

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. IPR2025-00976

U.S. Patent No. 11,924,743

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 11,924,743**

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. '743 PATENT.....	6
A. '743 Patent Specification	6
B. Prosecution History (EX1019).....	6
VI. PERSON OF ORDINARY SKILL	7
VII. CLAIM CONSTRUCTION	7
VIII. GROUNDS	8
A. Ground 1: Jain (EX1017)	8
1. Background	8
2. Analysis.....	9
B. Ground 2: Dua (EX1018).....	38
1. Background	38
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. 11,924,743 (“’743 patent”)
EX1002	Declaration of Kevin Almeroth, Ph.D.
EX1003	Exhibit Intentionally Omitted
EX1004	Curriculum Vitae 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 ’743 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/
EX1043	“IEEE 802.11a – Speeding Up Wireless Connectivity in the Home”, EETimes (February 1, 2001), https://www.eetimes.com/ieee-802-11a-speeding-up-wireless-connectivity-in-the-home/
EX1044	IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999), IEEE Computer Society, June 12, 2007
EX1045	“Getting Base Stations Ready for LTE”, EETimes (April 17, 2007), https://www.eetimes.com/getting-base-stations-ready-for-lte/
EX1046	3rd Generation Partnership Project; Technical Specification Group Radio Access Network; LTE Physical Layer – General Description (Release 8), 3rd Generation Partnership Project, March 2007

LIST OF CHALLENGED CLAIMS

Claim	Limitation
1[pre]	A method of establishing a capability at a smartphone to conduct a financial transaction; the method comprising:
1[a][i]	responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion,
1[a][ii]	selectively establishing a master-slave relationship, and
1[a][iii]	selectively requesting an authorization to establish said capability; then
1[b][i]	receiving the authorization to establish the capability, responsive to said selectively requesting an authorization, and
1[b][ii]	establishing the capability at the smartphone responsive to said receiving the authorization;
1[c]	wherein said selectively establishing a master-slave relationship, said selectively requesting an authorization and said receiving the authorization comprises wirelessly transmitting/receiving using a WiFi air interface protocol, an Orthogonal Frequency Division Multiplexing air interface protocol and/or an Orthogonal Frequency Division Multiple Access air interface protocol; and
1[d]	wherein the value of the parameter that is sensed comprises a signal, a number, a word, a code, a velocity, an acceleration, a time-of-day, a position, 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, further comprising:
2[a]	repeatedly sensing said value of the parameter and repeatedly deciding, based on comparing the value of the parameter to the criterion, whether or not to maintain enabled a first function of the smartphone while maintaining disabled a second function of the smartphone; and

Claim	Limitation
2[b]	maintaining enabled said first function while maintaining disabled said second function responsive to deciding that said value of the parameter continues to satisfy the criterion; or
2[c]	disabling said first function and enabling said second function responsive to deciding that the value of the parameter no longer satisfies the criterion.
3[pre][i]	The method of claim 1,
3[pre][ii]	wherein following said establishing the capability at the smartphone, the method further comprises:
3[a][i]	responsive to satisfying a proximity condition and
3[a][ii]	responsive to sensing the value of the parameter and determining that the value of the parameter sensed satisfies the criterion,
3[a][iii]	using the capability to conduct the financial transaction that has been established at the smartphone and conducting the financial transaction by paying for a product;
3[b][i]	wherein said paying for a product 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,
3[b][ii]	determining that the value of the parameter that is sensed satisfies the criterion and then,
3[b][iii]	responsive to having sensed that the proximity condition is satisfied relative to the access point and having determined that the value of the parameter sensed satisfies the criterion, paying for the product by selectively sending information to at least one device;
3[c]	wherein said paying for the 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
3[d]	wherein said paying for the product by selectively sending information to at least one device is further responsive to said

Claim	Limitation
	selectively requesting an authorization, said receiving the authorization and said establishing the capability at the smartphone.
4[a]	The method of claim 3, wherein said paying for a product further comprises deducting/withdrawing an amount of money from an account.
5[pre]	The method of claim 4,
5[a]	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
5[b]	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.
6[a]	The method of claim 4, wherein said using unlicensed frequencies comprises using unlicensed frequencies over a short-range link in a Time Division Duplex operation.
7[pre]	The method of claim 1,
7[a]	wherein prior to said selectively requesting an authorization the method comprises: enabling a first function of the smartphone while disabling a second function of the smartphone responsive to sensing the parameter and responsive to determining that the parameter sensed satisfies the criterion; then
7[b]	selectively communicating with a device by using a communications capability of the first function, selectively establishing the master-slave relationship with the device and selectively requesting from the device the authorization to establish the capability for conducting the financial transaction.
8[pre]	A smartphone that is configured to perform operations in order to establish a capability to conduct a financial transaction; the operations comprising:

Claim	Limitation
8[a]	responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion, selectively establishing a master-slave relationship, and selectively requesting an authorization to establish said capability; then
8[b]	receiving the authorization to establish the capability, responsive to said selectively requesting an authorization, and establishing the capability at the smartphone responsive to said receiving the authorization;
8[c]	wherein said selectively establishing a master-slave relationship, said selectively requesting an authorization and said receiving the authorization comprises wirelessly transmitting/receiving using a WiFi air interface protocol, an Orthogonal Frequency Division Multiplexing air interface protocol and/or an Orthogonal Frequency Division Multiple Access air interface protocol; and
8[d]	wherein the value of the parameter that is sensed comprises a signal, a number, a word, a code, a velocity, an acceleration, a time-of-day, a position, 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.
9[pre]	The smartphone of claim 8, wherein the operations further comprise:
9[a]	repeatedly sensing said value of the parameter and repeatedly deciding, based on comparing the value of the parameter to the criterion, whether or not to maintain enabled a first function of the smartphone while maintaining disabled a second function of the smartphone; and
9[b]	maintaining enabled said first function while maintaining disabled said second function responsive to deciding that said value of the parameter continues to satisfy the criterion; or
9[c]	disabling said first function and enabling said second function responsive to deciding that the value of the parameter no longer satisfies the criterion.
10[pre]	The smartphone of claim 8, wherein following said establishing the capability at the smartphone, the operations further comprise:

Claim	Limitation
10[a]	responsive to satisfying a proximity condition and responsive to sensing the value of the parameter and determining that the value of the parameter sensed satisfies the criterion, using the capability that has been established at the smartphone to conduct the financial transaction and conducting the financial transaction by paying for a product;
10[b]	wherein said paying for a product 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 the value of the 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 parameter sensed satisfies the criterion, paying for said product by selectively sending information to at least one device;
10[c]	wherein said selectively sending information to at least one device comprises selectively and wirelessly transmitting the information to the at least one device using unlicensed frequencies;
10[d]	wherein said paying for the 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
10[e]	wherein said paying for the product by selectively sending information to at least one device is further responsive to said selectively requesting an authorization, said receiving the authorization and said establishing the capability at the smartphone.
11[a]	The smartphone of claim 10, wherein said paying for a product further comprises deducting/withdrawing an amount of money from an account.
12[pre]	The smartphone of claim 11,
12[a]	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

Claim	Limitation
12[b]	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.
13[a]	The smartphone of claim 10, wherein said using unlicensed frequencies comprises using unlicensed frequencies over a short-range link in Time Division Duplex operation.
14[pre]	The smartphone of claim 8, wherein prior to said selectively requesting an authorization the operations comprise:
14[a]	enabling a first function of the smartphone while disabling a second function of the smartphone responsive to sensing the parameter and responsive to determining that the parameter sensed satisfies the criterion; then
14[b]	selectively communicating with a device by using a communications capability of the first function, selectively establishing the master-slave relationship with the device and selectively requesting from the device the authorization to establish the capability for conducting the financial transaction.

I. INTRODUCTION

The '743 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 '743 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 '743 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 '743 patent is in the same family as U.S. Patent Nos. 9,462,411, 9,832,708, 10,219,199, 10,674,432, 11,770,756, 11,937,172, and 12,028,793, all also asserted against Petitioner. Petitioner is concurrently filing IPR petitions against these family members.

C. Counsel and Service Information

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

LEAD COUNSEL	BACK-UP COUNSEL
James M. Glass (Reg. No. 46729) 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 94111 Tel: (415) 875-6600

D. Payment of Fees

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

E. Requirements for Inter Partes Review

Petitioner certifies that the '743 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(s)	Claims
1	§103	Jain (U.S. Pat. Appl. Pub. No. 2009/0069049)	1-14
2	§103	Dua (U.S. Pat. Appl. Pub. No. 2006/0165060)	1-14

IV. STATE OF THE ART

As the '743 patent recognizes, mobile phones communicated using a variety of wireless protocols and frequencies that were well known prior to the alleged invention in late 2008. EX1001 at 1:58-2:18. 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 it used RFID technology (*i.e.*, magnetic field induction) to allow short-range wireless communications between devices in close proximity. EX1002 ¶¶86, 141, 144. 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. Meanwhile, in the United States, mobile phone and payment companies teamed up to conduct pilot programs of their own mobile payment systems, 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. '743 PATENT

A. '743 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 1:58-2:6, 3:16-20. 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 1:37-38. It also assumes that mobile phones could act as digital wallets. EX1001 at 1:47-50. 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 (EX1019)

During prosecution, Applicant made several preliminary amendments. EX1013 at 67, 83, 106, 156. The Examiner required an election of a group of claims,

and Applicant elected the group “drawn to a method of establishing a capability at a smartphone to conduct a financial transaction.” EX1013 at 136, 150.

The Examiner rejected the pending claims 1 and 4 for double patenting “over claims 1, 6, 11, 14 of Patent No. 11,770,756.” EX1013 at 243. Applicant submitted a terminal disclaimer for the ’756 patent. EX1013 at 250.

VI. PERSON OF ORDINARY SKILL

A person of ordinary skill in the art at the time of the ’743 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 ’743 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 '743 patent. Jain discloses all limitations of the '743 patent claims, but Petitioner presents Jain as an obviousness reference in the event Patent Owner argues there are differences between Jain and the '743 patent claims.

While each limitation is addressed in the “Analysis” section below in detail, given the repetitive and nonsequential nature of the '743 patent’s claim language, below is a short, non-limiting overview of Ground 1:

'743 patent claim 1 requires “establishing a capability” to engage in a “financial transaction.” This consists of (1) determining if a parameter (*e.g.*, a signal, number, or physiological state) meets a criterion; (2) if the criterion is met, establishing a master-slave relationship; and (3) requesting and then receiving 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, establishing a master-slave relationship wherein the financial institution controls the smartphone and transaction card’s use of financial instruments in financial transactions through activation (Jain ¶¶[0028], [0075]); and (3) using the cellular communications to

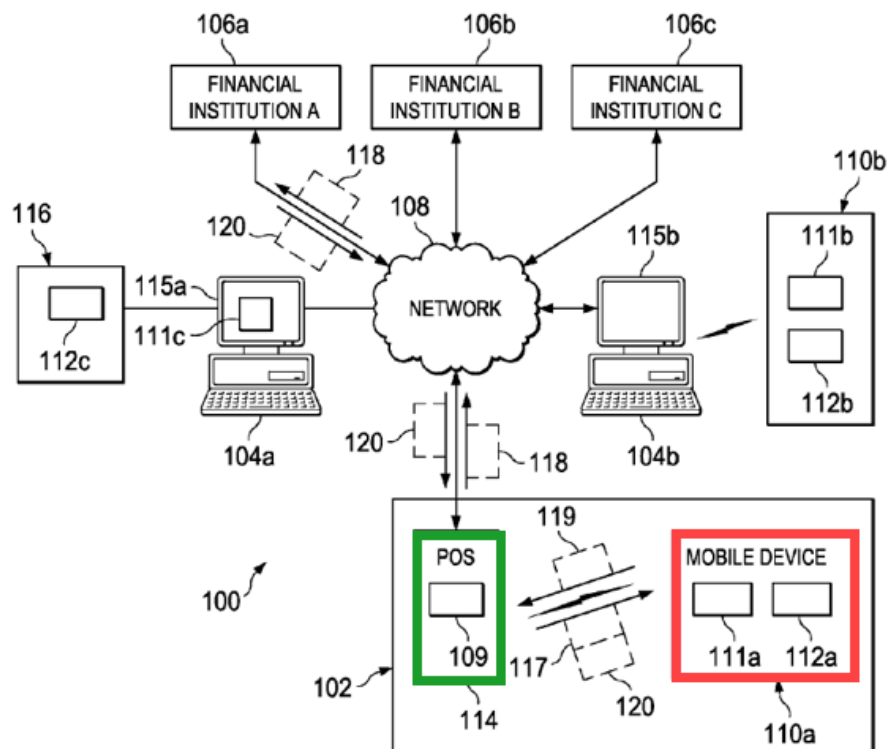
request and receive an activation code from the financial institution (e.g., Fig. 9, steps 920-926).

2. Analysis

(a) Claim 1

(i) 1[pre]: A method of establishing a capability at a smartphone to conduct a financial transaction; the method comprising:

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. 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.

Jain interfaces the mobile device 110 (e.g., "a smartphone" (¶[0018])) with a transaction card 112 that "convert[s] the mobile device 110 to a contactless payment device loaded with a financial vehicle (FV) that may be, for example, a credit card, a debit card, a gift card and/or other retail payment product" (¶[0029]). In such embodiments, transaction card 112 is included as part of the mobile device 110 (i.e., the smartphone). Jain ¶[0019] ("The offline store 102 includes a mobile device

[110a¹] having a transaction card 112a and a Point of Sale (POS) device 114 that executes transactions with customers.”), Fig. 1 (showing transaction card 112a within mobile device 110a). *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 ¶101. 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 ¶¶98-100. 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.

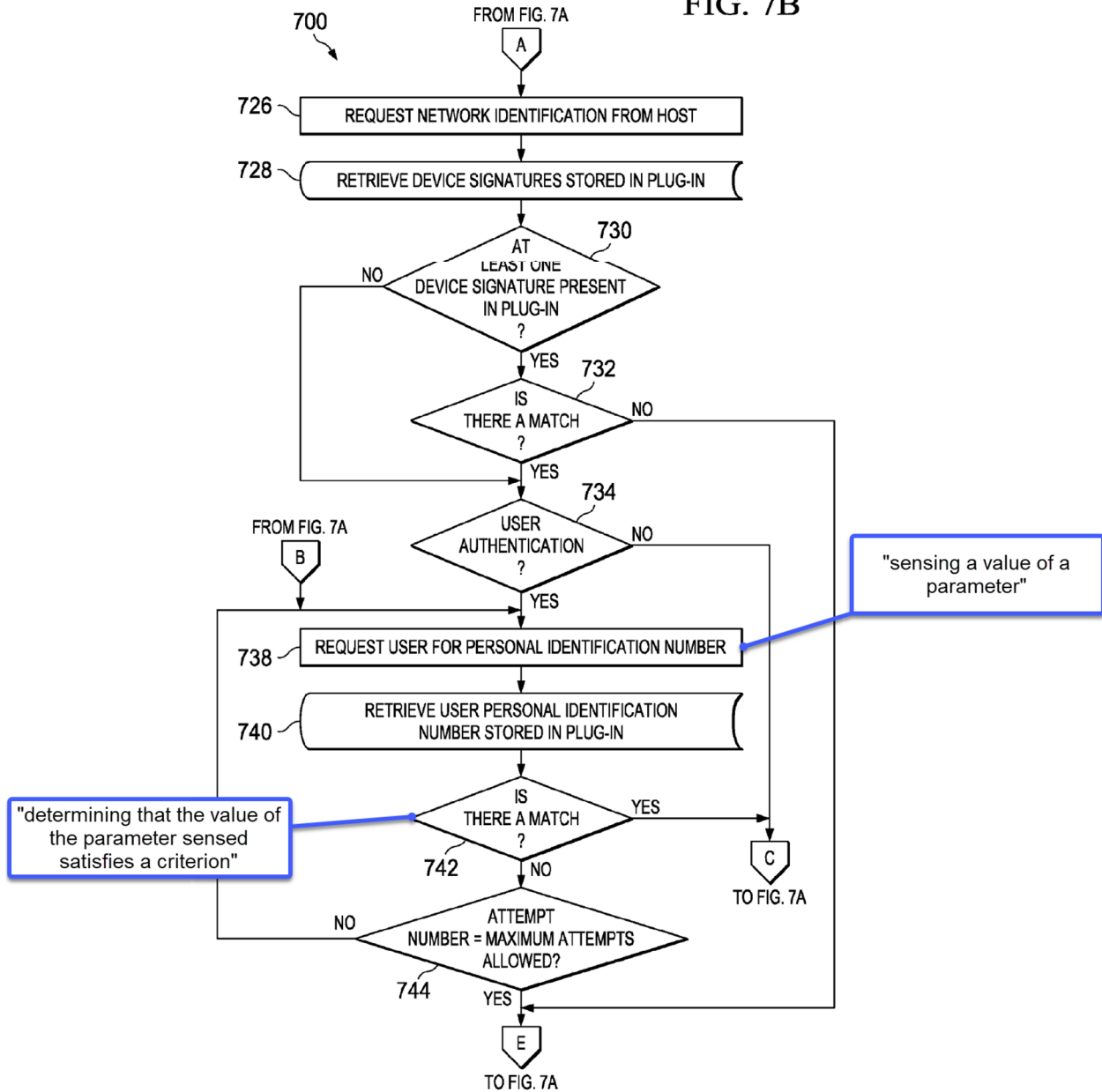
¹ The reference to “10a” in the specification is an obvious typographic error. No figures show a “10a” and Jain’s Figure 1 clearly shows element 110a that matches the description of “10a” in the specification.

Prior to conducting financial transactions, 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 at a smartphone to conduct a financial transaction*. By completing these steps, Jain’s mobile device with the transaction card can thereafter conduct financial transactions with a Point of Sale (“POS”) device. Jain, Abstract, ¶¶[0019], [0023], [0027]-[0029]; *see also* EX1002 ¶¶95-105.

- (ii) **1[a][i]: responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion,**

The claim begins with *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 ¶106.

FIG. 7B



At step 738, the smartphone receives a PIN (*sensing a value of a parameter*) via the mobile device's touch screen, 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 ¶107.

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 ¶¶108-109.

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 ¶110.

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 “*criterion*” 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 ¶¶111-113.

(iii) 1[a][ii]: selectively establishing a master-slave relationship,

Jain discloses *selectively establishing a master-slave relationship*. The ’743 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 ¶¶114-121. For example, the financial institution (*master*) has multiple opportunities to decide whether or not financial transactions are activated (*see* steps 906, 920 of Fig. 9), after authorization defines

the format of a transaction response sent by the mobile device 110 (*slave*), remains the final arbitrator for deciding to send an authorization response 120 approving a purchase, may request information (e.g., transaction history) from the mobile device 110 (*slave*), and can temporary prevent payments by mobile device 110 with transaction card 112 (*slave*) in response identifying potential fraudulent activity. Jain ¶¶[0027], [0032], [0046], [0057], [0081].

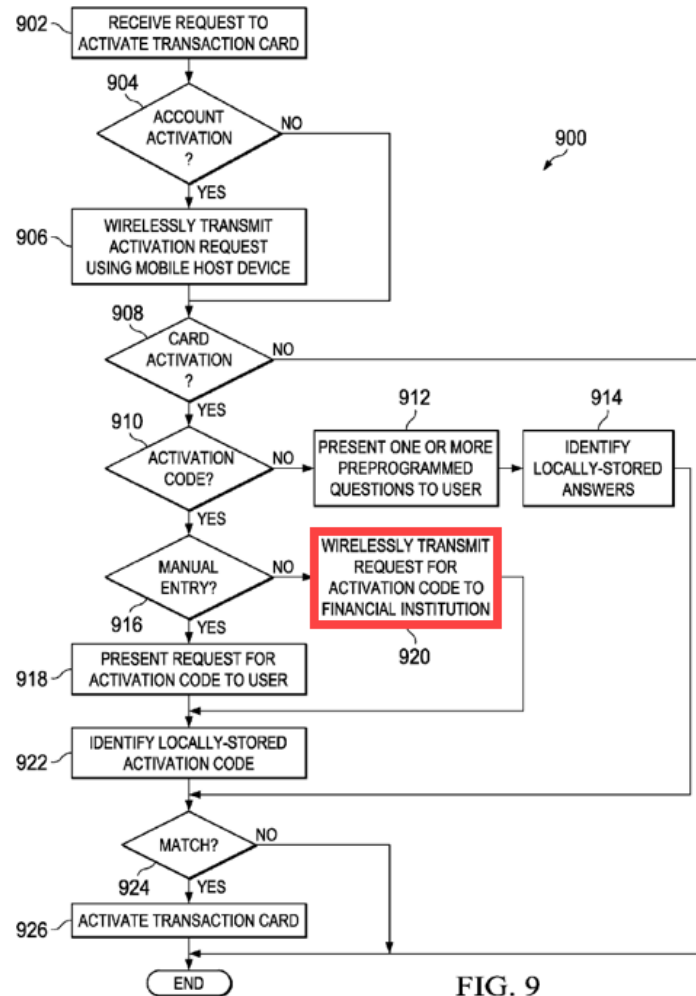
- (iv) 1[a][iii]: and selectively requesting an authorization to establish said capability; then
- (v) 1[b][i]: receiving the authorization to establish the capability, responsive to said selectively requesting an authorization, and

If the prerequisite of limitation 1[a][i] is met (*selectively*), claim 1 recites *requesting* and *receiving authorization to establish said capability* to conduct financial transactions. Jain discloses these steps.

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” (*requesting an authorization*) to the financial institution.² Jain ¶[0081],

Fig. 9 (annotated). *See also* EX1002 ¶122.



² 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].

In response to the request of step 924 (*requesting an authorization*), mobile device 110 receives an activation code (*receiving the authorization*) from the financial institution. 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 ¶¶123, 126.

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*), 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 the authorization to establish the capability*.” EX1016 at 8. *See also* EX1002 ¶¶123-127.

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 ¶122. 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 ¶¶121-127.

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 a “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 ¶128.

- (vi) **1[b][ii]: establishing the capability at the smartphone responsive to said receiving the authorization;**

[R]esponsive to said receiving the authorization as part of activating (see Jain ¶¶ [0080]-[0081], Fig. 9) a transaction card with an associated financial institution, Jain discloses *establishing the capability*. Specifically, Jain teaches that, after completing the activating process, “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. Then, 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” by wirelessly sending the POS device 114 information associated with the payment account. Jain ¶¶[0023], [0027], [0029]; *see also* EX1002 ¶128-29. Jain’s disclosure of the using the *capability* is addressed below regarding claim 3.

- (vii) **1[c]: wherein said selectively establishing a master-slave relationship, said selectively requesting an authorization and said receiving the authorization comprises wirelessly transmitting/receiving using a WiFi air interface protocol, an Orthogonal Frequency Division Multiplexing air interface protocol and/or an**

**Orthogonal Frequency Division Multiple Access
air interface protocol; and,**

Limitation 1[c] lists specific protocols that need to be used for the *establishing, requesting* and *receiving* of limitations 1[a] and 1[b]. In Jain, these steps involve communications with a financial institution using cellular radio technology. Jain ¶[0081]; *see also* EX1002 ¶[130]. The cellular radio technology in Jain includes GSM, CDMA, UMTS, and other modes. Jain ¶[0041]. A POSITA would be motivated to use the most advanced and performant cellular radio technologies such as LTE and WiMAX (a competitor to LTE) (also known as 4G cellular technologies), well-known next generation technologies for cellular communications, in addition to the cellular radio technology explicitly mentioned in Jain to keep up with ever-evolving technologies that allow for higher data rates and that even as of the priority date of the '743 patent were known to a POSITA to be in line to displace older technologies in the near future. EX1002 ¶131; *see also* EX1045, EX1046. Wi-Max and LTE both use both ***Orthogonal Frequency Division Multiplexing air interface protocol*** and ***an Orthogonal Frequency Division Multiple Access air interface protocol***. EX1002 ¶131; *see also* EX1045, EX1046.

Jain also discloses “the mobile device 110 [can] transmit packet data using its own connection to the external world (e.g., SMS, cellular, **Wi-Fi**).” Jain ¶[0053] (emphasis added); *see also* Jain at claim 13, 14. This includes using “WiFi technology” to “wirelessly interface” with financial institutions. Jain ¶[0068], Fig.

5. Accordingly, Jain discloses Wi-Fi as an alternative to “cellular” communications for implementing the *transmitting/receiving* the *requesting an authorization and... receiving the authorization* to/from a financial institution, as taught in Jain’s Fig. 9. Jain’s Wi-Fi is *a WiFi air interface protocol*. EX1002 ¶130-31; *see also* EX1043, EX1044.

(viii) 1[d]: wherein the value of the parameter that is sensed comprises a signal, a number, a word, a code, a velocity, an acceleration, a time-of-day, a position, 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 regarding 1[a][i], Jain discloses or renders obvious sensing a PIN (personal identification *number*) or fingerprint (*physiological state*). Jain ¶[0075], claim 10. EX1002 ¶¶132-34.

(b) Claim 2

(i) 2[pre]

See Claim 1, *supra*.

(ii) 2[a]

For limitation 2[a], based on the result of 1[a][i] *sensing* and *determining*, the smartphone decides whether to *maintain enabled a first function* and keep the *second function disabled*.

As discussed below regarding limitation 7[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 with **either** the capability to engage in 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 said value of the 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 is a change to the smartphone with potential security implications. EX1002 ¶¶136-137. Requiring re-authorization and re-activation under those circumstances would prevent fraud. EX1002 ¶138.

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 a second function*). EX1002 ¶138. **Second**, Jain discloses *enabl[ing] a first function* (enabling mobile device 110 to communicate with the financial institution using cellular radio technology in connection with process 900) *while maintaining disabled 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 ¶138-39; *see also* EX1002 ¶140.

(iii) 2[b]

Limitations 2[b] and 2[c] consist of two alternative limitations. Only one needs to be satisfied. Nonetheless, Jain discloses both.

As discussed regarding 2[a] above, Jain *maintain[s] enabled* the activation process (*first function*) while *maintaining disabled* the card's payment services (*second function*) based on deciding that the smartphone user is still authorized. EX1002 ¶141.

Alternatively, as discussed regarding 2[a] above, Jain *maintain[s] enabled said first function* (enabling mobile device 110 to communicate with the financial institution using cellular radio technology in connection with process 900) *while maintaining disabled said 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. EX1002 ¶142.

(iv) 2[c]

Alternatively, Jain discloses limitation 2[c] when it disables cellular communications (*disabling said first function*) with the financial institution by returning to the mode the transaction card was in before being inserted into the device (*enabling said second function*) 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 44; *see also* EX1002 ¶¶143-144.

(c) Claim 3

(i) 3[pre]

See Claim 1, *supra*.

As discussed regarding claim 1, Jain discloses “***establishing the capability at the smartphone.***” As discussed below in 3[a][iii] and 3[d] Jain discloses the method of claim 3 “***following said establishing***” of claim 1. See also EX1002 ¶146.

(ii) 3[a][i]

After 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], [0029].

To engage in such transactions, mobile device 110 detects, via its included transaction card 112, that it is proximate a payment terminal (*i.e.*, POS device 114). For example, mobile device 110 “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 mobile device 110 is only able to process the “request” if it is sufficiently close to POS device 114 to receive and decode the short-range signal corresponding to the request (***responsive to satisfying a proximity condition***). EX1002 ¶¶147-49; 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 detected such

that the device and the terminal can communicate using that protocol. EX1002 ¶¶147-49; EX1035 at 4, 36; EX1037 at 3. The signal strength correlates to proximity and rapidly deteriorates as distance increases. EX1002 ¶149; EX1035 at 4, 36; EX1037 at 3. Accordingly, receipt of a short-range NFC signal corresponds to and teaches ***satisfying a proximity condition*** between the smartphone and an entity (e.g., POS device of a retail store). *See also* EX1002 ¶148.

Moreover, Patent Owner’s infringement contentions allege that the use of NFC to conduct financial transactions with a POS terminal is *prima facie* evidence of ***satisfying a proximity condition***. EX1016 at 52-61. *See also* EX1002 ¶154.

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 conducting a payment transaction with the POS device. EX1002 ¶¶149-53. Otherwise, the NFC communication would fail. Indeed, such implementations were well-known to a POSITA. For example, EX1020 discloses leveraging NFC to limit the range at which communications occur. 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 ¶¶149-54.

(iii) 3[a][ii]

According to Patent Owner, limitation 3[a][ii] does not impose any new requirement relative to limitation 1[a][i]: the same *sensing the value of the parameter* and *determining that the value of the parameter sensed satisfies the criterion* in *establishing the capability* is also a prerequisite to then *using the capability*. 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 regarding limitation 1[a][i]. At a minimum, a POSITA would find that *sensing* a user-entered PIN and *determining* if it matches a previously-stored PIN (*criterion*) to be an

obvious implementation of PIN authorization: it does not require communication with any other devices and it reuses aspects of the software that implements the user authentication of Fig. 7. EX1002 ¶¶155-57.

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]. Reusing those elements in Jain rather than reimplementing them on POS device 114 would simplify design and development, conserve computing resources, and limit the transmission of sensitive user information (e.g. user PIN). Indeed, numerous prior art references require user authorization before permitting individual purchases. *See, e.g.*, EX1020 ¶¶[0083]-[0084], [0088], Fig. 14; EX1021 ¶[0052]; *see also* EX1002 ¶¶158-59.

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, a POSITA would 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 ¶162; 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 ¶¶160-63. In addition, as discussed regarding limitation 1[a], Jain discloses or at least renders obvious that implementing biometric authorization would entail the claimed *sensing* and *determining*.

(iv) 3[a][iii]

Jain discloses *using* the authenticated and activated transaction card (*capability to conduct the financial transaction that has been established at the smartphone*) for *conducting the financial transaction by paying for a product*. Jain Abstract, ¶¶[0019], [0023], [0027]-[0029]. As discussed below regarding 3[b][iii], Jain discloses transacting with a nearby retail payment terminal POS 114 to pay for a product—*conducting the financial transaction by paying for a product*. *See* Jain

¶¶[0019], [0023]; *see also* EX1002 ¶164. Jain’s disclosure of this limitation is addressed below in connection with limitations 3[b]-[d]. *See also* EX1002 ¶164.

(v) 3[b][i]

Limitation 3[b][i] for the most part just repeats the *satisfying* of limitation 3[a][i] and only further specifies “*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.*” Those requirements are addressed above regarding 3[a][i], 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 ¶¶165-167.

(vi) 3[b][ii]

Limitation 3[b][ii] just repeats the *sensing* and *determining* of limitation 3[a][ii] and is disclosed for the same reasons. *See also* EX1002 ¶168.

(vii) 3[b][iii]

Limitation 3[b][iii] for the most part just repeats the *detecting* of limitation 3[a][i] and the *sensing* of limitation 3[a][ii] and is disclosed for the same reasons.

The only additional requirement of limitation 3[b][iii] is *paying for the product by selectively sending information to at least one device*. Jain 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*).³ 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 3[a][i] and 3[a][ii]. *See also* EX1002 ¶¶169-70.

(viii) 3[c]

The only additional requirement of limitation 3[c] is that the “information” of limitation 3[b][iii] be sent *using unlicensed frequencies*. Jain meets this requirement by *selectively and wireless 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)” (*using unlicensed frequencies*). Jain ¶[0023]; *see also* EX1002 ¶171.

NFC used the 13.56 MHz ISM band, which comprise *unlicensed frequencies*. EX1002 ¶¶172; EX1031; EX1032 at 2. Patent Owner’s infringement contentions admit as much, alleging that “the wireless short-range communications link used by

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 62, 71, 72 (pointing to “the point-of-sale device” or “terminal” for both limitations).

NFC is based upon the unlicensed 13.56 MHz frequency.” EX1016 at 57-58; EX1002 ¶173. Bluetooth also used unlicensed frequencies. EX1002 ¶174; EX1041.

(ix) 3[d]

As discussed regarding Claim 1, Jain discloses that *paying for the product* requires (*is further responsive to*) authenticating (Jain ¶¶[0072]-[0075], Fig. 7) and activating (Jain ¶¶[0080]-[0081], Fig. 9) (*requesting ... [and] receiving*) a transaction card with an associated financial institution to *establish[] the capability at the smartphone* as discussed above regarding claim 1. EX1002 ¶175.

(d) Claim 4

(i) 4[pre]

See Claim 3, *supra*.

(ii) 4[a]

Jain discloses that when *paying for a product*, the smartphone sends transaction information corresponding to a credit, debit, or bank account. Jain ¶¶[0025], [0029], [0036]. Payments using debit 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 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 ¶¶177-78.

(e) **Claim 5**

(i) **5[pre]**

See Claim 4, *supra*.

(ii) **5[a] and [b]**

Limitation 5[a] mirrors limitation 3[b] but further requires that the *selectively sending* is to *the access point* of claim 3 and further requires *selectively sending information to...* and *selectively receiving information from... at least one other device that is predetermined*. Jain also 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 ¶¶180-82. Jain’s mobile device also receives the authorization response with the 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 ¶¶180-182.

Also, Patent Owner’s infringement contentions rely on the theory that the accused devices *send information to* and *receive information from* a “base station.”

EX1016 at 81. Jain’s smartphone also transmits data to and receives a transaction receipt from numerous intermediary devices, including network 108, GSM core network 202, RAN 204, MSC 206, Base Station Controllers 212, Base Stations 210, and/or client 115 (*one other device that is predetermined*) on the way to/from the financial institution. Jain ¶[0044]; Figs. 1-2. EX1002 ¶183.

Finally, to the extent Patent Owner argues the claimed *sending* 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], [0046].

(f) Claim 6

(i) 6[pre]

See Claim 4, *supra*.

(ii) 6[a]

Jain teaches the sending of information in limitation 3[c] 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 over a short-range link in a Time Division Duplex operation*.” EX1016 at 86 (emphasis added); EX1032 at 21 (describing NFC as a “half... duplex system”); EX1002 ¶185-86. Bluetooth also uses *unlicensed frequencies over a short-range link in a Time Division Duplex operations*. EX1002 ¶187; see also EX1038 at 1.

(g) Claim 7

(i) 7[pre]

See Claim 1, *supra*.

(ii) 7[a]

Limitation 7[a] requires that, when a *first function* in 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]-[c]. While 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 after activation process 900 in Fig. 9 is complete is the mobile device enabled for financial transaction (*second function*). EX1002 ¶¶189-91.

Second, Jain meets this limitation by *enabling a first function* (enabling mobile device 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). Patent Owner's infringement contentions argue that limitation 7[a] is met by "enabling a

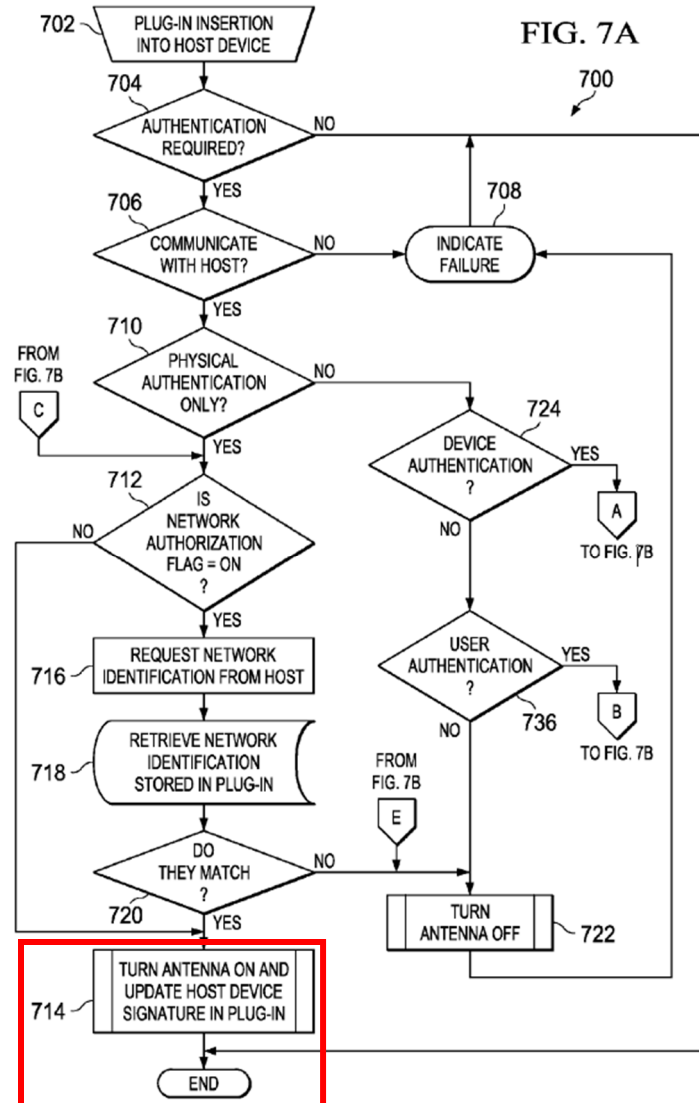
first function (unlocking the [] smartphone or application) while disabling a second function (locking the [] smartphone or application).” EX1016 at 88-89; *see also* EX1002 ¶192. Similarly, Jain’s authorization process 700 (Fig. 7) must be completed before turning on the antenna and updating the host device signature (step 714) to enable the cellular communication with the financial institution of 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 ¶¶193-94.

(iii) 7[b]

Limitation 7[b] mirrors the requirements of limitations 1[a][ii]-[iii] but adds *selectively communicating... by using a communications capability of the first function*.

Regarding *selectively communicating*, those steps are only performed in Jain if the *sensing* and *determining* requirements of limitation 1[a][i] are met. Thus, the *communicating*, *establishing*, and *requesting* in Jain are performed *selectively*. EX1002 ¶195.

For *using a communications capability*, in response to authenticating the user in steps 738-744 of Fig. 7B, Jain process 700 returns to step 712 (label C in both figures) and proceeds to step 714: “turn antenna on and update host device signature in plug-in.” Jain ¶¶[0072]-[0075], Fig. 7A (annotated). *See also* EX1002 ¶¶198-202.



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 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 (*a communications capability of the first function*). See also EX1002 ¶¶198-202. Jain’s mobile device 110 then performs “method 900 for activating a wireless transaction system” with the financial institution. Jain ¶[0080]. This activation process includes *establishing the master-slave relationship* (see claim 1[a][ii]) and *requesting from the device the authorization* (see claim 1[a][iii]).

(h) Claims 8-14

Claims 8-14 are substantively identical to claims 1-7.

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 ’743 patent. Dua discloses all limitations of the ’743 patent claims, but Petitioner presents Dua as an obviousness reference in the event Patent Owner identifies any differences between Dua’s disclosure and the ’743 patent claims.

While each limitation is addressed in the “Analysis” section below in detail, given the repetitive and nonsequential nature of the ’743 patent’s claim language, below is a short, non-limiting overview of Ground 2:

'743 patent claim 1 requires *establishing a capability* to engage in *financial transactions* and claim 3 requires *using* that *capability* for a particular *financial transaction*. Those steps are broken down in Section VIII.A.1 above. EX1002 ¶203-4.

Dua discloses the claimed *establishing a capability* 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. EX1002 ¶204-10.

2. Analysis

(a) Claim 1

(i) 1[pre]: A method of establishing a capability at a smartphone to conduct a financial transaction; the method comprising:

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 phone applications like a “wallet application.” Dua Abstract, ¶¶[0041], [0049], [0050], [0051], [0287]-[0288], FIGS. 3, 5, 6(a)-8; EX1002 ¶211. The wallet application can “conduct[] financial ... transactions” (*conduct a financial transaction*). Dua Abstract, ¶¶[0041], [0312]-[0313], [0333].

Dua discloses *establishing a capability* 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]); *see also* EX1002 ¶¶211-12.

(ii) 1[a][i]: responsive to sensing a value of a parameter and responsive to determining that

the value of the parameter sensed satisfies a criterion,

Dua discloses *sensing* and *determining* if a *criterion* is satisfied under either the **Card-Issuing Theory** or the **External-Storage-Authentication Theory**.

Card-Issuing Theory: Dua's 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 disclosures 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 store many credit cards and other confidential information. Dua ¶¶[0041], [0055], [0287]-[0288], [0334]. Regardless of how the wallet is opened, the wallet application allows the user to access the stored credentials and thus needs to be protected. Dua ¶¶[0324]-[0332], [0334], [0366], [0378]. *See also* EX1002 ¶¶213-15.

Further, a feature within a wallet/payment application to add an account or credit card is well known to a POSITA. EX1002 ¶211; 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 ¶¶216-18.

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 ¶¶216-17.

For Dua's PIN-entry, the wireless device receives a PIN code (*value of a parameter*) through a PIN entry or text field after the PIN code is typed (*sensing*) in with a keyboard or touchscreen keyboard (*e.g.*, capacitive touch screen). Dua ¶¶[0366], [0384], [0395], FIGS. 1, 3, 6(a), 8, FIG. 9; EX1042. The entered PIN code is used to decrypt data or otherwise matched against a validation PIN code stored in the wallet application, thereby validating the user's identity (*determining that the value of the parameter sensed satisfies a criterion*). Dua ¶¶[0050], [0366], [0399], [0429]; *see also* EX1002 ¶219.

Due further teaches that PIN codes can be replaced with fingerprints (*value of a parameter*) scanned by the “wireless device’s embedded biometric technologies,” which involves biometric sensors (*sensing*). 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 value of the parameter sensed satisfies a criterion*.” Dua ¶¶[0050], [0366], [0399], [0429]; EX1002 ¶¶220-21.

Further confirming this limitation is met, Patent Owner’s infringement contentions allege that the use of biometric verification is sufficient to show claimed *sensing* and *determining*. EX1016 at 7-20.

At a minimum, it would be obvious to implement Dua’s teaching of authentication using biometric information for the reasons explained above regarding Jain’s disclosure of limitation 1[a][i].

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

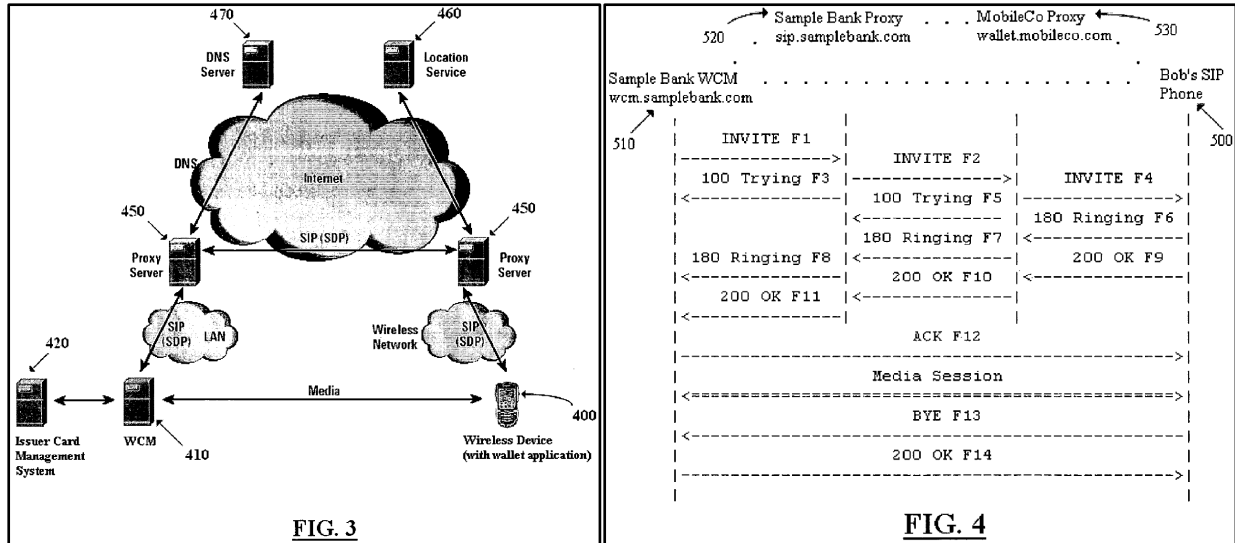
user's wallet application.” Dua ¶[0491]. Retrieval of credentials from the external storage is only possible after (*responsive to*) sensing (a) a PIN code or fingerprint as part of opening the wallet; or (b) a reader key transmitted by a point-of-sale reader. Dua ¶¶[0353]-[0354], [0366], [0429]; *see also* EX1002 ¶227. As addressed above regarding the **Card Issuing Theory**, Dua's requirement that the user enter a PIN code or 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” (*value of a 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 detects the reader key (*sensing*). Dua ¶[0353]. Then, 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 a key registered to a credential (*determining that the value of the parameter sensed 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.

- (iii) 1[a][ii]: selectively establishing a master-slave relationship,
- (iv) 1[a][iii]: and selectively requesting an authorization to establish said capability; then
- (v) 1[b][i]: receiving the authorization to establish the capability, responsive to said selectively requesting an authorization, and

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**.

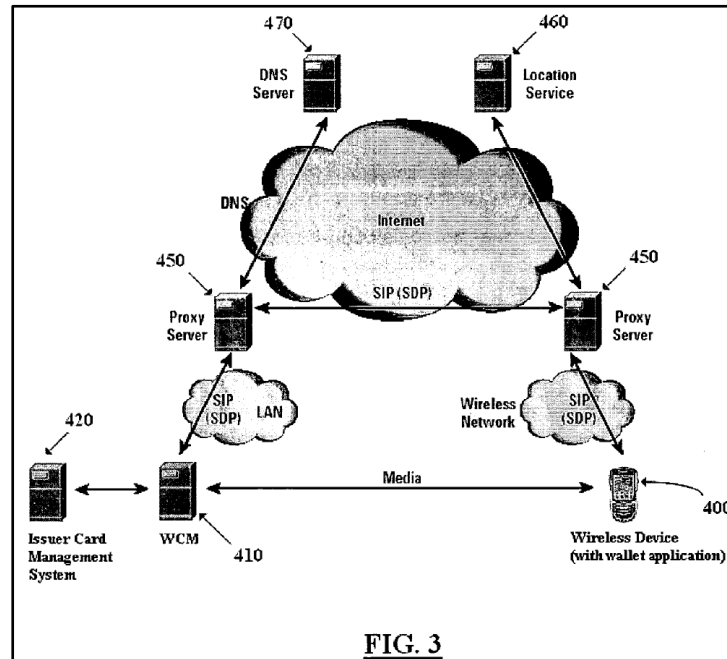
Card-Issuing Theory: After sensing the matching PIN code or fingerprint, the wallet application is opened for credential issuance. The wallet application then establishes Session Initiation Protocol (“SIP”) communication session between the wireless device and the issuer’s wireless credential manager (“WCM”). Dua ¶¶[0046], [0104], [0128], [0178]; *see also* EX1002 ¶222-23. “The... SIP architecture... establish[es] direct communication between... WCM and wallet application... for... transferring... credentials.” Dua ¶¶[0128], [0178], Figs. 3 and 4:



With this established connection, the wireless device “*establish[es] a master-slave relationship*” between the WCM and the wireless device. Dua discloses the same relationship found in the ’743 patent (’743 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 ¶224.

Through the SIP session, the “issuer’s system will authenticate the... user’s identity... to ensure that the [user]... is... the person that requested the digital credential.” Dua ¶[0180]. The “authentication process [is]... accomplished by... the issuer system prompting the user for some cardholder... information,” where the “user would see such a request for information within the wallet application.” Dua ¶[0180]. The credential-issuance request asks for a “special code or PIN that was mailed to the user in advance of the issuance.” Dua ¶[0180]. The wireless device’s

wallet application then sends the “special code or PIN” to the WCM to allow “the issuer’s system [to] validat[e] the user’s identity in real-time” (*requesting an authorization*). 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 the authorization... responsive to said selectively requesting*). Dua ¶[0180]. Because the exchange results in the issuance of a credential, the transmission of the PIN code requests *authorization to establish said capability*, and the credential (e.g., credit, debit, or bank account information) is an authorization to perform financial transactions (*authorization*), and enable the wireless device to execute those transactions (*establish[ing] said capability*). EX1002 ¶¶222-26, 234.

Similarly, Patent Owner’s infringement contentions allege that requesting and receiving of a credit card information meets the *requesting* and *receiving* limitations. EX1016 at 7-20; EX1002 ¶235.

External-Storage-Authentication Theory: Retrieving the credential from external storage requires initiating 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.” Dua ¶¶[0494]-[0495]. The wireless device authenticates itself to the external storage by transmitting a “username/password for the wallet application” (*selectively requesting an authorization*) to the storage service. Dua ¶[0492], ¶[0495]. The wireless device then receives “credential information” (*receiving the authorization... responsive to said selectively requesting*) 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 requests *authorization to establish said capability*, and the credential is an authorization to perform financial transactions (*authorization*). EX1002 ¶¶227-30, 236-38.

In the established connection, the wireless device “automatically authenticates itself” by providing a “username/password” established with the storage service. Dua ¶¶[0492], [0495]. Dua thereby discloses the same “*master-slave relationship*”

relationship found in the '743 patent ('743 patent at 5:57-63) because the wireless device (*slave*) is responsive to the external storage (*master*) authenticating the wallet application and sending back the requested credentials which controls whether the wireless is enabled for performing a financial transaction. EX1002 ¶¶231-32.

(vi) 1[b][ii]: establishing the capability at the smartphone responsive to said receiving the authorization;

Under both theories, after receiving/retrieving credentials, the wireless device may conduct proximity transactions with POS terminals using the credentials; thus receiving/retrieving the credentials *establish[es] the capability at the smartphone responsive to said receiving the authorization*. See also EX1002 ¶233. “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.

Card-Issuing Theory: Because the wireless device can use the issued credential in financial transactions, receiving the issued credential (*responsive to said receiving the authorization*) allows the wireless device (*at the smartphone*) to conduct transactions (*establishing the capability*). EX1002 ¶234-5, 238.

External-Storage-Authentication Theory: Because retrieving the credentials allows the wireless device use of that credential (*responsive to said receiving the authorization*), receiving the credential enables the wireless device (*at*

the smartphone) to perform transactions (*establishing the capability*). EX1002 ¶236-8.

- (vii) 1[c]: wherein said selectively establishing a master-slave relationship, said selectively requesting an authorization and said receiving the authorization comprises wirelessly transmitting/receiving using a WiFi air interface protocol, an Orthogonal Frequency Division Multiplexing air interface protocol and/or an Orthogonal Frequency Division Multiple Access air interface protocol; and,

Limitation 1[c] lists specific protocols for the establishing, requesting and receiving of limitations 1[a] and 1[b]. In Dua, these communication steps, involving the transmission and reception of data, use wireless communication channels and protocols, including “GSM/GPRS, CDMA2000, W-CDMA, EDGE, HDR, 1xRTT, UMTS, IMT-2000, 802.11a, 802.11b, 802.11g, or BLUETOOTH or other relevant protocols developed hereinafter.” Dua ¶[0041]. A POSITA would be motivated to use the most advanced and performant cellular radio technologies such as LTE and WiMAX (a competitor to LTE) (also known as 4G cellular technologies), well-known next generation technologies for cellular communications, in addition to the cellular technologies and protocols explicitly mentioned in Dua to keep up with ever-evolving technologies that allow for higher data rates and that even as of the priority date of the ’743 patent were known to a POSITA to be in line to displace older technologies in the near future. EX1002 ¶241, EX1045, EX1046. Wi-Max and LTE

both use both *Orthogonal Frequency Division Multiplexing air interface protocol* and *an Orthogonal Frequency Division Multiple Access air interface protocol*. EX1002 ¶241.

Dua also discloses Wi-Fi (*a WiFi air interface protocol*). Dua ¶¶[0016], [0041], [0494], FIGS. 3, 8; *see also* EX1002 ¶¶239-40. Further, Dua discloses the WiFi protocols “802.11a” and “802.11g” which use *an Orthogonal Frequency Division Multiplexing air interface protocol*. Dua ¶[0041]; EX1002 ¶241, EX1043, EX1044. Accordingly, Dua discloses Wi-Fi as an alternative to cellular communications for implementing the *transmitting/receiving the requesting an authorization and ... receiving the authorization to/from a financial institution*. Dua at [0104] (“The system disclosed herein is designed to interoperate with mobile 2.5G, 3G, and Wi-Fi networks.”).

- (viii) 1[d]: wherein the value of the parameter that is sensed comprises a signal, a number, a word, a code, a velocity, an acceleration, a time-of-day, a position, 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], 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 ¶242.

(b) **Claim 2**

(i) **2[pre]**

See Claim 1, *supra*.

(ii) **2[a], [b], and [c]**

Limitation 2[a] requires performing limitation 1[a][i] *repeatedly* and based on the result of the claimed *sensing, 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 below regarding 7[a], Dua discloses “*enabl[ing] a first function*” and “*disabl[ing] 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 36. 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 stolen with sensitive functionality (e.g. payment functions) enabled then the device could be misused. If, however, the device repeatedly prompted the user to re-

authenticate in order to maintain the enabled functionality, that risk is reduced.

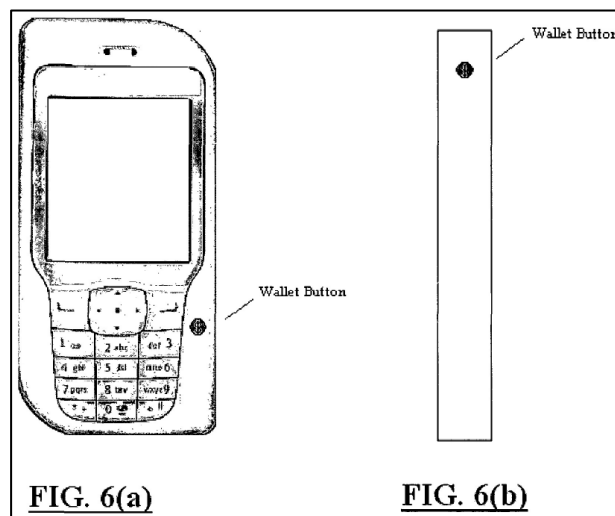
EX1002 ¶¶244-46.

External-Storage-Authentication Theory: As discussed regarding 7[a] and 7[b], Dua’s wireless device repeatedly checks for a reader key (*repeatedly sensing said value of 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 ¶247-49.

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 the value of the parameter to the criterion*). Dua ¶[0353]. Similarly, the wireless device determines when the reader key can no longer be detected (*repeatedly deciding, based on comparing the value of the parameter 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 ¶¶247-49.

It would be obvious to a POSITA to cause the wireless device to (1) end the real-time, encrypted connection with the external storage and delete any retrieved credentials (*disabling said first function*) and (2) re-enable PIN entry to launch the wallet application, access the credentials, and/or use credentials (*enabling said 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 the value of the parameter to the criterion, whether or not to maintain enabled a first function while maintaining disabled a second function*”).

Dua already discloses this functionality with a wallet button, 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 end the real-time connection between the wallet application and external storage. EX1002 ¶¶250-51.

A POSITA would be motivated to apply this system with reader keys to reduce the risk of inadvertent credential transmission; 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 ¶252.

(c) **Claim 3**

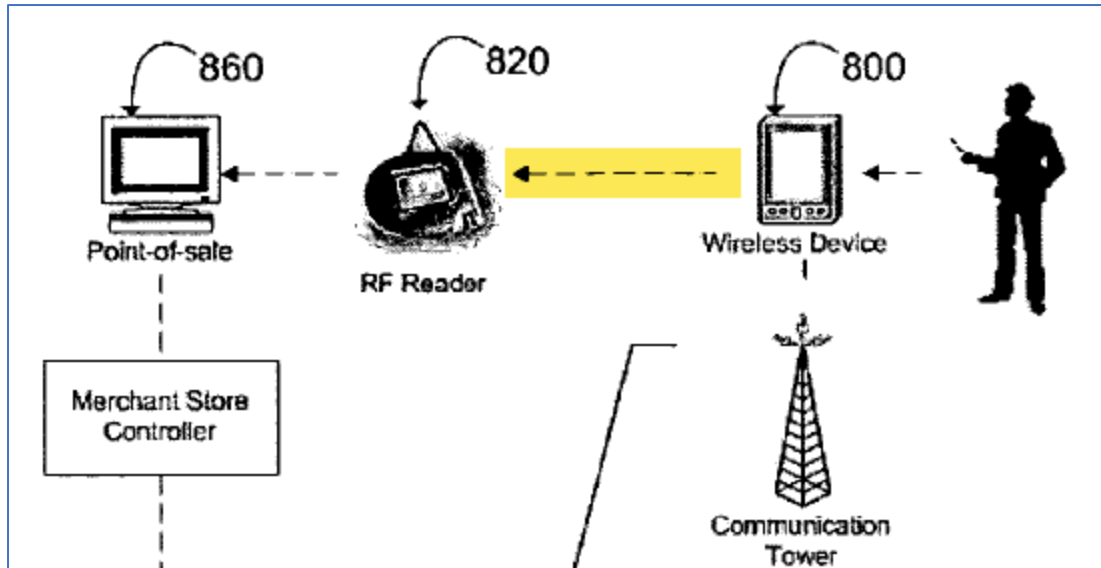
(i) **3[pre]**

See Claim 1, *supra*.

After receiving/retrieving credentials (*following said establishing the capability*), under either the **Card-Issuing Theory** or the **External-Storage-Authentication Theory**, Dua discloses that the wireless device makes proximity transactions with point-of-sale readers. “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 ¶254.

(ii) **3[a][i]**

A purpose of Dua is to facilitate transactions and other communications between a wireless device and POS terminal “via, for example, a short range wireless link” Dua ¶[0026], Abstract, ¶[0041]. The annotated excerpt of Figure 8, below, illustrates the short-range link (highlighted in yellow) between Dua’s wireless device 800 and merchant RF reader 820.



See also Dua ¶[0405].

Dua discloses that the wireless device must be “in close proximity to a reader device” to communicate and engage in a “proximity transaction.” Dua ¶[0315]. “For example, a wireless device loaded with a wallet application, that also has an integrated RFID chip can simply be waved slowly *in close proximity* to a reader device to facilitate a transaction.” Dua ¶[0315] (emphasis added); see also ¶¶[0321], [0355], [0371]. Dua also discloses the RFID chip can be an NFC chip—thus disclosing NFC transactions. *Id.* ¶[0016]; see also EX1002 ¶255-57.

A POSITA would further understand that short-range RFID/NFC links are established *responsive to satisfying a proximity condition*. 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 ¶255-57. Specifically, Dua’s RFID and NFC

communications are only effective if there is an underlying signal of sufficient strength detected such that the device and the terminal can communicate. EX1002 ¶257; EX1035 at 4, 36; EX1037 at 3. And that signal strength correlates to proximity and rapidly deteriorates as distance increases. EX1002 ¶257. When Dua is able to communicate with the POS terminal using NFC, the wireless device has detected that a *proximity condition* is *satisf[ie]d* (e.g., Dua at Abstract, ¶¶[0041], [0314]-[0315], [0382], [0395]) by receiving and decoding a short-range NFC signal from the POS device. EX1002 ¶257.

Further, Patent Owner's infringement contentions allege that the use of NFC is itself sufficient to show the claimed *satisfying a proximity condition*. EX1016 at 29-42; EX1002 ¶¶258.

In addition, it would be obvious to a POSITA that Dua's wireless device detects proximity to the POS based on a signal from the POS terminal. Dua's wireless device establishes a peer-to-peer communication session with the POS terminal over NFC using short-range signals. Dua Abstract, ¶¶[0016], [0041], [0314]-[0315], [0382], [0395], Claims 33, 36, 50. Dua contemplates NFC communication sessions transferring a significant amount of data, such as encryption keys and several credentials. Dua ¶[0359]. To ensure successful communications and avoid wasteful signaling and wasted user time, Dua's wireless device first detects it is near the POS prior to proceeding with a payment transaction. Further,

transmitting sensitive financial information when there is no bona fide POS in proximity poses a security risk. Therefore, it would have been obvious for a POSITA to configure the smartphone to first detect that it is proximate to Dua's POS prior to attempting short-range signal communication to prevent the error conditions or fraud. EX1002 ¶259-61. 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].

(iii) 3[a][ii]

According to Patent Owner, this limitation does not impose any new requirement relative to limitation 1[a][i]: the same sensing of the *value of the parameter* and *determining* it *satisfies the criterion* as a prerequisite to establishing the capability is also a prerequisite to then *using* that capability. Compare Ex1016 at 7-20 with EX1016 at 52-61 (pointing to the same “fingerprint unlock,” “facial recognition,” “iris authentication,” and similar security functionality and associated evidence for both limitations); see also EX1002 ¶266.

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

First, Dua discloses that each individual transactions requires opening the wallet application, similar to receiving or retrieving credentials. Opening the wallet for individual transactions is also subject to the “default security setting in the wallet application [] that PIN-entry is required before” (*responsive to*) “any credentials [are] transmitted to an external device,” such as for a transaction with a POS. 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 regarding limitation 1[a][i]. *See also* EX1002 ¶¶262-66.

Second, *sensing* a “reader key” occurs 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 3[a][ii].

(iv) 3[a][iii]

After receiving/retrieving credentials under either the **Card-Issuing Theory** or the **External-Storage-Authentication Theory**, Dua discloses that the wireless device uses those credentials (*using the capability*) for proximity transactions with POS terminals (*conducting the financial transaction by paying for a product*). “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 ¶¶267-69. 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 ¶¶270-72.

(v) 3[b][i]

This limitation mostly repeats the *proximity condition* of limitation 3[a][i] 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.*” Those requirements are addressed above in connection with limitation 3[a][i], 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 ¶¶270-71.

(vi) 3[b][ii]

Limitation 3[b][ii] repeats the *sensing* of limitation 3[a][ii] and is disclosed for the same reasons.

(vii) 3[b][iii]

This limitation mostly repeats the *proximity condition* of limitation 3[a][i] and the *sensing* of limitation 3[a][ii] and is disclosed for the same reasons.

The only additional requirement is *paying for a product by selectively sending information to at least one device*. Dua discloses, after satisfaction of all the requirements discussed above, that the wireless device sends credentials (*selectively sending information*) to the POS terminal (*to at least one device*) to

execute the financial transaction. Dua Abstract.⁴ 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 ¶¶270-72.

(viii) 3[c]

The only additional requirement of limitation 3[c] is that the “*information*” of limitation 3[b][iii] be *transmitt[ed]... using unlicensed frequencies*. Dua meets this requirement by transmitting credentials using NFC and Bluetooth (*using unlicensed frequencies*). Dua Abstract, ¶¶[0016], [0318]; EX1002 ¶¶273-74.

NFC uses unlicensed frequencies, such as the 13.56 MHz ISM band. EX1002 ¶275; EX1031; EX1032 at 2. Patent Owner’s infringement contentions admit 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 ¶275. Bluetooth also uses unlicensed frequencies. EX1002 ¶263, 276; EX1027; EX1041.

(ix) 3[d]

Under both the **Card-Issuing Theory** and the **External-Storage Theory**, Dua discloses that the receiving/retrieving of credentials is a prerequisite to the

⁴ 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 62, 71, 72 (pointing to “the point-of-sale device” or “terminal” for both limitations).

wireless device conducting a financial transaction (*paying for the product by selectively sending information to at least one device*). As discussed above, conducting the financial transaction using those credentials requires previously (*responsive to*) *selectively requesting authorization* (1[a][iii]), *receiving the authorization* (1[b][i]), and *establishing the capability* (1[b][ii]). See also EX1002 ¶278.

(d) Claim 4

(i) 4[pre]

See Claim 3, *supra*.

(ii) 4[a]

Dua discloses *paying for a product*, such as groceries and train tickets, as discussed with limitation 3[b]. 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 ¶¶280-81.

(e) Claim 5

(i) 5[pre]

See Claim 4, *supra*.

(ii) 5[a] and [b]

Limitation 5[a] mirrors limitation 3[b] but further requires that the *selectively sending* is to *the access point* of claim 1 and further requires *selectively sending*

information ... to at least one other device that is predetermined. Dua discloses the wireless device sending credentials to a POS 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 ¶¶283-85.

Limitation 5[b] further requires *selectively receiving information from the access point* of claim 1 and *at least one other device that is predetermined*. After completing a transaction, the POS terminal transmits to the wireless device an indication of a “successful transmission of credentials to [the POS] reader.” Dua ¶¶[0364]-[0365]; *see also* Dua ¶¶[0015], [0041], [0293]. Additionally, the wireless device sends a “BYE” message to close the communication channel. Dua ¶[0182], FIG. 4; *see also* EX1040 at 5, 12. In other words, after a transaction is complete, the wireless device receives a message from the POS terminal indicating a “successful transmission of credentials”—*selectively receiving information from the access point*. Dua ¶¶[0364]-[0365]; *see also* Dua ¶¶[0015], [0041], [0293]. 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 ¶¶286.

(f) **Claim 6**

(i) **6[pre]**

See Claim 4, *supra*.

(ii) **6[a]**

Dua teaches wirelessly transmitting information *using unlicensed frequencies* 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 over a short-range link in a Time Division Duplex operation.*” EX1016 at 142 (emphasis added); EX1032 at 21 (describing NFC as a “half... duplex system”). EX1002 ¶288. Both NFC and Bluetooth operate *over a short-range link*. Dua at [0016]; *see also* EX1002 ¶289. Bluetooth—a half-duplex system (EX1038 at 1.)—also used *unlicensed frequencies over a short-range link in a Time Division Duplex operations* for bidirectional communication such as the transactional communications at issue. EX1002 ¶¶289-90; *see also* EX1032 at 21.

(g) **Claim 7**

(i) **7[pre]**

See Claim 1, *supra*.

As discussed regarding limitation 1[a], under the **Card-Issuing Theory**, prior to card-issuance the wallet application must be opened (*prior to said selectively requesting an authorization*). *See also* EX1002 ¶291-92. As discussed regarding

limitation 1[a], under the **External-Storage-Authentication Theory**, prior to retrieving credentials from the external storage, an SIP communication must be initiated with the external storage service (*prior to said selectively requesting an authorization*). See also EX1002 ¶293.

(ii) 7[a]

Limitation 7[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” and “locking” “the [] smartphone or application.” EX1016 at 88-89. 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 ¶¶294-96.

External-Storage-Authentication Theory: As discussed with limitations 1[a][i], Dua’s wireless device can receive through its wireless communication

capabilities (*sensing*) 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 (*determining that the parameter sensed satisfies the criterion*), the wallet application automatically selects the credential to transmit for a financial transaction. Dua ¶[0353]-[0354]; *see also* EX1002 ¶297.

As discussed with limitations 1[a][i], because credentials can be stored in the external wallet storage service (Dua ¶[0491]), receiving a registered reader key (*sensing the parameter*) causes (is *responsive* to) retrieval of the credentials from the external storage prior. Dua ¶¶[0492], [0494]. As part of retrieval, Dua’s device *enable[s] a first function* when “real-time connection is initiated between the wallet application and the storage service” by “utiliz[ing] SIP.” Dua ¶¶[0494]-[0495], *see also* EX1002 ¶298.

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 ¶299.

(iii) 7[b]

Limitation 7[b] mirrors the requirements of limitations 1[a][ii] and 1[a][iii] but adds that the *selectively communicating* and *using a communications capability of the first function*.

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

As discussed regarding 1[a][ii], Dua discloses *selectively establishing a master-slave relationship with the first device* under both the **Card-Issuing Theory** and the **External-Storage-Authentication Theory**. *see also* EX1002 ¶¶302, 304-5.

Card-Issuing Theory: As discussed with limitation 1[a] and 1[b], 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 a device*). Dua ¶[0180]. Because communication is through the unlocked wallet application, Dua ¶[0180], the “*communicat[ion]... us[es] [a] communications capability of the first function*.” EX1002 ¶294. These communications are used for the *establishing* and *requesting* as discussed above regarding 1[a][ii] and 1[a][iii]. *see also* EX1002 ¶¶300-301.

External-Storage-Authentication Theory: As discussed with limitation 1[a] and 1[b], 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 a device*). Dua ¶¶[0353], [0355], [0384], [0392], [0491]. To retrieve the credential, Dua sets up a “real-time connection ... 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 ¶303.

As discussed regarding 1[a][iii], the request to the external wallet storage service for a specific credential (*selectively requesting from the device*) is a “request[] [for] the authorization to establish the capability for conducting the *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 ¶306.

(h) Claims 8-14

Claims 8-14 are substantively identical to claims 1-7.

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 '743 patent. EX1002 ¶308. Additionally, there was no long felt, unresolved need met by the '743 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 ¶308-309. Further, the vast number of contactless payment systems and trials of those systems before the '743 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 '743 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 '743 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 '743 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 [0366], [0429], [0441], [0543]. ***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, less than nine months after being served with the complaint—more than three 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 13, 2025

Petition for *Inter Partes* Review

U.S. Patent No. 11,924,743

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 13,658 words, which is within the word limit allowed under 37 C.F.R. § 42.24(a)(i).

Date: May 13, 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 '743 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 14, 2025

/s/ James Glass

James Glass (Reg. No. 46729)