).

2. Analysis

(a) Claim 1

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

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 retail point-of-sale terminal 114. Jain ¶¶[0005], [0018], [0021], [0029]; FIG 1 (annotated):



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

111. Jain ¶[0027]. The exchange between the mobile device 110 and POS device 114 uses short range signals such as NFC or Bluetooth. Jain ¶[0023]. *See also* EX1002 ¶97.

A POSITA would understand that transaction card 112 is part of the smartphone because transaction card 112 can be “software, hardware, and/or firmware” while “mobile device 110 does not require additional hardware, software, and/or firmware.” Jain ¶[0023], Fig. 1. *See also* EX1002 ¶¶95-96.

Moreover, to the extent Patent Owner argues Jain’s transaction card 112 cannot be considered part of mobile device 110, Jain at least renders obvious implementing the processes discussed herein in connection with a transaction card 112 that is integrated into mobile device 110. EX1002 ¶¶97-100. A POSITA would make this change because separability of the transaction card is not always advantageous (e.g., a smartphone vendor might find it commercially advantageous to provide transaction card functionality with their smartphone but not allow users to leverage that functionality with other devices). EX1002 ¶100. 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 while leveraging components of the mobile device 110. EX1002 ¶¶97-99. Finally, incorporating transaction card 112 into mobile device 110 protects

against inadvertent loss of the transaction card 112 if it were to, *e.g.*, become detached from mobile device 110 without the user noticing. EX1002 ¶101.

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

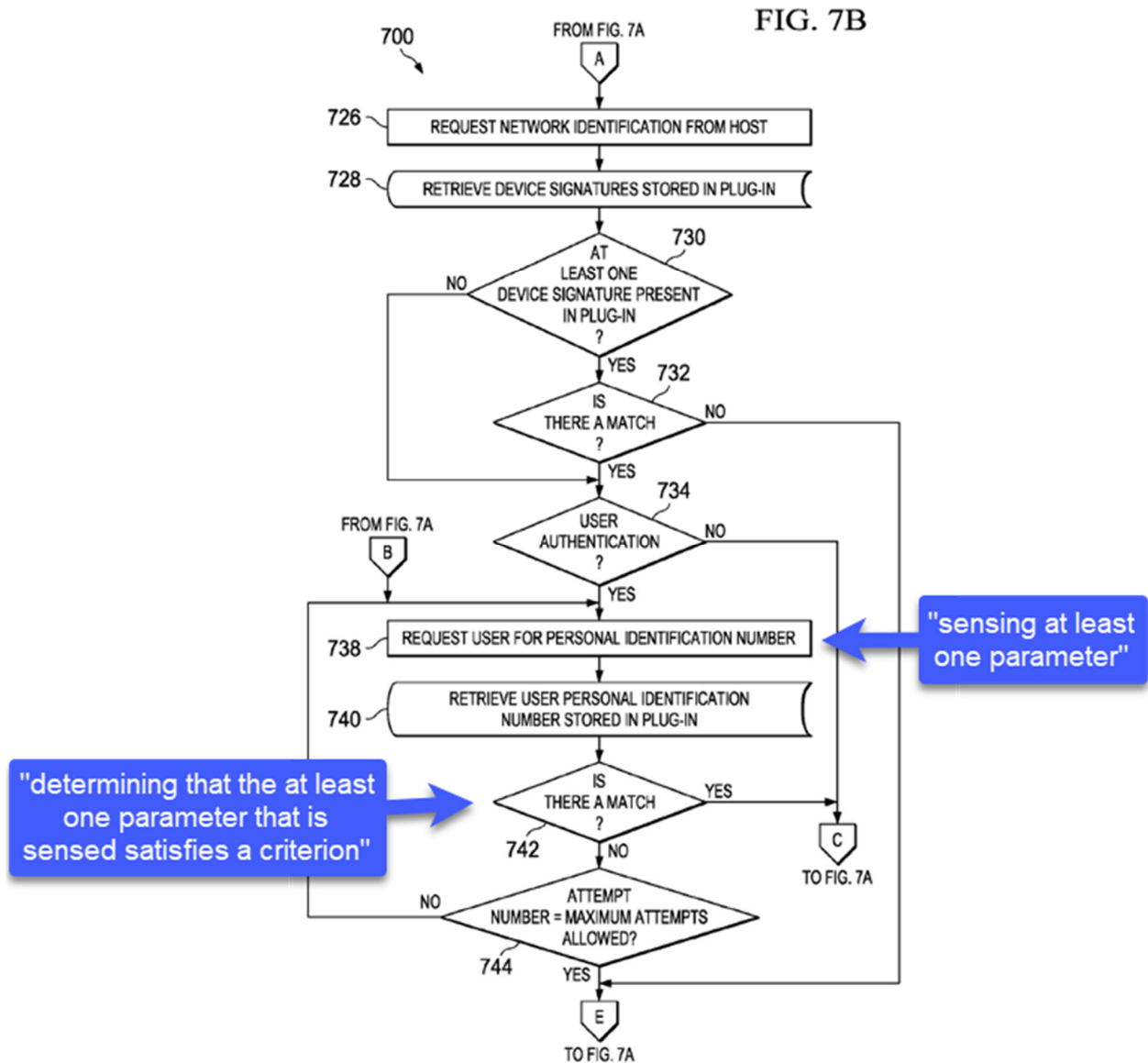
Jain discloses the claimed *two-step process*. For the claimed *first step*, Jain discloses authenticating (Jain ¶¶[0072]-[0075], Fig. 7) and activating (Jain ¶¶[0080]-[0081], Fig. 9) a transaction card with an associated financial institution to *establish... a capability in order to perform said at least one financial transaction*. Jain's disclosure of the claimed first step is addressed below in connection with limitations 1[a]-[c]. *See also* EX1002 ¶¶102-105.

For the claimed *second step*, Jain discloses then using the transaction card to *perform said at least one financial transaction*. Jain, Abstract, ¶¶[0019], [0023], [0027]-[0029]. Jain's disclosure of the claimed second step is addressed below in connection with limitations 1[d]-[f]. *See also* EX1002 ¶106.

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

The claim begins with a prerequisite to the *first step: determining* if a *criterion* is satisfied. Jain discloses this prerequisite in steps 734-742 of Fig. 7B. Specifically, Jain discloses an authentication process for “automatically

bootstrapping” transaction card 112 to mobile device 110, which includes authenticating a user using a PIN number or biometrics (e.g., fingerprint). Jain ¶¶[0072], [0075], Fig. 7B (annotated); EX1002 ¶107.



At step 738, the smartphone receives a PIN (*sensing at least one parameter*) via the mobile device’s touch screen (*at least one sensor of the smartphone*), which a POSITA would also understand as a sensor for sensing touch (e.g., capacitive touch

screen). Jain ¶¶[0022], [0075]; EX1042. At step 740, the smartphone retrieves a locally stored PIN. Jain ¶[0075]. Then, at step 742 (“is there a match?”), the mobile device *determin[es]* whether the user-inputted PIN matches the locally-stored PIN (*satisfies a criterion*). Jain ¶[0075], Fig. 7B. *See also* EX1002 ¶108.

Jain also discloses that rather than “entering a PIN... the user may be authenticated using... biometric information (*e.g.*, fingerprint).” Jain ¶[0075]. Thus, Jain discloses performing steps 738, 740, and 742 in the context of biometric verification, where step 738 senses “biometric information” using a biometric sensor, step 740 retrieves locally stored biometric information, and step 742 determines if the sensed biometric information matches the stored biometric information. EX1002 ¶¶109-110.

Further confirming this limitation is met, Patent Owner alleges in its infringement contentions in the district court litigation that the use of biometric verification is itself sufficient to show the claimed *sensing* and *determining*. EX1016 at 29-42; *see also* EX1002 ¶¶111.

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 well aware of such implementations. *See* EX1021 ¶¶[0040]-[0042]; EX1024 ¶[0009], [0025]; EX1025 ¶[0044], [0086]-[0092]; EX1026 at 28-29, 196; EX1027 at 1370-73. The purpose of biometric authentication is to ensure biometric

information of a current user matches the biometric information of the rightful owner of the device. This entails first storing the biometric information of the rightful owner during a setup stage and then comparing that stored biometric information to the biometric information of a current user. The claimed “*criteria*” requires that the stored and sensed biometric information sufficiently correlate such that there is adequate confidence that the current user is the device’s owner. Otherwise, biometric information authentication would not serve its central purpose. EX1002 ¶¶112-114.

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

The next limitation is a second prerequisite to the claimed *first step*: after *determining* an unspecified *criterion* is satisfied, the claims require *enabling a mode to communicate*. Jain discloses this limitation. In response to authenticating the user in steps 738-744 of Fig. 7B (claimed *determining*), 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], Fig. 7A (annotated). *See also* EX1002 ¶¶115-117.



Once the host-device signature is updated in step 714 to match the host device, the transaction card completes the bootstrap operation and can communicate with the host, which includes using the host's cellular radio technology; otherwise, the "host device is rejected, bootstrap is aborted and the card 400 is returned to the mode it was before being inserted into the device." Jain ¶[0065]. Only after bootstrapping/authentication (Figure 7) is complete 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 radio communication with a financial institution as part of process 900 (*enable[s] a mode to communicate by the smartphone information*). See also EX1002 ¶¶118-120.

As explained below in connection with limitations 1[b] and 1[c], process 900 entails “*requesting an authorization to establish [a] capability*” to perform financial transactions.

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

Finally, with the claimed *determining* and *enabling* complete, claim 1 recites *requesting* and *receiving authorization* to engage in *financial transactions*.

In Jain, after the user is authenticated by PIN or biometrics and the host device signature is updated to allow the 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 of this method, mobile device 110 “wirelessly transmits a request for the activation code using the cellular radio technology” (*transmitting by the smartphone first data*) to the financial institution¹ (*first device*). Jain ¶[0081], Fig. 9 (annotated). *See also* EX1002 ¶¶121.

¹ Jain uses the term “financial institution” to refer to devices, such as devices in an enterprise that authorize transactions through the network 108 by accepting data from clients and returning appropriate responses using, for example, the HTML or XML formats. Jain ¶¶[0038], [0039].

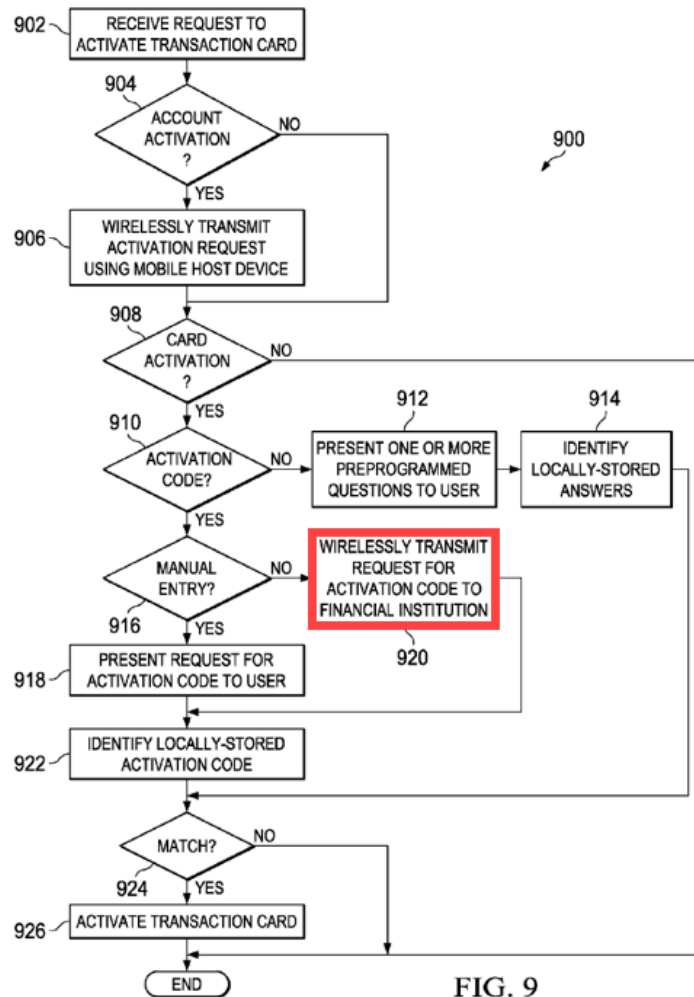


FIG. 9

In response to the request of step 924, mobile device 110 (*smartphone*) receives an activation code (*second data... comprising the authorization*) from the financial institution (*first device*). The received activation code is then 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 then perform payments

with the associated financial account by “signifying activation of the financial vehicle carried on the card” (Jain ¶[0071]). *See also* EX1002 ¶¶122, 125.

Thus, step 920 and 924 are performed in order to “activat[e] the transaction card and/or financial account.” Jain ¶[0026]. Because the matching “activation code” is required to enable that card to perform financial transactions (*establish said capability to perform said at least one financial transaction*), a matching “activation code” is an *authorization* to engage in financial transactions, and requesting the same is thus *requesting the authorization*. This mirrors Patent Owner’s infringement contentions, where Patent Owner asserts that receiving an issued credit card to enable financial transactions is sufficient to establish “*receiving... second data... comprising... authorization.*” EX1016 at 23-28. *See also* EX1002 ¶¶122-126.

A POSITA would further understand that the financial institution would not provide a matching activation code if the smartphone is not authorized to perform payment services with the financial institution. This understanding is supported by step 924, which compares the activation code received by the financial institution with a locally stored activation code to determine “[i]f the locally stored information matches the provided” activation code. Jain ¶[0081]; Fig. 9; EX1002 ¶125. This step (indeed, the entire requirement for an activation code) would be superfluous if

receipt of a matching activation code did not serve an *authorization* function.

EX1002 ¶¶122-126.

At a minimum, such an implementation was well known and would have been obvious, as evidenced by numerous references describing similar processes. *See, e.g.,* EX1019 ¶¶[0145]-[0146] (describing “verification process” whereby information is “transmitted to the corresponding credit card provider” so the provider can confirm the information is “valid” and “confirm the identi[ty] of the user by transmitting one or more verification codes” to the user device, thereby “ensur[ing] that only the authorized user or users will receive the verification code”). A POSITA would be motivated to treat Jain’s matching activation code as an authorization (and not provide the same if the transaction card is unauthorized) in order to improve system security and guard against fraudulent transaction cards. Indeed, if Jain’s system returned a matching activation code every time, including in response to requests from fraudulent transaction cards, there would be no reason to implement steps 920-924 of Jain’s process 900. *See also* EX1002 ¶127.

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

For the claimed *second step*, Jain discloses using the authenticated and activated transaction card to *perform a first financial transaction*. Jain Abstract,

¶¶[0019], [0023], [0027]-[0029]. Jain’s disclosure of the claimed *second step* is addressed below in connection with limitations 1[d][ii]-[f]. *See also* EX1002 ¶128.

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

After the claimed *first step* is performed, including Jain’s authentication process 700 (Fig. 7) and activation process 900 (Fig. 9), Jain’s mobile device 110 can execute contactless payment transactions with a nearby POS device using short range signals, such as NFC or “proximity signals.” Jain ¶[0023]. The mobile device first “wirelessly receive[s] a request from the POS device 114 to execute a transaction and/or and provide a response.” Jain ¶[0023]. A POSITA would understand that Jain’s mobile device 110 is only able to processes the “request” if sufficiently close to POS device 114 to actually receive and decode the short-range signal corresponding to the request (*responsive to detecting by the smartphone that a proximity condition is satisfied*). EX1002 ¶¶129-31; EX1034 at 11-12; *see also* EX1036 at 220. Specifically, Jain’s NFC and other short range wireless communication protocols are only effective if there is an underlying signal of sufficient strength is detected such that the device and the terminal can communicate using that protocol. EX1002 ¶¶128-32; EX1035 at 4, 36; EX1037 at 3. That signal strength rapidly deteriorates as distance increase. EX1002 ¶131; EX1035 at 4, 36; EX1037 at 3. Indeed, Jain itself recognizes that NFC communication requires

proximity of “10 cm or less.” Jain ¶[0030]. Accordingly, for Jain’s mobile device to receive a request from the POS device received via NFC and process it as such, the mobile device and POS device must be sufficiently close, which a POSITA would understand corresponds to *detecting that a proximity condition is satisfied* (e.g., the device is within a range of “10 cm or less” to the POS device, Jain ¶[0030]).

Further confirming this limitation is met, Patent Owner alleges in its infringement contentions in district court litigation 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 also* EX1002 ¶136.

In addition, it would be obvious to a POSITA that Jain’s smartphone would first detect it is proximate to the POS terminal based on a signal from the POS device (e.g., a “request,” Jain ¶[0023]) prior to communicating with that POS. To ensure communications would be successful and not wasted signaling, and further to avoid the security risk of indiscriminately transmitting sensitive financial information, Jain’s smartphone first needs to detect it is near the POS prior to proceeding with a payment transaction with the POS device. EX1002 ¶¶130-35. Otherwise, the NFC communication would fail. Indeed, such implementations were well-known to a POSITA. For example, EX1020 discloses and leverages NFC to limit the range at which communication may take place. EX1020 ¶[0041], [0063] [0041]. Indeed, in the context of Wi-Fi, EX1020 even more explicitly discloses using the ability to

receive such signals as an indication of proximity. Jain ¶[0073] (“The [identifying information] may be used by the device 10 to indicate that the device is located within communication range of the hot spot 169.”). A POSITA would be motivated and able to use Jain’s NFC “request” in the same manner. EX1002 ¶¶130-35.

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

According to Patent Owner, limitation 1[d][iii] does not impose any new requirement relative to limitation 1[a][i]: the same sensing of *the* at least parameter and determining it meets *the* criterion in the *first step* is also a prerequisite to then *using* that capability in the *second step*. Compare Ex1016 at 8-14 with Ex1016 at 29-42 (pointing to the same “fingerprint unlock” and similar security functionality for both limitations).

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

a user-entered PIN and **determining** if that PIN matches a previously-stored PIN (**criteria**) to be a simple and natural, and thus obvious, way of implementing PIN authorization: it does not require communication with any other devices and allows the POSITA to reuse aspects of the software that implements the user authentication of Fig. 7. EX1002 ¶137-40.

To the extent Patent Owner argues that this second **sensing** and **determining** on the claimed **smartphone** as part of a specific transaction is required but not disclosed by Jain, at a minimum Jain renders this obvious. Jain already discloses requiring a user to enter a PIN as part of a specific transaction. Jain ¶[0029]. Jain further discloses authenticating a user via a PIN on mobile device 110. Jain ¶[0075]. Thus, Jain discloses all the elements of limitation 1[d][iii], and reusing those elements in Jain rather than, *e.g.*, reimplementing them on POS device 114 would simplify design and development, conserve computing resources, and limit transmission of sensitive user information (such as the user's PIN). Indeed, numerous prior art references requires such user authorization before permitting individual purchases. *See, e.g.*, EX1020 ¶¶[0083]-[0084], [0088], Fig. 14; EX1021 ¶[0052]; *see also* EX1002 ¶¶138-145.

Also, it would be obvious for a POSITA to replace the disclosed PIN with user biometrics to authorize the transaction. 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 additional costs. Moreover, Jain itself recognizes that biometrics are a good alternative to PINs. In addition, a POSITA would recognize 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 further improve system security. Alternatively, POSITA would also be familiar with two-factor authentication and would both (a) know how to retain PIN authentication while augmenting it with biometric authentication and (b) appreciate that the cost of doing so is warranted because of the extra security it provides for financial transactions. EX1002 ¶143; EX1028 Abstract; EX1029 Abstract; EX1030. Indeed, requiring biometric authentication before authorization of individual transactions was well known in the art. *See, e.g.*, EX1020 ¶¶[0083]-[0084], [0088], Fig. 14; EX1021 ¶[0052]; *see also* EX1002 ¶¶138-145. In addition, for the reasons discussed above in connection with limitation 1[a], Jain discloses or at least renders obvious that implementing biometric authorization would entail the claimed **sensing** and **determining**.

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

Limitation 1[e][i] for the most part just repeats the *detecting* of limitation 1[d][ii] and only further specifies that this is done “*relative to an access point maintained by a vendor at a point of purchase counter*” and by detecting “*a short-range signal that is transmitted by the access point.*” Even those requirements, however, are addressed above in connection with limitation 1[d][ii], since the POS device in Jain is *an access point maintained by a vendor at a point of purchase counter* and the request used to perform the *detecting* is a *short-range signal* (specifically, an NFC signal). Jain ¶[0023], [0029]; *see also* EX1002 ¶¶146-148.

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

Limitation 1[e][ii] just repeats the *sensing* of limitation 1[d][iii] and is disclosed for the same reasons. *See also* EX1002 ¶149.

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

Limitation 1[e][iii] for the most part just repeats the *detecting* of limitation 1[d][ii] and the *sensing* of limitation 1[d][iii] and is disclosed for the same reasons.

The only additional requirement of limitation 1[e][iii] is *paying for a product by selectively sending information to at least one device*. Jain also discloses this requirement by teaching that its mobile device, in response to a request from the

POS device, generates a transaction response 119 identifying information associated with a payment account (*information*) and *send[s]* the transaction response 119 to the nearby POS device 114 (*at least one device*).² Jain ¶¶[0027], [0029]. This sending is *selective* because it only occurs if the mobile device is sufficiently close to the POS device 114 and the user has authorized the purchase. *See supra* limitations 1[d][ii] and 1[d][iii]. *See also* EX1002 ¶¶150-151.

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

The only additional requirement of limitation 1[f] is that the “information” of limitation 1[e][iii] be sent *using unlicensed frequencies*. Jain meets this requirement by transmitting information to the POS device (*at least one device*) “using short range signals such as NFC (*e.g.*, ISO 18092/ECMA 340), ... proximity signals, and/or other signals compatible with retail payment terminals (*e.g.*, POS 114).” Jain ¶[0023]; *see also* EX1002 ¶152.

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

NFC used the 13.56 MHz ISM band, which is unlicensed. EX1002 ¶¶152-53; EX1031; EX1032 at 2. Patent Owner, in its infringement contentions, admits as much, alleging that “the wireless short-range communications link used by NFC is based upon the unlicensed 13.56 MHz frequency.” EX1016 at 57-58; EX1002 ¶154. Bluetooth also used unlicensed frequencies. EX1002 ¶155; EX1041.

(xiv) 1[g]: *wherein said at least one parameter comprises a signal, a number, a word, a code, a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state.*

As discussed with limitations 1[a][i] and 1[d][ii], Jain discloses or renders obvious sensing a PIN (personal identification *number*) or fingerprint (*physiological state*). Jain ¶[0075], claim 10. EX1002 ¶¶156-158.

(b) Claim 2

(i) 2[pre]

Claim 1, *supra*.

(ii) 2[a]

Limitation 2[a] requires that, when the *first function* of claim 1 is enabled responsive to the claimed *sensing* and *determining* of limitation 1[a][i], a *second function* is *disabl[ed]*. Jain discloses this limitation under two theories.

First, Jain’s smartphone bootstrapping/authentication process enables the mobile device 110 to communicate with the financial institution using cellular radio

technology. *See* limitations 1[a][i]-[ii]. Even after the mobile device is able to communicate with the financial institution using cellular radio technology (***enabling first function***), the mobile device remains unable to engage in payment transactions (***while disabling a second function of the smartphone***) because the transaction card is not yet activated. Jain ¶[0081]. Only once activation process 900 in Fig. 9 is also complete can the mobile device engage in financial transaction (***second function***). EX1002 ¶¶160-162.

Second, Jain meets this limitation by ***enabling a first function*** (enabling mobile device 110 to communicate with the financial institution using cellular radio technology in connection with process 900) ***while disabling a second function*** (mode the transaction card was in before being inserted into the device). In its infringement contentions, Patent Owner argued that limitation 2[a] is met by “enabling a first function (unlocking the [] smartphone or application) while disabling a second function (locking the Samsung smartphone or application).” EX1016 at 64-65. Similarly, Jain’s authorization process 700 (Fig. 7) must be completed before turning on the antenna and updating the host device signature (step 714) to enable cellular communication with the financial institution, as described in connection with process 900. Jain ¶[0073]. Conversely, if the “host device is rejected, bootstrap is aborted and the card 400 is returned to the mode it was before being inserted into the device.” Jain ¶[0065]. EX1002 ¶¶163-165.

(iii) 2[b]

Limitation 2[b] mirrors the requirements of limitations 1[a][ii], 1[b], and 1[d], but adds that the *communicating* and *requesting* are done *selectively* and further requires *selectively establishing a master-slave relationship with the first device*.

Regarding *selectively communicating* and *requesting*, those steps are only performed in Jain if the *sensing* and *determining* requirements of limitation 1[a][i] are met. Thus, the *communicating* and *requesting* in Jain is done *selectively*. EX1002 ¶166.

Additionally, Jain discloses *selectively establishing a master-slave relationship with the first device*. The '172 specification discloses a first wireless communications device acting as a “master” and a second wireless communications device acting as a “slave” if “the second wireless communications device is configured to enable a mode/function thereof” only “responsive to receiving an authorization from the first wireless communications device.” EX1001 at 5:57-63. Applying the same understanding of master-slave relationship, Jain discloses such a relationship between Jain’s financial institution (*master*) and its mobile device 110 (*slave*). Jain’s financial institution (*master*) controls operational aspects of the mobile device 110 (*slave*) related to performing financial transactions, such as allowing financial transactions in the first instance and controlling financial

instruments (e.g., credit cards, debit cards, etc.). Jain ¶¶[0028], [0075]. *See also* EX1002 ¶¶167-168.

(c) **Claim 3**

(i) **3[pre]**

Claim 2, *supra*.

(ii) **3[a]**

Limitation 3[a] repeats limitation 1[a][i] and based on the result of the claimed *sensing* and *determining* decide whether to maintain the *first function* and keep the *second function disabled*.

As discussed above in connection with limitation 2[a], in Jain, the *first function* corresponds to use of radio communication with the financial institution in connection with process 900 and the *second function* corresponds either the capability to engage financial transactions or the mode the transaction card was in before being inserted into the device. Either way, it would be an obvious security measure to repeatedly perform Jain's user authentication process in steps 734-742 of process 700 (*repeatedly sensing the at least one parameter and repeatedly deciding*), such as prompting for a PIN or biometric, when, for example, idleness causes the smartphone to re-lock to the home screen, there is network delay, or there was a change to the smartphone with potential security implications. EX1002 ¶¶170-171. Requiring re-authorization and re-activation under those circumstances would help prevent fraud. EX1002 ¶172.

With this obvious modification, the other claim elements also fall into place.

First, to further ensure security, the activation process 900 of Fig. 9 would also need to be repeated, leaving the mobile device unable to perform financial transactions until that re-activation is complete (*while maintaining disabled said second function*). EX1002 ¶173. **Second**, Jain discloses *enabling a first function* (enabling mobile device 110 to communicate with the financial institution using cellular radio technology in connection with process 900) *while disabling a second function* (the mode the transaction card was in before being inserted into the device) based on whether process 700 (including user authorization steps 734-742) is successfully completed. EX1002 ¶174.

(iii) 3[b]

Limitations 3[b] and 3[c] consist of two alternative limitations. Only one needs to be satisfied. Nonetheless, Jain discloses both.

As discussed re 2[a] and 3[a] above, Jain *maintain[s] enabled* the activation process (*first function*) while *maintain[s] disabled* the card's payment services (*second function*) based on deciding that the smartphone user is still authorized. EX1002 ¶175.

Alternatively, as discussed re 2[a] and 3[a] above, Jain *maintain[s] enabled the first function* (enabling mobile device 110 to communicate with the financial institution using cellular radio technology in connection with process 900) *while*

maintaining disabled the second function (the mode the transaction card was in before being inserted into the device) based on deciding that the smartphone user is still authorized. EX1016 at 94; *see also* EX1002 ¶176.

(iv) 3[c]

Alternatively, Jain discloses limitation 3[c] when it disables cellular communications with the financial institution by returning to the mode the transaction card was in before being inserted into the device when the user is not authenticated responsive to the *repeatedly sensing*, similar to Patent Owner's theory of locking and unlocking the smartphone's screen. EX1016 at 94; *see also* EX1002 ¶¶177-178.

(d) Claim 4

(i) 4[pre]

Claim 1, *supra*.

(ii) 4[a]

Limitation 4[a] does not add any requirements relative to limitations 1[a] and 1[b] and is thus met for the same reasons. EX1002 ¶¶180-181.

(iii) 4[b]

Limitation 4[b] repeats the requirements of limitations 1[a]-[c] and is thus met for the same reasons. EX1002 ¶¶182-183.

(e) Claim 5

(i) 5[pre]

Claim 1, *supra*.

(ii) 5[a]

Limitation 5[a] repeats the requirements of limitation 1[e][iii] but further requires *causing data to be received selectively from at least one device*. Jain meets this additional requirement by explaining that the mobile device receives from the financial institution, either directly or via POS device 114, a transaction receipt (*data*). Jain ¶[0041], [0046]. This information is transmitted after payment is complete (*responsive to performing a financial transaction*). Jain ¶[0046]; *see also* EX1002 ¶¶185-187.

In addition, in its infringement contentions, the Patent Owner stated that the smartphone “includes causing data (transaction data) to be transmitted selectively to a device (base station) and further causing data (updated account information) to be received selectively from a device (base station).” EX1016 at 130. Applying this theory, Jain’s smartphone also causes data to be transmitted selectively to and selectively received from other devices, such as Jain’s network 108, GSM core network 202, RAN 204, Base Station Controllers (BSC) 212, and/or Base Stations (BS) 210. Jain ¶[0044]; Fig. 2; *see also* EX1002 ¶188.

(f) Claim 6

(i) 6[pre]

Claim 1, *supra*.

(ii) 6[a]

Limitation 6[a] lists specific protocols that need to be used for the *transmitting* and *receiving* of limitations 1[b] and 1[c], respectively. In Jain, this *transmitting* and *receiving* is implemented using cellular radio technology. Jain ¶[0081]. The specific cellular radio technology in Jain includes GSM, CDMA, UMTS, and other modes. Jain ¶[0041]. These use *licensed frequencies*. EX1002 ¶190. And if they do not, they would use *unlicensed frequencies*, as also claimed. Either way, this claim limitation is disclosed. EX1002 ¶¶190-191.

(g) Claim 7

(i) 7[pre]

Claim 1, *supra*.

(ii) 7[a]

Jain discloses that when paying for products, the smartphone sends transaction information corresponding to credit, debit, or bank accounts. Jain ¶¶[0025], [0029], [0036]. Payments using such accounts, particularly debit accounts and bank accounts, constitute *deducting / withdrawing an amount of money from an account*. As explained, “[t]he financial institution 106 may be a credit card provider, a bank, an association (*e.g.*, VISA), a retail merchant (*e.g.*, Target), a prepaid/gift card provider, an internet bank, and/or others.” Jain ¶[0039]. During a transaction, the financial institution “may identify an account number (*e.g.*, bank account, debit-card number) and associated verification information (*e.g.*, PIN, zip code) and determine funds available to the account holder.” Jain ¶[0039]. Jain also explains

that the merchant “POS 114 may receive an indication that a transaction amount has been accepted or declined for the identified account and/or request additional information from the transaction card.” Jain ¶[0036]; *see also* EX1002 ¶¶193-194.

(h) Claim 8

(i) 8[pre]

Claim 7, *supra*.

(ii) 8[a]

Jain teaches the sending of limitation 1[f] is done via NFC or Bluetooth. Jain ¶[0023]. According to Patent Owner, “NFC communications”—which includes the NFC communications disclosed in Jain—use “*unlicensed frequencies... in a Time Division Duplex operation.*” EX1016 at 142 (emphasis added); EX1032 at 21 (describing NFC as a “half... duplex system”); EX1002 ¶197. Bluetooth also uses *unlicensed frequencies in a Time Division Duplex operations*. EX1002 ¶198; *see also* EX1038 at 1.

(iii) 8[b] & 8[c]

Limitations 8[b] and 8[c] consist of two alternative limitations. Only one needs to be satisfied. Jain discloses both.

Limitation 8[b] mirrors limitation 1[e] but further requires that the *selectively sending* is to *the access point* of claim 1 and further requires *selecting sending information ... to at least one other device that is predetermined*. Jain discloses sending the transaction response 119 identifying information associated with a

payment account to the POS device 114 (*access point*), which is then forwarded to the financial institution (*at least one other device that is predetermined*). Jain ¶¶[0027], [0029]; *see also* EX1002 ¶¶199-202.

Limitation 8[c] mirrors limitation 1[e] but further requires *selectively receiving information from the access point* of claim 1 and *selecting receiving information ... from at least one other device that is predetermined*. Jain's mobile device receives a transaction receipt from the POS terminal (*access point*) that was originally sent by the financial institution (*one other device that is predetermined*). Jain ¶[0027]; *see also* EX1002 ¶¶199-202.

Also, Patent Owner's infringement contentions rely on the theory that the accused devices "transmit the first data to a first device (base station) and receive second data (the authorization) from the device (base station) in connection with establishing the capability to perform a financial transaction." EX1016 at 130. Applying this theory to Jain, Jain's smartphone also transmits data to and receives a transaction receipt from network 108, GSM core network 202, RAN 204, MSC 206, Base Station Controllers (BSC) 212, and/or Base Stations (BS) 210 (*one other device that is predetermined*) on the way to/from the financial institution. Jain ¶[0044]; Figs. 1-2. EX1002 ¶188

Finally, to the extent Patent Owner argues the claimed *transmitting* and *receiving* to/from the *one other device that is predetermined* cannot be via the

claimed *access point*, Jain also discloses that such communication can bypass the POS device (*access point*). Jain ¶[0027] (“In 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 ¶202.

(i) Claims 9-16

Claims 9-16 are substantively identical to claims 1-8.

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 on July 27, 2006, and thus more than a year before the earliest effective filing date of the '172 patent. Dua discloses all limitations of the '172 patent claims, but Petitioner presents Dua as an obviousness reference in the event Patent Owner identifies any differences between Dua's disclosure and the '172 patent claims.

While each limitation is addressed in the “Analysis” section below in detail, given the repetitive and nonsequential nature of the '172 patent's claim language, below is a short, non-limiting overview of Ground 2:

'172 patent claim 1 requires a *first step* for *establishing a capability* to engage in *financial transactions* and a *second step* for then *using* that *capability* for a particular *financial transaction*. Those steps are broken down in Section VIII.A.1 above.

Dua discloses the claimed *first step* under two theories, the **Card-Issuing Theory** and the **External-Storage-Authentication Theory**. Under the **Card-Issuing Theory**, Dua discloses (1) performing PIN or biometric authentication to open a wallet application; (2) once the wallet is opened, establishing a SIP communication session with a credit card issuer's wireless credential manager; and (3) using the SIP communication session to receive credentials from the wireless credential manager. 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 claimed *second step* 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) if both conditions are met, transmitting the received/retrieved credentials to the point-of-sale terminal to perform the transaction.

2. Analysis

(a) Claim 1

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

Dua discloses a wireless device, which includes a *smartphone*. Dua Abstract, FIGS. 3, 5, 6(a)-8. The wireless device includes a “handheld device, such as a mobile telephone,” “capable of wirelessly connecting to the internet” and with 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[] at least one financial transaction*). Dua Abstract, ¶¶[0041], [0312]-[0313], [0333]. *See also* EX1002 ¶212.

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

Dua discloses the *two-step process [of] establishing and using*. The first *establishing* step is disclosed under two theories: (1) the issuer’s Wireless Credential Manager (WCM) 510 issuing a credit card to a mobile device (“**Card-Issuing Theory**”) (Dua ¶[0128].); and (2) the wallet application “automatically authenticat[ing] itself” to an external wallet storage service for “access[ing]... stored credentials” (“**External-Storage-Authentication Theory**”) (Dua ¶¶[0492], [0495]). Dua’s disclosure of the claimed *first step* under both theories is addressed below in connection with limitations 1[a]-[c]. *See also* EX1002 ¶¶213-214.

The second *using* step is disclosed by a subsequent “authorized transaction... via... a short range wireless link with a point-of-sale... terminal.” Dua Abstract.

Dua's disclosure of the claimed *second step* is addressed below in connection with limitations 1[d]-[f]. *See also* EX1002 ¶¶213-214.

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

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

The claim begins with two prerequisites to performing the claimed *first step* from the preamble: (1) *determining* if a *criterion* is satisfied; and (2) *enabling a mode to communicate*. Dua discloses both prerequisites under either the **Card-Issuing Theory** or the **External-Storage-Authentication Theory**.

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]. Thus, the “default security setting in the wallet application is that PIN-entry is required before the wallet application can be ‘opened’” or otherwise “allow[s] the user access to the application,” which receive an issued a credit card. Dua ¶¶[0366], [0429]. This understanding is confirmed by additional disclosure in Dua. **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 ¶¶[0366], [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 pieces credit card and other confidential information. Dua ¶¶[0041], [0055], [0287]-[0288], [0334]. Regardless of how the wallet is opened, 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]. *See also* EX1002 ¶¶216-217.

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 the wallet application’s utility regarding credit card management. EX1002 ¶¶218-220.

At a minimum, requiring PIN entry under these circumstances would be obvious. To ensure security of the other credentials, alongside allowing use of an encrypted wallet application and changes to the wallet application by an authenticated user, a POSITA would retain Dua’s “default” user authentication—PIN-entry—for credit card issuance. Dua ¶[0366]. Indeed, it was well known to require such verification before permitting access to such sensitive functionality. EX1019 ¶[0107], Fig. 10A, 10B; EX1002 ¶¶219-220.

For Dua's PIN-entry, the wireless device receives a PIN code (*parameter*) through a PIN entry or text field after the PIN code is typed in with a keyboard or touchscreen keyboard (*sensing... by at least one sensor of the smartphone*), which a POSITA would also understand as a sensor for sensing touch (*e.g.*, capacitive touch screen). Dua ¶¶[0366], [0384], [0395], FIGS. 1, 3, 6(a), 8, FIG. 9; EX1042. 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 (*determining that the at least one parameter that is sensed satisfies a criterion*). Dua ¶¶[0050], [0366], [0399], [0429]; *see also* EX1002 ¶221.

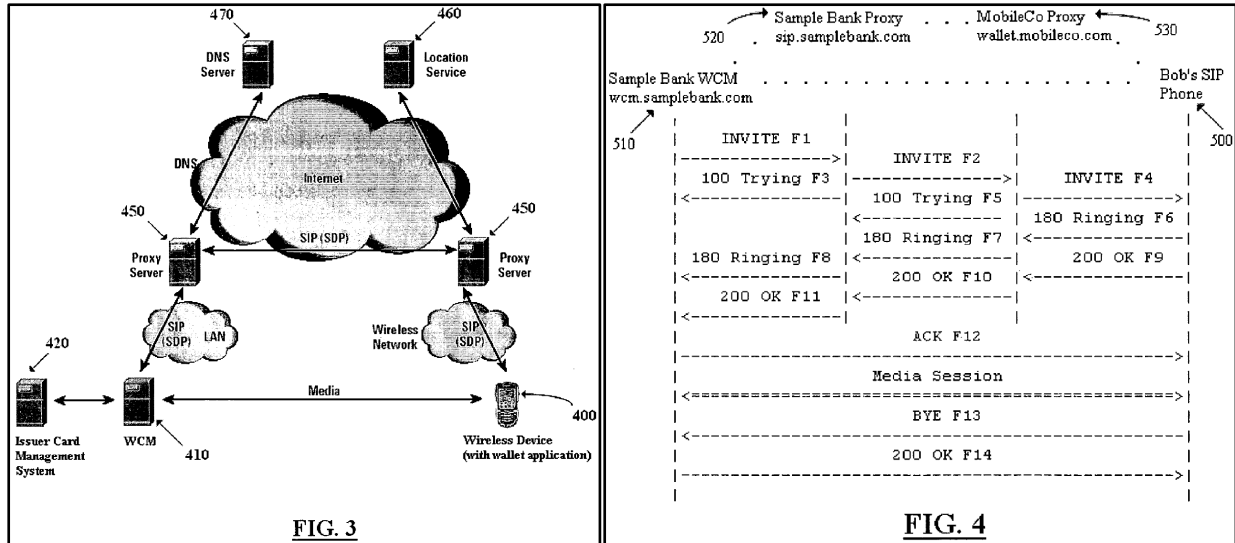
Due further teaches that PIN codes can be replaced with fingerprints (*parameter*) scanned by the "wireless device's embedded biometric technologies," which involves biometric sensors (*sensing... by at least one sensor of the smartphone*). Dua ¶¶[0366], [0414]. Dua also contemplates other biometric 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 also disclosed by Dua, determining if the scanned biometric data can decrypt the wallet application's data. Both entail "*determining that the at least one*

parameter that is sensed satisfies a criterion.” Dua ¶¶[0050], [0366], [0399], [0429]; EX1002 ¶¶222-223.

Further confirming this limitation is met, Patent Owner alleges in its infringement contentions in the district court litigation that the use of biometric verification is itself sufficient to show claimed *sensing* and *determining*. EX1016 at 29-42.

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].

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 (*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.” 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 connection with limitations 1[b] and 1[c], this process entails “*requesting an authorization to establish [a] capability*” to perform financial transactions. EX1002 ¶¶224-226.

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) a PIN code or fingerprint as part of opening the wallet; or (b) a reader key transmitted by a point-of-sale reader. Dua ¶¶[0353]-[0354], [0366], [0429]; *see also* 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* and *determining*. EX1002 ¶228.

Dua also discloses that a “reader key” (*parameter*) “is transmitted from [a point-of-sale] reader to the wireless device.” Dua ¶[0353]. When the wireless device is sufficiently close to the reader, the wireless device can detect the reader key (*sensing... by at least one sensor*). Dua ¶[0353]. When it does, the “key... received by the wallet application is used as a search string to locate a specific credential.” Dua ¶[0353]. If a reader key matches with a key registered to a credential (*determining that the... parameter... satisfies a criterion*), the wallet application automatically selects that credential for retrieval from external storage. Dua ¶[0353]-[0354]. Dua thus discloses the claimed *sensing* and *determining*. EX1002 ¶229.

Retrieving the credential from external storage (*performing [the] first [establishing] step*) 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]; *see also* EX1002 ¶¶230. As explained below in connection with limitations 1[b] and 1[c], this process

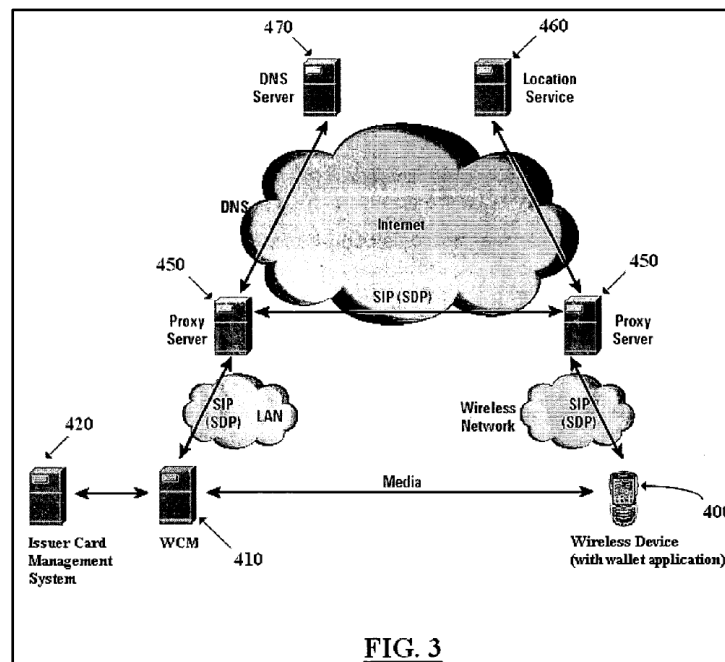
entails “*requesting an authorization to establish [a] capability*” to perform financial transactions.

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

Finally, with the claimed *determining* and *enabling* complete, claim 1 recites the specific steps for *establishing a capability* to engage in *financial transactions: requesting* and *receiving* authorization. Dua discloses these steps under either the **Card-Issuing Theory** or the **External-Storage-Authentication Theory**.

Card-Issuing Theory: As discussed with limitations 1[a][i] and 1[a][ii], the *mode to communicate* between the wireless device and wireless credential manager for user authentication that is *enabled* is SIP communications. Dua ¶¶[0046], [0104], [0128], [0178]. *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 wireless credential manager (*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]. Because the exchange results in the issuance of a credit card, the transmission of the PIN code (*first data*) requests *authorization to establish said capability to perform said at least one financial transaction*, and the credentials (*second data*) are an authorization to perform financial transactions (*authorization*), and enable the

wireless device to execute those transactions (*establish[ing] said capability*).

EX1002 ¶¶232-235, 240.

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]. *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 the storage area (*first device*). Dua ¶[0492], ¶[0495]. The wireless device then receives “credential information” (*second data*) that is “temporarily made available for use by the wireless device[.]” Dua ¶¶[0491]-[0492], [0495]. Because the exchange results in the receipt of credential information, the transmission of the username/password (*first data*) requests *authorization to establish said capability to perform said at least one financial transaction*, and the credentials (*second data*) are an authorization to perform financial transactions (*authorization*). EX1002 ¶¶236-240, 242-243.

Further confirming this limitation is met, Patent Owner alleges in its infringement contentions in the district court litigation that similar requesting and receiving of a credit card information meets the *transmitting* and *receiving* limitations. EX1016 at 23-28; EX1002 ¶241.

- (vi) **1[d][i]: *then performing the second step of said two-step process comprising performing a first transaction of said at least one financial transaction,***
- (vii) **1[d][ii]: *responsive to detecting by the smartphone that a proximity condition is satisfied and***

After receiving/retrieving credentials under either the **Card-Issuing Theory** of the **External-Storage-Authentication Theory**, Dua discloses that the wireless device makes proximity transactions with point-of-sale readers (*second step... comprising performing a first transaction*). “Credentials... may [be] use[d] [by] the handheld device to conduct... [a] transaction... via... a short range wireless link with a point-of-sale terminal.” Dua Abstract; *see also* EX1002 ¶¶244-245.

Because the short range wireless link between the wireless device and point-of-sale reader includes NFC, the transaction occurs only if (*responsive to*) the wireless device is in “close proximity” to the point-of-sale reader and can thus detect its NFC communications, including the “reader key” (*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 ¶246. Signal strength attenuates with increasing distance. EX1002 ¶¶246-247. Thus, when Dua is able to communicate with the POS terminal using NFC, the wireless device has *detected that a proximity*

condition is satisfied (e.g., Dua at Abstract, ¶¶[0041], [0314]-[0315], [0382], [0395]) by receiving and decoding a short-range NFC signal from the POS device.

Further confirming this limitation is met, Patent Owner alleges in its infringement contentions in district court litigation that the use of NFC is itself sufficient to show the claimed *detecting*. EX1016 at 29-42; EX1002 ¶¶248.

In addition, it would be obvious to a POSITA that Dua's wireless device would detect proximity to the POS terminal based on a signal from the POS terminal. 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. 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. Dua Abstract, ¶¶[0016], [0041], [0314]-[0315], [0382], [0395]. To ensure communications will be successful and not just wasted signals and wasted user time, Dua's wireless device first needs to detect it is near the POS prior to proceeding with a payment transaction with the POS device. In addition, transmitting sensitive financial information when there is no bona fide POS in proximity poses a security risk. As such, it would have been obvious for a POSITA to configure the smartphone to first detect that it is proximate to Dua's POS device

prior to attempting short-range signal communication to prevent the error conditions or fraud. EX1002 ¶¶249-251. Indeed, such implementations were well-known to a POSITA. For example, EX1020 discloses and leverages NFC to limit the range at which communication may take place. EX1020 ¶¶[0041], [0063]. Indeed, in the context of Wi-Fi, EX1020 even more explicitly discloses using the ability to receive such signals as an indication of proximity. Dua ¶[0073].

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

According to Patent Owner, limitation 1[d][iii] does not impose any new requirement relative to limitation 1[a][i]: the same sensing of *the* at least parameter and determining it meets *the* criterion as a prerequisite to *enabling* a capability in the claimed *first step* is also a prerequisite to then *using* that capability in the claimed *second step*. Compare Ex1016 at 8-14 with Ex1016 at 29-42 (pointing to the same “fingerprint unlock,” “facial recognition,” “iris authentication,” and similar security functionality and associated evidence for both limitations); *see also* EX1002 ¶¶256.

Even if the claims require an additional transaction-specific *sensing* and *determining*, Dua discloses this limitation.

First, Dua discloses individual transactions, same as receiving or retrieving credentials, requires 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* and *determining* via PIN entry or fingerprint scanning for the reasons discussed above in connection with limitation 1[a][i]. *See also* EX1002 ¶¶252-255.

Second, sensing a “reader key” is for a specific transaction, thereby occurring immediately prior to the transaction. Accordingly, the *sensing* and *determining* based on Dua’s “reader key” discussed above in connection with limitation 1[a][i] also meets the requirements of limitation 1[d][iii].

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

Limitation 1[e][i] for the most part just repeats the *detecting* of limitation 1[d][ii] and only further specifies that this is done “*relative to an access point maintained by a vendor at a point of purchase counter*” and by detecting “*a short-range signal that is transmitted by the access point.*” Even those requirements, however, are addressed above in connection with limitation 1[d][ii], since Dua’s “RFID reader[.]” (*access point*) is “installed at POS terminals in [the grocery chain’s] stores” (*maintained by a vendor at a point of purchase counter*). Dua Abstract, ¶¶[0016], [0041], [0314]-[0315]; *see also* EX1002 ¶¶257-259.

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

Limitation 1[e][ii] just repeats the *sensing* of limitation 1[d][iii] and is disclosed for the same reasons.

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

Limitation 1[e][iii] for the most part just repeats the *detecting* of limitation 1[d][ii] and the *sensing* of limitation 1[d][iii] and is disclosed for the same reasons.

The only additional requirement of limitation 1[e][iii] is *paying for a product by selectively sending information to at least one device*. Dua further discloses, after satisfaction of all the requirements discussed above, that the wireless device sends credentials (*selectively sending information*) to the point-of-sale terminal (*to at least one device*) to execute the financial transaction. Dua Abstract.³ The executed transaction results in paying for a product, such as groceries or train ticket (*paying for a product*). Dua ¶¶[0352]-[0353]; *see also* EX1002 ¶¶257-259.

³ According to Patent Owner's infringement contentions, the claimed *access point* and claimed *at least one device* can be one and the same device. EX1016 at 43, 53, 57 (pointing to "the point-of-sale device" or "terminal" for both limitations).

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

The only additional requirement of limitation 1[f] is that the “information” of limitation 1[e][iii] be sent *using unlicensed frequencies*. Dua meets this requirement by transmitting credentials using NFC and Bluetooth (*using unlicensed frequencies*). Dua Abstract, ¶¶[0016], [0318]; EX1002 ¶¶260-261.

NFC uses unlicensed frequencies, such as the 13.56 MHz ISM band. EX1002 ¶262; EX1031; EX1032 at 2. Patent Owner, in its infringement contentions, admits as much, alleging that “the wireless short-range communications link used by NFC is based upon the unlicensed 13.56 MHz frequency.” EX1016 at 53, 57; EX1002 ¶263. Bluetooth also uses unlicensed frequencies. EX1002 ¶263; EX1027; EX1002 ¶264.

- (xi) 1[g]: *wherein said at least one parameter comprises a signal, a number, a word, a code, a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state.*

As discussed with limitations 1[a][i] and 1[d][ii], Dua discloses or renders obvious a PIN code (*a number, a word, [or] a code*), fingerprint (*a physiological state*), and/or reader key (*a signal*). EX1002 ¶265.

(b) **Claim 2**

(i) **2[pre]**

Claim 1, *supra*.

(ii) **2[a]**

Limitation 2[a] requires that, when the *first function* of claim 1 is enabled responsive to the claimed *sensing* and *determining* of limitation 1[a][i], a *second function* is *disabl[ed]*. Dua discloses this limitation under both the **Card-Issuing Theory** and the **External-Storage-Authentication Theory**.

Card-Issuing Theory: Patent Owner contends that the “*enabling a first function*” and “*disabling a second function of the smartphone*” limitations are met by “unlocking the Samsung smartphone or application” and “locking the Samsung smartphone or application.” EX1016 at 64-65. The same disclosure is also found in Dua. The “default security setting in the wallet application is that PIN-entry is required before the wallet application can be ‘opened.’” Dua ¶¶[0366], [0429]. And the “wireless device... could use a fingerprint in lieu of a PIN code...” Dua ¶[0366]. Once the PIN or fingerprint is received and the wallet is opened, the PIN-entry or fingerprint-scanning function for opening the wallet is disabled. EX1002 ¶¶268-269.

External-Storage-Authentication Theory: As discussed with limitations 1[a][i] and 1[a][ii], Dua’s wireless device can receive through its wireless communication capabilities (*sensed by... [a] sensor of the smartphone*) a reader key (*parameter*). Dua ¶[0353]. “[A] key... received by the wallet application is used

as a search string to locate a specific credential.” Dua ¶[0353]. If a reader key matches with a key registered to a credential (*determined that the... parameter... satisfies the criterion*), the wallet application automatically selects the credential to transmit for a financial transaction. Dua ¶[0353]-[0354]; *see also* EX1002 ¶270.

As discussed with limitations 1[a][i] and 1[a][ii], because credentials can be stored in the external wallet storage service (Dua ¶[0491]), receiving a registered reader key (*parameter having been sensed... and... having determined that the... parameter... satisfies the criterion*) requires (is *responsive* to) retrieving the credentials from the external storage prior. Dua ¶¶[0492], [0494]. To retrieve the credential, 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]. The “real-time connection” includes “encrypt[ion] [for] all messages between the wallet application and the storage service,” where “[n]ew communication keys can be dynamically generated for each communication session” (*mode to communicate*). Dua ¶¶[0493], [0495]; *see also* EX1002 ¶271.

Further, receiving a reader key registered with a credential can also cause the process of retrieving and transmitting to be PIN-less, thereby disabling the PIN-entry function for opening the wallet (*while disabling a second function of the smartphone*). Dua ¶¶[0353]-[0355], [0384], [0392]; *see also* EX1002 ¶272.

(iii) 2[b]

Limitation 2[b] mirrors the requirements of limitations 1[a][ii], 1[b], and 1[d], but adds that the *communicating* and *requesting* are done *selectively* and further requires *selectively establishing a master-slave relationship with the first device*.

Regarding *selectively communicating* and *requesting*, those steps are only performed in Dua if the *sensing* and *determining* requirements of limitation 1[a][i] are met. Thus, the *communicating* and *requesting* in Dua is done *selectively*.

Additionally, Dua discloses *selectively establishing a master-slave relationship with the first device* under both the **Card-Issuing Theory** and the **External-Storage-Authentication Theory**.

Card-Issuing Theory: As discussed with limitation 2[a], Dua discloses that, after finding a matching PIN/fingerprint (*then*), the wireless device launches and prompts the user for an issuer PIN to transmit to the WCM for credential issuance (*selectively communicating with the first device*). Dua ¶[0180]. Because communication is through the unlocked wallet application, Dua ¶[0180], the “*communicat[ion]... us[es] [the] communications capability of the first function*.” EX1002 ¶274.

Part of this established connection, the wireless device “*establish[es] a master-slave relationship*” between the WCM (*with the first device*) and the wireless device. Dua discloses the same relationship found in the ’172 patent (’172 patent at 5:57-63) because the wireless device is responsive to the WCM validating

the issuer PIN sent by the wallet application, and the WCM issuing the credential to wallet application. Dua ¶[0180]; *see also* EX1002 ¶275.

External-Storage-Authentication Theory: As discussed with limitation 2[a], Dua discloses that, after finding a registered reader key (*then*), the wireless device automatically launches and selects a credential for transmission, thereby requiring requests to the external storage (*selectively communicating with the first device*). Dua ¶¶[0353], [0355], [0384], [0392], [0491]. To retrieve the credential, Dua sets up “real-time connection is initiated between the wallet application and the storage service” by “utiliz[ing] SIP,” which includes “encrypt[ion] [for] all messages between the wallet application and the storage service,” and “[n]ew communication keys... dynamically generated for each communication session” (*using a communications capability of the first function*). Dua ¶¶[0493]-[0495]; *see also* EX1002 ¶276.

In the established connection, the wireless device “automatically authenticates itself” by providing a “username/password” established with the storage server. Dua ¶¶[0492], [0495]. Dua thereby discloses the same “*master-slave relationship*” relationship found in the ’172 patent (’172 patent at 5:57-63) because the wireless device is responsive to the external storage authenticating the wallet application and sending back the requested credentials. EX1002 ¶¶277-278.

The request to the external wallet storage service for a specific credential (*selectively requesting from the first device*) is a “request[]... [for] the authorization to establish the capability to conduct... [a] financial transaction.” This is because the request results in “credential information [being] securely transmitted to the wireless device and temporarily made available for use by the wireless device[].” Dua ¶[0495]. EX1002 ¶279.

(c) **Claim 3**

(i) **3[pre]**

Claim 2, *supra*.

(ii) **3[a]-[c]**

Limitation 3[a] requires performing limitation 1[a][i] *repeatedly* and based on the result of the claimed *sensing* and *determining* whether to maintain the *first function* and keep the *second function disabled*. Dua discloses this limitation under both the **Card-Issuing Theory** and the **External-Storage-Authentication Theory**.

Card-Issuing Theory: As discussed with limitation 2[a], Dua discloses “*enabling a first function*” and “*disabling a second function of the smartphone*” by PIN/fingerprint entry to enable the unlocked wallet application and disable the locked function on the wallet application, similar to Patent Owner’s infringement read. EX1016 at 86. Further, “*repeatedly sensing*” a PIN/fingerprint entry and “*repeatedly deciding... whether... to maintain enabled*” the unlocked wallet application “*while maintaining disabled*” the lock function on the wallet application

is rendered obvious to a POSITA by Dua. Dua discloses security risks regarding the wireless device being lost, stolen, or otherwise ending up in possession of someone other than the rightful owner. Dua ¶[0451]. If the device were lost or taken while sensitive functionality, including transaction related functionality, was enabled, then the device could be misused. For example, enabled functionality might remain enabled so long as someone (anyone) continued to use the device before it could enter sleep mode. If, however, the device repeatedly prompted the user to re-authenticate in order to maintain the enabled functionality, that risk is reduced. EX1002 ¶¶282-283.

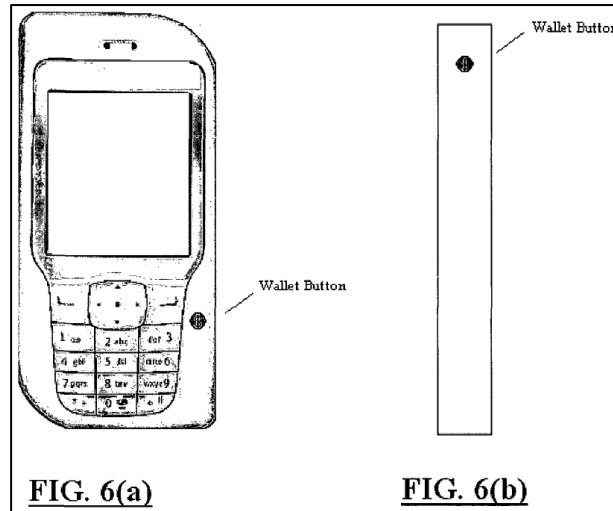
External-Storage-Authentication Theory: As discussed with limitations 2[a] and 2[b], Dua's wireless device has to repeatedly check for a reader key (*repeatedly sensing the... parameter*). A wireless device can receive a reader key from a point-of-sale reader at any time, (*see, e.g.*, Dua ¶[0380]) and can concurrently "receiv[e] and process[] multiple incoming reader keys" (Dua ¶[0364]). EX1002 ¶284.

Every time a reader "key... [is] received by the wallet application," the reader key "is used as a search string to locate a specific credential" (*repeatedly deciding, based on comparing a value of the at least one parameter sensed to the criterion*). Dua ¶[0353]. Similarly, the wireless device determines when the reader key can no longer be detected (*repeatedly deciding, based on comparing a value of the at least*

one parameter sensed to the criterion). A reader key cannot be detected when the wireless device is not nearby the point-of-sale reader because the point-of-sale reader wirelessly broadcasts the reader key to the wireless device. Dua ¶¶[0353]-[0354], [0370]. And communication between the reader and the wireless device is through a “short range wireless link,” such as NFC. Dua Abstract, ¶¶[0016], [0318]; *see also* EX1002 ¶¶285-286.

It is obvious to a POSITA to cause the wireless device to (1) cut the real-time, encrypted connection with the external storage and delete any retrieved credentials (*disabling [the] first function*) and (2) re-enable PIN entry to launch the wallet application, access the credentials, and/or use credentials (*enabling [the] second function*), when the registered reader key is no longer detected (*responsive to deciding that the value of the... parameter no longer satisfies the criterion*) and “repeatedly deciding, based on comparing a... parameter... the criterion, whether or not to maintain enabled said first function while maintaining disabled said second function).

Dua already discloses this functionality with a wallet button. Examples of wallet buttons are shown in Figures 6(a) and 6(b):



Like the reader key, the wallet button opens the wallet application and transmits credentials. *Dua* ¶¶[0383]-[0384], [0395], [0399], [0402], [0416]. When the wireless device no longer detects a pressed wallet button, RF communications for transmitting credentials during a transaction are disabled. *Dua* ¶[0386]. Because credentials retrieved from the external wallet storage service are only held temporarily for a transaction, the retrieved credentials are deleted from the wireless device. *Dua* ¶[0495]. Further, “disabl[ing] RF communications” causes the wallet “application [to] shutdown or go into its normal dormant state.” *Dua* ¶[0383]. A POSITA would understand that this will cut off a real-time connection between the wallet application and external storage. EX1002 ¶¶287-288.

A POSITA would be motivated to apply this system with reader keys in order to reduce the risk of inadvertent credential transmission. Inadvertent credential transmission is a problem contemplated by *Dua*. *Dua* ¶[0383]. When the wireless device no longer detects a registered reader key, RF communications to transmit a

credential can be disabled. Because credentials retrieved from the external wallet storage service are only held temporarily for a transaction (Dua ¶[0495]), the retrieved credentials can be deleted from the wireless device. Disabling RF communications causes the wallet application to shut down or transition into its normal dormant state. This re-enables PIN-entry because the “default security setting in the wallet application is that PIN-entry is required before the wallet application can be ‘opened’ and any credentials transmitted to an external device.” Dua ¶[0366]; *see also* EX1002 ¶289.

(d) Claim 4

(i) 4[pre]

Claim 1, *supra*.

(ii) 4[a]

Limitation 4[a] does not add any requirements relative to limitations 1[a] and 1[b] and is thus met for the same reasons. EX1002 ¶¶291.

(iii) 4[b]

Limitation 4[b] repeats the requirements of limitations 1[a]-[c] and is thus met for the same reasons. EX1002 ¶¶292-293.

(e) Claim 5

(i) 5[pre]

Claim 1, *supra*.

(ii) 5[a]

Limitation 5[a] repeats the requirements of limitation 1[e][iii] but further requires *causing data to be received selectively from at least one device*. Dua discloses this requirement by transmitting a credential to a point-of-sale reader (*data to be transmitted selectively to at least one device*) during a transaction (*responsive to performing a financial transaction*). Dua Abstract, ¶¶[0015]-[0016], [0041], [0293], [0314]-[0315], [0365]; EX1002 ¶296.

Alternatively, the wireless device transmits multiple credentials to a point-of-sale reader, (*see, e.g.,* Dua ¶[0359].) where each credential is a separate financial transaction. Because credentials are sent sequentially (*data to be transmitted selectively to at least one device*), the credentials sent after the first transmitted credential are therefore “*responsive to performing a financial transaction.*” EX1002 ¶297.

Alternatively, Dua discloses that the wireless device transmits messages to close out the communication channel between it and the POS reader “*responsive to performing a financial transaction.*” A wireless device sets up a “peer-to-peer communication session... through Near Field Communication.” Dua Abstract, ¶[0016], Claim 38. This peer-to-peer communication is based on the “Transmission Control Protocol (TCP).” Dua ¶¶[0101], [0205], [0279], [0311], [0488]; EX1002 ¶¶298-300; *see also* EX1040 at 1. After a transaction is complete, the wireless device

sends a “BYE” message to close the communication channel. Dua ¶[0182], FIG. 4; EX1002 ¶301-03; *see also* EX1040 at 5, 12.

The point-of-sale reader can transmit to a wireless device an indication of a “successful transmission of credentials to [the] reader” (*data to be received selectively from at least one device*) after a transaction is complete (*responsive to performing a financial transaction*). Dua ¶¶[0015], [0041], [0293], [0364]-[0365]; *see also* EX1002 ¶304.

(f) **Claim 6**

(i) **6[pre]**

Claim 1, *supra*.

(ii) **6[a]**

Limitation 6[a] lists specific protocols that need to be used for the *transmitting* and *receiving* of limitations 1[b] and 1[c], respectively. In Dua, transmission and reception of data can occur across a number of wireless communication channels and protocols, including Wi-Fi (which uses *unlicensed frequencies* and *a WiFi air interface protocol*). Dua ¶¶[0016], [0041], [0494], FIGS. 3, 8. And if Wi-Fi does not use *unlicensed frequencies*, then it uses *licensed frequencies*, as also claimed. Either way, this claim limitation is disclosed. EX1002 ¶¶307-308.

(g) **Claim 7**

(i) **7[pre]**

Claim 1, *supra*.

(ii) 7[a]

Dua discloses paying for a product, such as groceries and train tickets (*paying for a product*), as discussed with limitation 1[f]. Dua Abstract, ¶[0352]. The money to pay for the product could come out of any number of accounts, such as an account linked to a debit card (*deducting/withdrawing an amount of money from an account*). Dua ¶¶[0290], [0336], Claim 44; EX1002 ¶¶310-311.

(h) Claim 8

(i) 8[pre]

Claim 7, *supra*.

(ii) 8[a]

Dua teaches sending of limitation 1[f] is done via NFC or Bluetooth. Dua Abstract, ¶¶[0016], [0318]. According to Patent Owner, “NFC communications”—which includes the NFC communications disclosed in Dua—use “*unlicensed frequencies... in a Time Division Duplex operation.*” EX1016 at 142 (emphasis added); EX1032 at 21 (describing NFC as a “half... duplex system”). Bluetooth—a half-duplex system (EX1038 at 1.)—also used *unlicensed frequencies in a Time Division Duplex operations* for bidirectional communication such as the transactional communications at issue. EX1002 ¶¶313-315; *see also* EX1032 at 21.

(iii) 8[b] & 8[c]

Limitations 8[b] and 8[c] consist of two alternative limitations. Only one needs to be satisfied.

Limitation 8[b] mirrors limitation 1[e] but further requires that the *selectively sending* is to *the access point* of claim 1 and further requires *selecting sending information ... to at least one other device that is predetermined*. Dua discloses the wireless device sending credentials to a point-of-sale reader (*access point*), which is then forwarded to the issuer system (*at least one other device that is predetermined*). Dua Abstract, ¶¶[0009], [0015], [0041], [0293], [0365], Fig. 8; EX1002 ¶¶316-318.

Limitation 8[c] mirrors limitation 1[e] but further requires *selectively receiving information from the access point* of claim 1 and *selecting receiving information ... from at least one other device that is predetermined*. Dua also discloses the wireless device receiving digital receipts of the transaction from a merchant's wireless credential manager (*selectively receiving information... from at least one other device that is predetermined*). Specifically, 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]; EX1002 ¶¶316-318.

(i) Claims 9-16

Claims 9-16 are substantively identical to claims 1-8.

C. Secondary Considerations

Any secondary considerations further weigh in favor of obviousness, and certainly do not overcome the strong showing of obviousness. First, Patent Owner has not practiced the claimed invention—at any point in time—evidencing a lack of commercial success for any product practicing the '172 patent. EX1002 ¶321. Additionally, there was no long felt, unresolved need met by the '172 patent: to the extent wide-scale deployment of contactless payments with mobile devices was delayed in the United States, it was because of industry and market barriers, not technical barriers. EX1002 ¶322-323. Further, the vast number of contactless payment systems and trials of those systems before the '172 patent's priority date indicates that many within the market observed the desirability of such systems and were concurrently working towards implementing them. Section IV.A-B.

IX. NO BASIS FOR DISCRETIONARY DENIAL

A. 35 U.S.C. § 325(d) Supports Institution

The Board should not exercise its discretion under § 325(d). Jain (Ground 1) was not considered by the office during prosecution of this or any related application. That alone warrants not exercising discretion under § 325(d).

Even if the *Becton* factors are analyzed just in relation to Dua (Ground 2), they weigh against discretionary denial. Dua was cited during prosecution of the '172 patent, but was only relied upon for rejections in the prosecution of related patents (the '015 and '432 patents) that contain substantially different limitations.

Becton factors (a) and (b): The '015 patent claims required “detecting by a sensor that a product for purchase has been placed in or on the carrying structure,” which is not found in the '172 patent claims. EX1008 at 207, 208. The '432 patent claims required “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,” whereas the '172 patent’s claims do not contain this limitation or similar language. EX1009 at 171. ***Becton factors (c) and (d):*** Applicant argued, and the examiner agreed, that Dua’s paragraphs [0026], [0089], and [0495] do not “teach or suggest ‘enabling a mode to communicate... responsive to at least one physiological parameter.” EX1009 at 253, 275-276. But, in portions of Dua that were seemingly overlooked by the examiner, Dua ***does*** disclose “biometric technologies” including using a “fingerprint in lieu of a PIN code to authenticate a user to the wallet application.” Dua at 39:9-13, 45:55-58, 45:58-61. ***Becton factors (e) and (f):*** 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 above-cited disclosures of “biometric technologies,” which were seemingly overlooked by prior examiners. Thus, Ground 2 based on Dua does not warrant discretionary denial.

B. *Fintiv* Supports Institution

The six-factor *Fintiv* analysis weighs in favor of the Board declining to exercise discretionary denial. In addition to the strong merits presented herein, Petitioner also 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 patent 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.

In addition, investment in parallel litigation has been minimal: the parties have only just served infringement and invalidity contentions, they have produced a minimal amount of documents, they have not deposed any witnesses, claim construction briefing has not begun, and opening expert reports are still months away. Further, the district court has invested no time in assessing the parties' claims and defenses. Moreover, Petitioner diligently worked to file this IPR, along with seven other petitions for the related patents-in-suit with a total of 118 claims, only about eight months after being served with the complaint—almost four months before its statutory bar date (August 23, 2025). Thus, the *Fintiv* factors weigh in favor of the Board declining to exercise its discretion to deny the petition.

X. CONCLUSION

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

Date: May 2, 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 13,999 words, which is within the word limit allowed under 37 C.F.R. § 42.24(a)(i).

Date: May 2, 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 '172 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

apederson@carlsoncaspers.com

Date: May 2, 2025

/s/ *James Glass*

James Glass (Reg. No. 46729)