

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. IPR2025-00977

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

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 11,770,756**

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	3
III. GROUNDS	3
IV. STATE OF THE ART	3
V. '756 PATENT.....	6
A. '756 Patent Specification	6
B. Prosecution History (EX1011).....	6
VI. PERSON OF ORDINARY SKILL	7
VII. CLAIM CONSTRUCTION	7
VIII. GROUNDS	7
A. Ground 1: Jain	7
1. Background	7
2. Analysis.....	9
B. Ground 2: Dua	40
1. Background	40
2. Analysis.....	42
C. Secondary Considerations	70
IX. STIPULATION	71
X. CONCLUSION.....	72

EXHIBIT LIST

Exhibit	Description
EX1001	U.S. Patent No. 11,770,756 (“’756 Patent”)
EX1002	Declaration of Dr. Kevin Almeroth, Ph.D.
EX1003	Exhibit Intentionally Omitted
EX1004	Curriculum Vitae of Dr. Kevin Almeroth, Including List of Recent Expert Witness Engagements of Dr. Kevin Almeroth
EX1005	Prosecution History for U.S. Pat. No. 9,462,411
EX1006	Prosecution History for U.S. Pat. No. 9,832,708
EX1007	Prosecution History for U.S. Pat. No. 10,219,199
EX1008	Prosecution History for U.S. Pat. No. 10,660,015
EX1009	Prosecution History for U.S. Pat. No. 10,674,432
EX1010	Prosecution History for U.S. Pat. No. 11,304,118
EX1011	Prosecution History for U.S. Pat. No. 11,770,756
EX1012	Prosecution History for U.S. Pat. Appl. Pub. No. 2023/0403631
EX1013	Prosecution History for U.S. Pat. No. 11,924,743
EX1014	Prosecution History for U.S. Pat. No. 11,937,172
EX1015	Prosecution History for U.S. Pat. No. 12,028,793
EX1016	Patent Owner’s District Court Infringement Chart for ’756 Patent
EX1017	U.S. Pat. Pub. No. 2009/0069049 (“Jain”)
EX1018	U.S. Pat. Pub. No. 2006/0165060 (“Dua”)
EX1019	U.S. Pat. Pub. No. 2010/0082481
EX1020	U.S. Pat. Pub. No. 2010/0082490
EX1021	U.S. Pat. Pub. No. 2009/0307140

Exhibit	Description
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)

Exhibit	Description
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	“Enabling Fast Wireless Networks with OFDM,” EETimes (February 1, 2001), https://www.eetimes.com/enabling-fast-wireless-networks-with-ofdm/
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
EX1047	Near Field Communication – Interface and Protocol (NFCIP-1), Standard ECMA-340 (2nd Edition)

LIST OF CHALLENGED CLAIMS

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

Claim	Limitation
3[c]	responsive to receiving the authorization, enabling at the device the function for conducting the financial transaction.
4[pre]	The method of claim 3, further comprising:
4[a]	responsive to the device satisfying a proximity condition relative to an entity and responsive to the device sensing the parameter and determining the value that is associated with parameter that is sensed satisfies the threshold criterion, using by the device the function for conducting the financial transaction and conducting by the device the financial transaction by paying for a product.
5[pre]	The method of claim 3, further comprising:
5[a]	enabling at the second device a function for conducting the financial transaction.
6[pre]	A device that is configured to perform operations comprising:
6[a]	sensing by the device, using a device-based sensor, a parameter that is associated with the device, an environment of the device and/or a user of the device;
6[b]	determining by the device a value of the parameter that is sensed; and
6[c]	responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion, enabling by the device a number of functions of the device and disabling by the device a function of the device;
6[d]	wherein the parameter that is sensed using the device-based sensor, comprises a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state; and
6[e]	wherein the device comprises a smartphone.
7[pre]	The device of claim 6,

Claim	Limitation
7[a]	wherein said enabling by the device a number of functions of the device comprises enabling by the device a number of functions of the device that is greater than or equal to one.
8[pre]	The device of claim 6, wherein the operations further comprise:
8[a]	while said number of functions is enabled by having sensed the parameter and by having determined by the device that the value of the parameter that is sensed satisfies the threshold criterion, requesting by the device from a second device an authorization to enable a function for conducting a financial transaction by the device;
8[b]	responsive to the requesting, receiving from the second device the authorization to enable the function for conducting the financial transaction; and
8[c]	responsive to receiving the authorization, enabling the function for conducting the financial transaction.
9[pre]	The device of claim 8, wherein the operations further comprise:
9[a]	detecting by the device that a proximity condition has been satisfied between the device and an entity;
9[b]	sensing by the device the parameter and determining by the device the value that is associated with the parameter that is sensed satisfies the threshold criterion; and
9[c]	responsive to the value that is associated with the parameter that is sensed satisfying the threshold criterion, using by the device the function for conducting the financial transaction and conducting by the device the financial transaction by paying for a product.
10[pre]	The device of claim 8, wherein the operations further comprise:
10[a]	causing a function for conducting the financial transaction to be enabled at the second device.
11[pre]	A method of operating a wireless device, the method comprising:

Claim	Limitation
11[a]	sensing by the wireless device, using a sensor of the wireless device, a parameter that is associated with the wireless device, an environment of the wireless device and/or a user of the wireless device;
11[b]	determining by the wireless device a value of the parameter that is sensed and determining by the wireless device whether or not the value that is sensed satisfies a threshold criterion;
11[c]	responsive to the value that is sensed satisfying the threshold criterion, enabling a number of functions of the wireless device and disabling a function of the wireless device;
11[d]	requesting by the wireless device from a second device an authorization to enable a function for conducting a financial transaction;
11[e]	responsive to the requesting, receiving by the wireless device from the second device the authorization to enable the function for conducting the financial transaction;
11[f]	responsive to receiving the authorization, enabling at the wireless device the function for conducting the financial transaction; and
11[g]	responsive to the wireless device satisfying a proximity condition relative to an entity and responsive to the wireless device sensing the parameter and determining that the value sensed satisfies the threshold criterion, using the function for conducting the financial transaction and conducting the financial transaction by paying for a product;
11[h]	wherein the parameter that is sensed, using the sensor of the wireless device, comprises a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state; and
11[i]	wherein the wireless device comprises a smartphone.
12[pre]	The method of claim 11,

Claim	Limitation
12[a]	wherein said enabling a number of functions of the wireless device comprises enabling a number of functions of the wireless device that is greater than or equal to one.
13[pre]	The method of claim 11, further comprising:
13[a]	enabling at the second device a function for conducting the financial transaction.
14[pre]	A wireless device that is configured to perform operations comprising:
14[a]	wherein said transmitting first data to a first device and said receiving second data from the first device comprises wirelessly transmitting/receiving by the smartphone using unlicensed frequencies, licensed frequencies, a WiFi air interface protocol, an Orthogonal Frequency Division Multiplexing air interface protocol and/or an Orthogonal Frequency Division Multiple Access air interface protocol.
14[b]	using a sensor of the wireless device and sensing a parameter that is associated with the wireless device, an environment of the wireless device and/or a user of the wireless device;
14[c]	determining a value that is associated with the parameter that is sensed and determining whether or not the value satisfies a threshold criterion;
14[d]	responsive to the value satisfying the threshold criterion, enabling a number of functions of the wireless device and disabling a function of the wireless device;
14[e]	requesting from a second device an authorization to enable a function for conducting a financial transaction;
14[f]	responsive to the requesting, receiving from the second device the authorization to enable the function for conducting the financial transaction;
14[g]	responsive to receiving the authorization, enabling the function for conducting the financial transaction; and

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

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

I. INTRODUCTION

The '756 patent is directed to enabling “functions” (such as the ability to perform financial transactions) of a “smartphone.” It does not, however, disclose any non-obvious technology for enabling functions, including the ability to engage in financial transactions. In the early 2000s, conducting financial transactions using smartphones was garnering significant attention due to the meteoric rise of smartphone, with pilot programs and commercial deployments by multiple companies, including Nokia, Motorola, Kyocera, and NTT. Multiple patent publications from this timeframe, including the prior art Jain and Dua references, render the '756 patent claims obvious.

Accordingly, Petitioner respectfully requests that the Board institute this IPR and find all '756 patent claims invalid.

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 '756 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 '756 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 '756 patent is in the same family as U.S. Patent Nos. 9,462,411, 9,832,708, 10,219,199, 10,674,432, 11,924,743, 11,937,172, and 12,028,793, which have also been asserted against Petitioner. Petitioner is concurrently filing IPR petitions against these family members.

C. Counsel and Service Information

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

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

D. Payment of Fees

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

E. Requirements for *Inter Partes* Review

Petitioner certifies that the '756 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)	1-18
2	§103	Dua (U.S. Pat. Appl. Pub. No. 2006/0165060)	1-18

IV. STATE OF THE ART

As the '756 patent recognizes, mobile phones could communicate using a variety of wireless protocols and frequencies that were well known prior to the alleged invention in late 2008. EX1001 1:34-55. 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 ¶86. 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 ¶86. So too were phones with Bluetooth capabilities, such as the Nokia 6310 and, again, the Samsung SCH-i730. EX1002 ¶86.

Near Field Communication (NFC) was also common at that time, and used RFID technology (*i.e.*, magnetic field induction) to allow short-range wireless

communications between devices in close proximity. EX1002 ¶¶87. 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 ¶¶87.

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 ¶¶88. This technology soon spread to the United States, with mobile phone and payment companies teaming up to conduct pilot programs of their own mobile payment software, including a 2006 pilot by Nokia and MasterCard, a 2007 pilot by Motorola and Discover, and a 2007 pilot by Kyocera and MasterCard, with companies such as ViVOtech releasing full mobile payment solutions. EX1002 ¶¶88; *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 ¶89. 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 ¶89. For example, the mobile phones used for mobile payments in the 2007 Kyocera and MasterCard trial included fingerprint scanners and required biometric authentication. EX1002 ¶89; *see also* EX1023 (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. '756 PATENT

A. '756 Patent Specification

The '756 patent specification relies on long-existing technologies, such as “wireless communications device[s],” “air interface protocol[s],” “signal strength measurement such as RSSI,” “Radio Frequency (RF),” and the “Internet Protocol (IP).” EX1001 3:12-22, 7:17-27, 8:9-20, 10:1-31; EX1002 ¶38. It further relies on long-established, generic concepts of computer systems such as “authorization,” “identity,” “sensors,” and “communications system[s].” EX1001 4:5-30, 5:39-63, 6:13-30, 8:62-9:21. For example, the specification acknowledges that the “adaptivity and mobility aspects of wireless communications” were already “important in people’s lives” at the time of alleged invention. EX1001 1:34-47. It also assumes, in the “Background of the Invention” section, that mobile phones could act as digital wallets. *See* EX1001 1:44-47. The '756 patent specification also relies on already-existing communications protocols. *See* EX1001 7:17-27. Nor does the specification disclose new or improved means of sensing (including physiological/biometric) or proximity detection by mobile phones. EX1002 ¶39.

B. Prosecution History (EX1011)

Amongst the file history of the other patents in the family (*see* EX1002 ¶¶45-77.), the Examiner rejected then-pending claims 1, 9, 16, and 22 for double patenting “over claims 1, 7, 17 of Patent No. 11,304,118.” EX1002 ¶¶41-44; EX1011 at 105. Applicant submitted a terminal disclaimer for the '118 patent. EX1011 at 148. The

Examiner then rejected the claims as obvious. EX1011 at 106. In response, applicant argued that the prior art lacked the claimed “disabling a function of the device” and a “physiological parameter satisfy[ing] any criterion.” EX1011 at 136-37. The Examiner then allowed the application. EX1011 at 213-14.

VI. PERSON OF ORDINARY SKILL

A person of ordinary skill in the art at the time of the '756 patent (“POSITA”) had at least a Bachelor of Science in electrical engineering, computer engineering, or similar fields and at least two years of practical experience in the field of secure wireless communication applications. More education can supplement for less practical experience, and vice versa. EX1002 ¶¶78-80.

Petitioner’s expert, Dr. Almeroth, exceeded this level by the priority date. EX1002 ¶81.

VII. CLAIM CONSTRUCTION

No express constructions are required to find the '756 patent claims invalid; however, Petitioner addresses the plain meaning of certain terms in the analysis for the presented Grounds.

VIII. GROUNDS

A. Ground 1: Jain

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 '756 patent—

Nov. 4, 2008. EX1002 ¶¶90. Jain discloses all limitations of the '756 patent claims, but Petitioner presents Jain as an obviousness reference in the event Patent Owner argues there are differences between Jain and the '756 patent claims. Jain was not considered by the office during prosecution of this or any related application.

Below is a short, non-limiting overview of Ground 1:

'756 patent claim 1 requires two steps to be performed by a smartphone—a sensing-and-determining step and enabling-and-disabling step. The first sensing-and-determining step consists of (1) sensing a parameter (*e.g.*, physiological state), (2) determining a value associated with the sensed parameter, and (3) determining if that value meets a criterion. Jain discloses this step by its smartphone performing user authentication via fingerprint authentication. *E.g.*, Jain ¶¶[0018], [0021], [0075], FIG. 7B (depicting steps 734-742); *see also* EX1002 ¶¶91-93.

After sensing a parameter that meets a criterion, the second enabling-and-disabling step consists of (1) enabling a function and (2) disabling a function of the smartphone. Jain discloses this step. EX1002 ¶¶94-95. After successful authentication, the mobile device with the transaction card is enabled to use cellular radio technology to request authorization from a financial institution to activate the transaction card. *See* Jain FIG. 7A (714, 720, 736), FIG. 9 (920-926). And because fingerprint authentication also means that the transaction card is not activated,

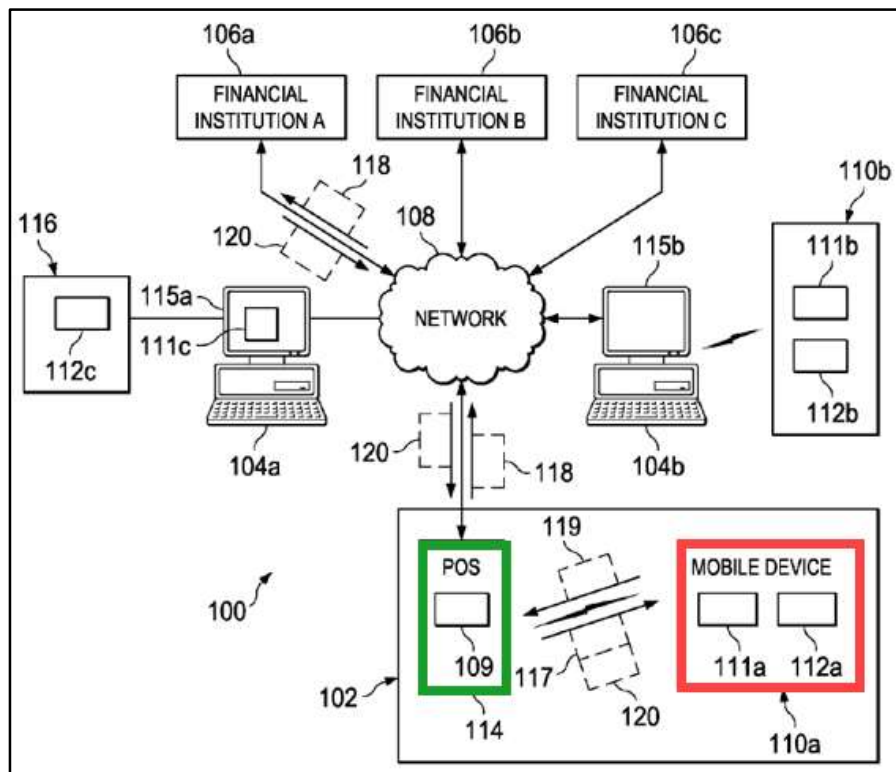
fingerprint authentication disables the smartphone’s ability to engage in financial transactions while the authorization request is processed. Jain ¶[0081], FIG. 7A.

2. Analysis

(a) Claim 1

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

Jain describes operating a “mobile device 110,” which can include a “transaction card 112” attached thereto or incorporated therein to “wirelessly execut[e] transactions” with retail point-of-sale terminal 114. See Jain ¶¶[0005], [0018]-[0019], [0021], [0029], FIG. 1; EX1002 ¶96:



Jain FIG. 1 shows a customer’s mobile device 110a with transaction card 112a and GUI 111a (red box) wirelessly executing transactions with a nearby POS device

114 (green box). See Jain ¶[0019]. The POS device 114 transmits transaction request 117 to the transaction card. Jain ¶[0027]; EX1002 ¶97. The mobile device 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 to a financial institution. Jain ¶[0027]. The financial institution transmits authorization response 120 to the POS device, which in turn transmits it to the mobile device's transaction card. Jain ¶[0027]. This response includes a payment transaction receipt presentable to the user through the mobile device's GUI. Jain ¶[0027]. The exchange between the mobile device's transaction card and POS device uses short range signals such as NFC or Bluetooth. Jain ¶[0023].

Jain interfaces the mobile device with a transaction card that “convert[s] the mobile device... to a contactless payment device loaded with a financial vehicle... that may be... a credit card... .” Jain ¶[0029]. In such embodiments, the transaction card is included as part of the mobile device. Jain ¶[0019] (“The offline store 102 includes a mobile device [110a¹] having a transaction card 112a and a Point of Sale

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

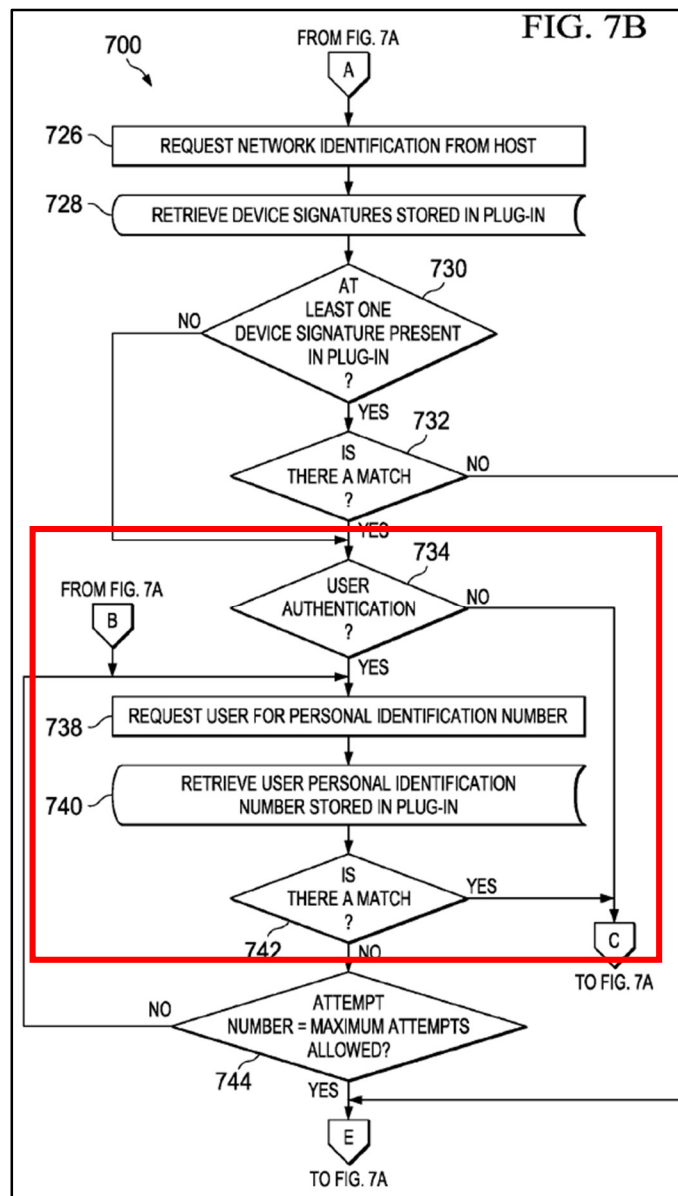
(POS) device 114 that executes transactions with customers.”), FIG. 1 (showing transaction card 112a within mobile device 110a). *See also* EX1002 ¶¶98-100.

To the extent Patent Owner argues Jain’s transaction card cannot be considered part of the mobile device, Jain at least renders obvious implementing the processes discussed herein in connection with a transaction card 112 that is integrated into mobile device 110. 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 ¶99. Integrating the transaction card with the mobile device achieves the benefits disclosed in Jain without incurring the cost of implementing an independent transaction card, instead leveraging components of the mobile device. EX1002 ¶99. Finally, incorporating the transaction card into the mobile device protects against inadvertent loss if the transaction card were to become detached without the user noticing. EX1002 ¶100.

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

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

Jain discloses, as part of its authentication process for “automatically bootstrapping” transaction card 112 to mobile device 110, authenticating a user using a PIN number or biometrics (*e.g.*, fingerprint) (*a parameter that is associated with... a user of the device*). See Jain ¶¶[0072], [0075], FIG. 7B (below); EX1002 ¶¶101-102.



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

Jain discloses that rather than “entering a PIN,” “the user may be authenticated using... biometric information (*e.g.*, fingerprint)” (*parameter that is associated with... a user of the device*). Jain ¶[0075]. Thus, Jain discloses performing steps 738, 740, and 742 in the context of biometric verification, where the steps include scanning a fingerprint (*sensing by the device, using a device-based sensor*), extracting a set of features representing the fingerprint (*determining... a value of the parameter that is sensed*), retrieving locally-stored fingerprint data of the rightful owner, and comparing the two sets of fingerprint data. At a minimum, this parameter-data comparison requires assigning values to the parameter.

Further, Patent Owner’s infringement contentions allege that the use of biometric verification is sufficient to show *sensing*, *determining*, and *threshold criterion*. EX1016 at 5-20; *see also* EX1002 ¶¶102-103.

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. EX1021 ¶¶[0040]-[0042]; EX1024 ¶¶[0009], [0025]; EX1025 ¶¶[0044], [0086]-[0092]; EX1026 at 196; EX1002 ¶104.

Biometric authentication is to ensure biometric information of a user matches that of the rightful owner. The rightful owner's biometric information must be stored during device setup, and then used to compare against a current user's biometric information. To pass, the two must correlate to provide adequate confidence that the current user is the device's owner.

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

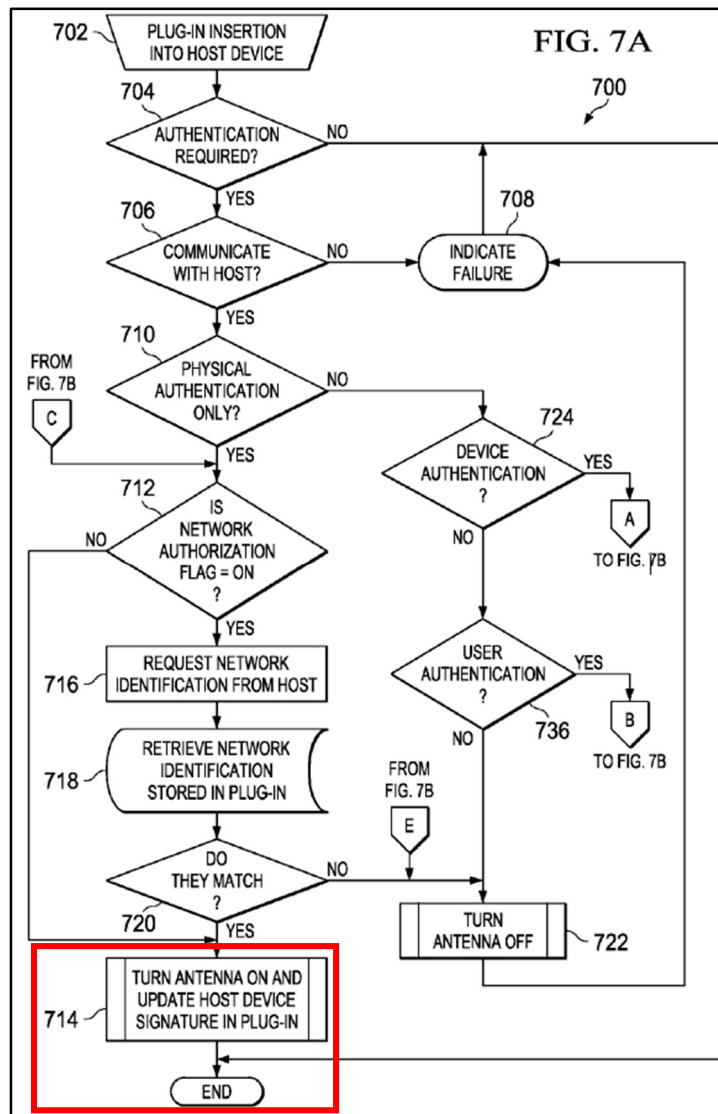
This limitation includes two parts: determining if the *parameter* satisfies a *threshold criterion*, and if it does, (a) *enabling by the device a number of functions*, where the *number of functions* could be just one (*see* limitation 2[a] (specifying *the number of functions* is *greater than or equal to one*)), and (b) *disabling by the device a function*. Jain discloses all of those requirements. EX1002 ¶105.

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

sufficiently close (*satisfying a threshold criteria*). See limitations 1[a]-[b]; EX1002

¶106.

Second, in response to authenticating the user (in steps 738-744 of FIG. 7B) (*responsive to satisfying a threshold criterion*), Jain process 700 returns to step 712 (see label C in both figures) and proceeds to step 714: “turn antenna on and update host device signature in plug-in” (*enabling by the device a number of functions of the device*). See Jain ¶¶[0072]-[0075], FIG. 7A; EX1002 ¶107.



Specifically, if the host-device signature is updated (as described in FIG. 7) to match the host device, the transaction card completes the bootstrap operation and can communicate with the host; otherwise, the “host device is rejected, bootstrap is aborted and the card 400 is returned to the mode it was before being inserted into the device.” Jain ¶[0065]. Only after bootstrapping/authentication (FIG. 7) is complete can activation (FIG. 9) begin, where activation includes communicating with a financial institution “using cellular radio technology of the host device.” Jain ¶¶[0065], [0072] (“an intelligent card may execute one or more authentication procedures prior to activation.”), [0081]. Thus, successful authentication as part of “automatically bootstrapping” (Jain ¶[0072].) allows the cellular radio communication required to activate the transaction card with a financial institution (*number of functions of the device*). EX1002 ¶108.

As for the claimed *disabling by the device a function of the device*, Jain discloses this part of the claim under two theories (EX1002 ¶¶109-112.):

First Theory for Enabling/Disabling Limitation: While the mobile device is enabled to use cellular radio technology communicate with a financial institution to perform the activation process (*enabling by the device a number of functions*), payment transactions are disabled (*disabling by the device a function of the device*) because the transaction card is not yet activated. Jain ¶[0081]. Only once bootstrapping/authentication (Jain FIG. 7) is complete can activation (Jain FIG. 9)

begin, which includes communicating with a financial institution “using cellular radio technology of the host device.” Jain ¶¶[0065], [0072], [0081]. Otherwise, the transaction card lacks access to the host-device’s cellular radio technology, because it lacked access to this cellular radio technology “before being inserted into the device.” Jain ¶[0065].

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

Second Theory for Enabling/Disabling Limitation: Jain meets this limitation by *enabling a number of functions of the smartphone* (turning its

antenna on and enabling cellular communications when the user is authenticated) and *disabling a function of the smartphone* (mode before transaction card was inserted into the device). In its infringement contentions, Patent Owner argued that this limitation is met by “enabling a number of functions of the smartphone, such as unlocking the smartphone or an application, and disabling a function of the smartphone, such as disabling the lock function.” EX1016 at 20. Similarly, Jain’s bootstrapping/authorization process (FIG. 7) must be fully completed prior to turning on the antenna and updating the host device signature to enable cellular communication (step 714), and conversely, the “host device is rejected, bootstrap is aborted and the card 400 is returned to the mode it was before being inserted into the device” if that bootstrapping/authorization process was unsuccessful. Jain ¶[0065].

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

As discussed with limitations 1[a]-[b], Jain discloses authenticating a user using a fingerprint (*physiological state*). See Jain ¶[0075]; see also EX1016 at 28; EX1002 ¶113.

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

Jain's "mobile device 110" can be a "*smartphone*." See Jain ¶¶[0018], [0021]; EX1002 ¶114.

(b) Claim 2

(i) 2[pre]

See Claim 1, *supra*; EX1002 ¶115.

(ii) 2[a]

As discussed with limitation 1[c], Jain discloses enabling one or more (*a number... greater than or equal to one*) functions. EX1002 ¶116.

(c) Claim 3

(i) 3[pre]

See Claim 1, *supra*; EX1002 ¶117.

(ii) 3[a]-[b]

Claim 3 identifies additional steps to be performed after *enabling... functions* discussed with limitation 1[c]. Jain discloses these steps. EX1002 ¶118. The first of these additional steps is *requesting by the device from a second device an authorization to enable a function for conducting a financial transaction by the device*.

After authenticating the user and enabling the mobile device to use cellular technology, Jain's smartphone performs "method 900 for activating a wireless transaction system" with the financial institution. Jain ¶[0080]. During step 920 of this method, the transaction card, via the smartphone, "wirelessly transmits a request

for the activation code using the cellular... technology” to the financial institution²

(*requesting by the device from a second device authorization*). Jain ¶[0081], FIG.

9; see also EX1002 ¶120:

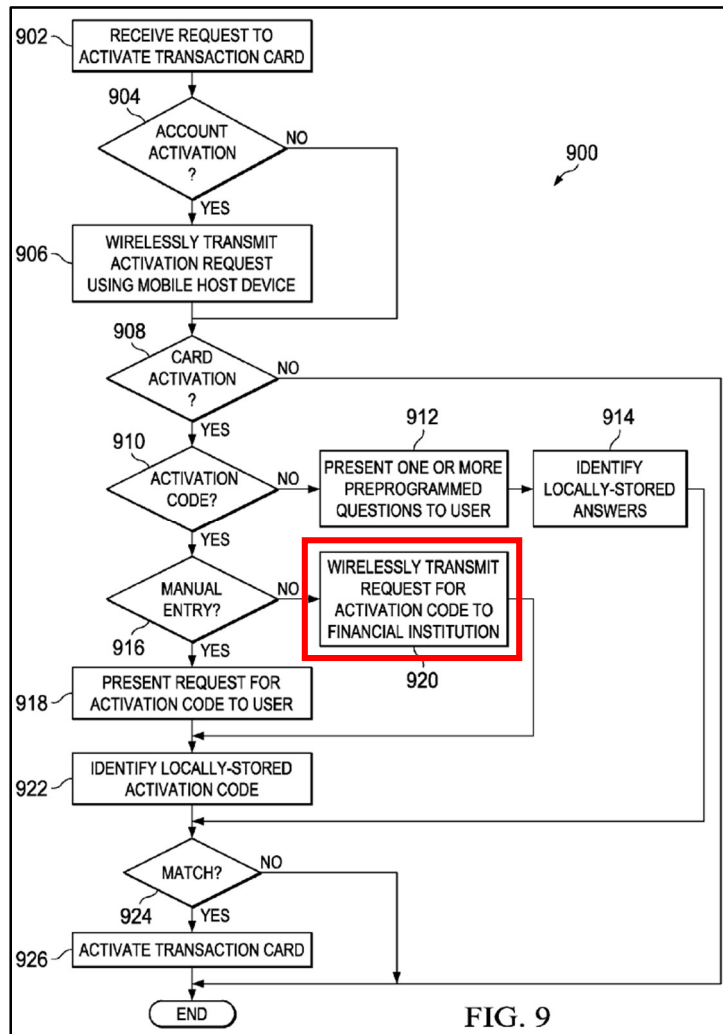


FIG. 9

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

In response to the request of step 920, mobile device 110 receives an activation code (*receiving by the device... the authorization*) from the financial institution (*second device*). EX1002 ¶121. The received activation code is then checked against a stored activation code (retrieved at step 922). Jain ¶[0081]. If the codes match, “the transaction card is activated” at step 926. Jain ¶[0081]. This “activation process may include activating the transaction card and/or financial account” (Jain ¶[0026].), 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 ¶¶120-122.

Thus, steps 920 and 924 are performed in order to “activat[e] the transaction card and/or financial account.” Because the “activation code” is required to enable transactions with that card (*function for conducting a financial transaction*) and because receipt of an activation code matching a stored activation code is the last step before the card is activated in step 926, a matching “activation code” is an *authorization* to engage in financial transactions, and requesting and receiving the same are thus *requesting* and *receiving... the authorization*. *See* Jain, FIG. 9. This mirrors Patent Owner’s infringement contentions, asserting that adding a credit card is sufficient to establish “*requesting authorization*” and “*receiving... authorization to enable the function for conducting the financial transaction.*” EX1016 42-55; *see also* EX1002 ¶122.

A POSITA would further understand that the financial institution would not provide a matching activation code to a request by the smartphone for an activation code, if the smartphone is not authorized to perform payment services. This understanding is supported by step 924, which compares the received activation code with a local activation code from step 922 to determine “[i]f the locally stored information matches the provided” activation code. Jain ¶¶[0081]; FIG. 9; *see also* EX1002 ¶¶[123-24]. 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 ¶¶[120-24].

At a minimum, such an implementation was well known and would have been obvious to a POSITA, as evidenced by numerous references describing similar processes. EX1019 ¶¶[0145]-[0146]. A POSITA would be motivated to treat Jain’s matching activation code as an authorization (and not provide the same if the transaction card is unauthorized) in order to improve system security and guard financial institutions against fraudulent transaction cards. 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.

(iii) 3[c]

As a result of *receiving the authorization* discussed with limitation 3[b] (*responsive to receiving the authorization*), Jain discloses that the mobile device with the transaction card checks that the received activation code matches the stored activation code. Jain ¶[0081]. Upon finding a match, the transaction card is activated at step 926, allowing the smartphone and transaction card to engage in financial transactions (*enabling at the device the function for conducting the financial transaction*). See Jain ¶¶[0071], [0081], FIG. 9; EX1002 ¶125.

(d) Claim 4

(i) 4[pre]

See Claim 3, *supra*; EX1002 ¶126.

(ii) 4[a]

Claim 4 builds on claim 3, which builds on claim 1. Claim 1 recites steps for *enabling... functions*. Claim 3 recites steps for using those functions for enabling a *function for conducting a financial transaction*. Claim 4 recites steps for engaging in a financial transaction. Engaging in a transaction requires two prerequisites—*satisfying a proximity condition relative to an entity*; and *sensing the parameter... satisf[ying] the threshold criterion*—before finally *paying for a product*. Jain discloses claim 4. EX1002 ¶127.

Satisfying a proximity condition: Jain’s smartphone and transaction card use short range signals, such as NFC or “proximity signals,” to determine proximity with a POS terminal prior to executing a transaction. See Jain ¶[0023]; EX1002 ¶128.

The smartphone first “wirelessly receive[s] a request from the POS device 114 to execute a transaction and/or provide a response.” Jain ¶[0023]. A POSITA would understand that Jain’s mobile device 110 is only able to process the “request” if sufficiently close to POS device 114 to actually receive and decode the requests short-range signal (*responsive to the device satisfying a proximity condition*). EX1002 ¶¶128-29; EX1034 at 11-12; *see also* EX1036 at 220. Jain’s NFC and other short range wireless communication protocols are only effective if a signal of sufficient strength is detected such that the device and the terminal can communicate using that protocol. EX1002 ¶¶128-29; EX1035 at 4, 36; EX1037 at 3. That signal strength rapidly deteriorates as distance increase. EX1002 ¶128; EX1035 at 4, 36; EX1037 at 3. Jain recognizes that NFC requires proximity of “10 cm or less.” Jain ¶[0030]. For Jain’s mobile device to receive and process a request over NFC, the mobile device and POS device must be sufficiently close. A POSITA would understand that this corresponds to *satisfying a proximity condition*.

In addition, *satisfying a proximity condition* also occurs earlier in Jain’s NFC exchange. Jain’s NFC “wireless connection” is based on the “ISO 18092/ECMA 340” standards. Jain ¶¶[0018], [0023], [0051]; EX1002 ¶129. The ECMA 340

Interface and Protocol Standard for NFC³ explains that an NFC “transaction” requires an “initialization” and then a “data exchange.” EX1034 §§4.25, 10-12, FIG.

5. The standard specifies two devices (“Initiator” and “Target”) and two communication modes (“Passive” and “Active”). EX1034 §§1, 4.1, 4.16, 7. It does not matter whether Jain’s POS device or mobile device is the “Initiator,” with the other being the “Target,” or what communication mode they use: every combination results in Jain’s mobile device *satisfying a proximity condition* and then establishing a connection for subsequent communications. Specifically, in both modes, an “Initiator” device “shall activate its RF field” and a “Target” device then “shall be activated by the RF field of the Initiator.” EX1034 § 10. Then, the “Initiator” sends one or more commands (*e.g.*, ALL_REQ, SENS_REQ, and/or ATR_REQ) and receives one or more responses (*e.g.*, SENS_RES and/or ATR_RES). *See* EX1034 §§11.2.1.16-.17, 11.2.1.23, 11.3.2, 12.2-.3, FIGS. 13, 24-25. Thus, regardless of

³ The cited 2nd edition of “ECMA-340” was released in December 2004 (before Jain’s filing date) and not updated until June 2013 (after Jain’s filing). <https://ecma-international.org/publications-and-standards/standards/ecma-340/>. This version was also published as the “ISO 18092” standard cited in Jain. *Id.* The disclosures of ECMA-340 referenced here are found in both the 1st (December 2002) and the 2nd edition. *Compare* EX1047 (2004) *with* EX1034 (2002).

what mode is being used and which device in Jain is the Initiator and which device is the Target, the Target device detects a sufficiently strong field from the Initiator (*satisfying a proximity condition*), and the Initiator device detects that a Target is within its field by receiving a response to a command from the Target (*satisfying a proximity condition*). In addition, this exchange of commands and responses results in the selection of a particular “Target” and attributes/parameters for further communication with the same, thereby establishing a *short-range link*. EX1034 §§7, 11.2.1.24-25, 12, 12.1, FIGS. 22, 24-25. After this *link* is established, the Initiator and the Target communicate using ECMA 340’s data exchange protocol. EX1034 FIGS. 5, 23, 24. This includes transmission of Jain’s transaction request 117, transaction response 119, and authorization response 120.

Further confirming this limitation is met, Patent Owner alleges in its infringement contentions that the use of NFC is itself sufficient to show *the device satisfying a proximity condition*. EX1016 at 29-42; EX1002 ¶130.

In addition, it would be obvious to a POSITA that Jain’s smartphone would first detect it is proximate to the POS device (*satisfying a proximity condition*) based on a signal from the POS device (e.g., a “request,” Jain ¶[0023], or earlier commands and responses exchanged as part of implementing ECMA 340) prior to communicating with that POS device. To ensure communications would be successful and not wasted signaling, and further to avoid the security risk of

indiscriminately transmitting sensitive financial information, Jain's smartphone first needs to detect it is near the POS device prior to proceeding with a payment transaction with the POS device. EX1002 ¶¶130-35. Otherwise, the NFC communication would fail. Indeed, such implementations were well-known to a POSITA. For example, EX1020 discloses and leverages NFC to limit the range at which communication may take place. EX1020 ¶¶[0041], [0063]. Indeed, in the context of Wi-Fi, EX1020 even more explicitly discloses using the ability to receive such signals as an indication of proximity. Jain ¶[0073] ("The [identifying information] may be used by the device 10 to indicate that the device is located within communication range of the hot spot 169."). A POSITA would be motivated and able to use Jain's "request" or ECMA 340's commands and responses in the same manner. EX1002 ¶¶130-35.

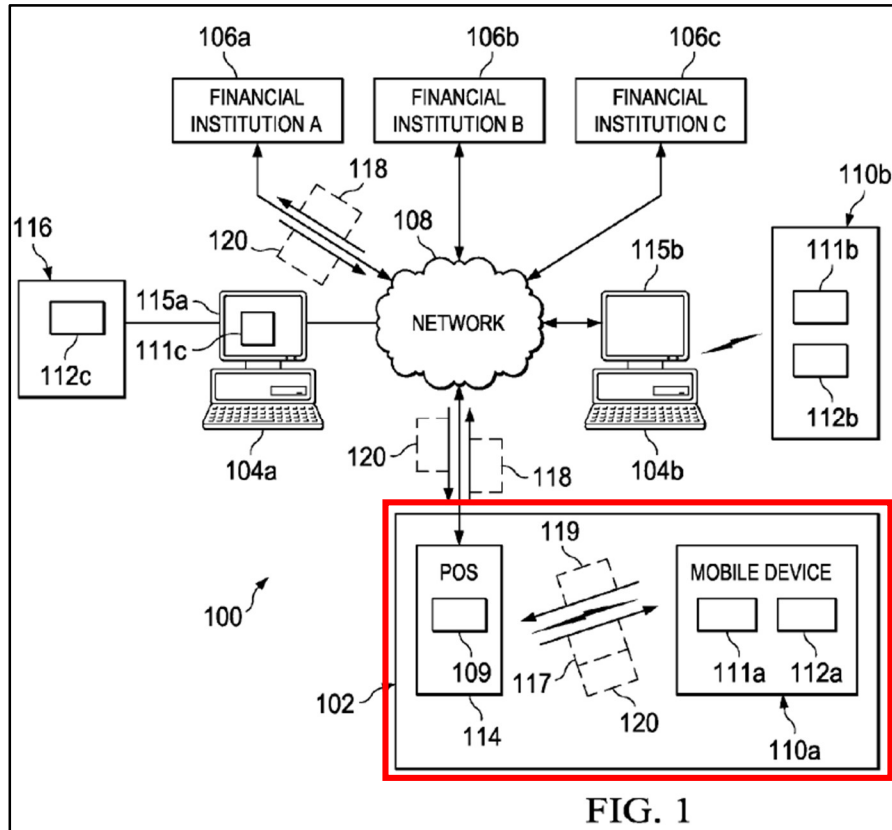
Determining the... parameter... satisfies the threshold criterion: According to Patent Owner, limitation 4[a] does not impose any new requirement relative to limitations 1[a]-[b]: the same sensing of *the* at least parameter and determining it meets *the* criterion prior to establishing the function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

Even if the claims require an additional transaction-specific **determining**, Jain discloses or renders this limitation obvious. For example, Jain discloses that during payment, the merchant terminal may “prompt the user to authorize a transaction such as by” fingerprint. Jain ¶¶[0029], [0075]. Jain further discloses that this request is presented and user information is received via GUI 111 of mobile device 110. Jain ¶¶[0023]-[0025]. Authorization via PIN involves or at least obviously involves the authentication process of Jain ¶[0075], as discussed with limitations 1[a]-[c]. At a minimum, a POSITA would find that using the previously other disclosed authentication process to be a simple and natural, and thus obvious, way of implementing PIN authorization: it does not require communication with any other devices and allows the POSITA to reuse aspects of the software that implements the user authentication of FIG. 7. EX1002 ¶¶132-34.

Jain’s disclosure of authorizing individual transactions via PIN also renders obvious doing so via biometrics (**determining the value... associated with parameter... satisfies the threshold criterion**). Jain already contemplates using biometrics (*e.g.*, fingerprints) for its user authentication process (Jain ¶[0075], FIG. 7.), and reusing that software and hardware for individual transactions would not further complicate the system or incur material additional costs.

Paying for a product: Jain discloses the transaction card and smartphone performing a contactless payment transaction with a nearby retail POS terminal 114

to *pay[] for a product*. See Jain ¶¶[0019], [0023], [0029]. Jain describes this referencing FIG. 1:



Jain’s smartphone and transaction card transacts with the POS terminal by using NFC (*using... the function for conducting the financial transaction*), which makes the transaction *responsive to the* smartphone and transaction card being within *proximity relative to* the POS terminal, and only after the bootstrapping/authentication process (*responsive to... sensing the parameter... satisf[ying] the threshold criterion*), both of which are discussed above. See Jain ¶[0023]; EX1002 ¶¶135-36.

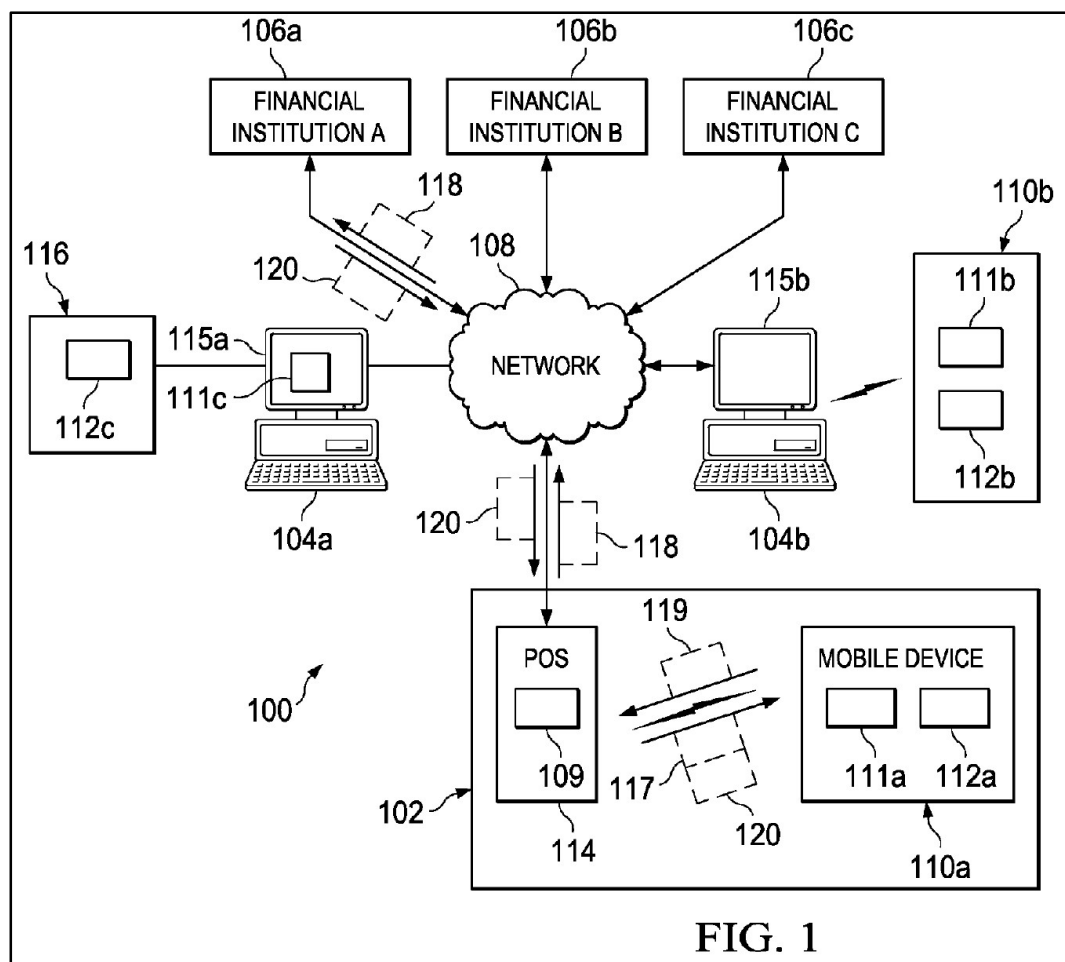
(e) **Claim 5**

(i) **5[pre]**

See Claim 3, *supra*; EX1002 ¶137.

(ii) **5[a]**

While Jain's smartphone conducts transactions with a POS terminal, Jain discloses an additional step where the POS terminal further sends transaction requests to a financial institution (*second device*) for authorization (*enabl[ed]... function for conducting the financial transaction*). See Jain ¶¶[0019], [0027], FIG. 1 (below); EX1002 ¶138.



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

The authorization by the financial institution checks whether the transaction card and mobile device used in the transaction is authenticated and activated. *See* Jain ¶[0026]; EX1002 ¶139. Jain’s bootstrapping/authentication process is a fraud control process. Jain ¶[0075]. If the process is failed, the mobile device “may execute one or more processes to... notify financial institutions of fraudulent activity,” and “block... the transaction card.” Jain ¶[0026]. This requires the financial institutions to check each transaction for a blocked mobile device and transaction card (*function for conducting the financial transaction*). Jain ¶[0026]. Because financial institutions perform authorization functions specific to transactions by the transaction card and mobile device, turning on those underlying authorization functionalities constitutes *enabling at the second device function for conducting the financial transaction*.

(f) Claims 6-16

Claims 6-16 are substantively identical to claims 1-5. Claims 6-10 are directed to “[a] device that is configured to perform operations,” whereas claims 1-

5 are directed to “[a] method of operating a device.” This distinction is immaterial since Jain discloses both methods and systems. Jain Title; EX1002 ¶140.

Independent claims 11 and 14 is substantively identical to independent claim 1 incorporated with dependent claims 3 and 4. Claims 12-13 and 15-16 are substantively identical to claims 2 and 5. Claims 11-13 are directed to “[a] method of operating a wireless device,” and claims 14-16 are directed to “[a] wireless device that is configured to perform operations,” whereas claims 1-5 are directed to “[a] method of operating a device.” These distinctions are immaterial since Jain is directed to a wireless “mobile device,” such as “smartphone,” and discloses both methods and systems. *E.g.*, Jain Title, Abstract, ¶[0018]; EX1002 ¶141.

(g) Claim 17

(i) 17[pre]

See Claim 14, *supra*; EX1002 ¶142.

(ii) 17[a]

Jain discloses the mobile device with the transaction card performing transactions with a nearby retail POS terminal 114 (*entity*) by sending requests and responses between one another over a “wireless connection (*e.g.*, NFC...)” (*a short-range wireless link*). *See* Jain ¶¶[0018]-[0019], [0023], [0027], [0029], [0051], [0054]; EX1002 ¶143. This is addressed in more detail in the ECMA 340 standard implemented by Jain (*see* limitation 4[a]), which describes an “Initiator” device and a “Target” device exchanging communications to select a particular “Target” and

attributes/parameters for further communication (*establishing... a short-range wireless link*). Indeed, Patent Owner’s infringement contentions allege the use of NFC as sufficient to show *establishing... a short-range wireless link*. EX1016 at 309-10.

(iii) 17[b]-[d]

Jain meets these requirements by transmitting information to the POS device (*i.e.*, “*entity*”) “using short range signals such as NFC (*e.g.*, ISO 18092/ECMA 340),... proximity signals, and/or other signals compatible with retail payment terminals (*e.g.*, POS 114)” (*i.e.*, “*wirelessly transmitting information*”). Jain ¶[0023]; *see also* EX1002 ¶145.

NFC used the 13.56 MHz ISM band, which is an *unlicensed frequency*. EX1002 ¶146; EX1031; EX1032 at 2. Patent Owner’s infringement contentions allege that “NFC is based upon the unlicensed 13.56 MHz frequency.” EX1002 ¶147; EX1016 at 57-58. Bluetooth also used unlicensed frequencies. EX1002 ¶148; EX1041. Jain discloses the smartphone *wirelessly transmitting information* related to transaction execution and authentication to the POS terminal (*entity*). Jain ¶¶[0019], [0027]. In response, the POS terminal transmits to the wireless device “receipts of the transaction” (*wirelessly receiving information from the entity*). Jain ¶¶[0019], [0027]. These transmissions are done with protocols including NFC and Bluetooth. Jain ¶[0023].

NFC is a *time domain duplex protocol*. Patent Owner's alleges NFC as such a *protocol*. EX1016 at 310-14. A POSITA would have known these things too. See EX1032 at 21 (describing NFC as a "half... duplex system"); EX1002 ¶149.

Bluetooth also *us[es] unlicensed frequencies* and a *time domain duplex protocol*. EX1002 ¶150.

(iv) 17[e]

This limitation further requires that *establishing the short range link* occurs *responsive to... satisfying the proximity condition* (addressed with limitation 4[a]) and *responsive to the... parameter... satisf[ying] the threshold criterion* (addressed with limitations 1[a]-[c] and 4[a]). Jain discloses both requirements. EX1002 ¶¶151-55.

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

Responsive to... satisf[ying] the threshold criterion: As discussed with limitations 1[a]-[c], Jain discloses fingerprint authentication (***parameter... satisf[ying] the threshold criterion***) for the bootstrapping/authentication process prior to activating the mobile device with the transaction card. Because the activation is required to execute transactions, fingerprint authentication is also a prerequisite (***responsive to... satisf[ying] the threshold criterion***) to executing transactions over NFC (***establishing... a short-range wireless link with the entity***). EX1002 ¶153.

At a minimum, it would be obvious to a POSITA that Jain's smartphone would establish a NFC connection with the POS device (***establishing... a short-range wireless link with the entity***) after detecting ***the wireless device satisfying the proximity condition relative to the entity*** and ***sensing the parameter... satisfies the criterion***. To ensure communications would be successful and not wasted signaling, and further to avoid the security risk of indiscriminately transmitting sensitive financial information, Jain's smartphone needs to detect proximity and then establish a short-range communication link prior to proceeding with a payment transaction with the POS device. EX1002 ¶¶154-55. Use of a link after detecting proximity further improves reliability and security, because once a link is established, Jain's mobile device can receive confirmation of receipt of individual packets. Indeed, such implementations of devices communicating via NFC establishing a connection

prior to transmitting information were well-known to a POSITA. EX1019 ¶¶[0011], [0124], [0182]. For example, in EX1019, “to facilitate the establishment of an NFC connection (e.g., typically 2-4 cm)” (*satisfying the proximity condition*), an “RF field generated by the payee device [] may induce [] transition to an active mode of operation, thus establishing an NFC connection between the two devices.” EX1019 ¶[0124]. “Accordingly, by way of this established NFC connection, the payment [information] may be transmitted to and received by the payor device.” EX1019 ¶[0124].

At a same time, it would be undesirable from the perspective of the POS device to establish a link before the user of the device has been authenticated (e.g., via the biometric processes discussed in connection with limitation 4[a]), since the established link can then be hijacked by other, unauthorized if the device is in the possession of an unauthorized user. Accordingly, a POSITA would be motivated to delay completion of the ECMA initiation process (described above in connection with limitation 4[a]) to ***establish[] by the wireless device a short-range wireless link with the entity*** until after the user has completed the biometric authorization process (described above in connection with limitation 4[a]) (***responsive to the wireless device sensing the physiological parameter and determining that the physiological parameter sensed satisfies the criterion***).

(h) Claim 18

(i) 18[pre]

See Claim 14, *supra*; EX1002 ¶156.

(ii) 18[a]

Limitation 18[a] repeats language found in claim 14, also found in limitations 3[a]-[c] and addressed above. EX1002 ¶157.

(iii) 18[b]

Jain discloses the smartphone and transaction card “wirelessly transmit[ing] a request for the activation code using the cellular radio technology” to the financial institution, where those transmissions are over established links (*establishing by the wireless device a link with the second device*). Jain ¶¶[0041]-[0043] (“establishing connections between packet-switched networks and communication devices” where a financial institution is part of a packet switched network), [0046], [0081], FIG. 2. Indeed, Patent Owner’s infringement contentions allege the use of mobile data as sufficient to show *establishing... a link*. EX1016 at 309-10; EX1002 ¶158.

Plus, to improve reliability, a POSITA would further implement this communication using TCP, a very well-known connection-based protocol that is even referenced in Jain itself. Jain ¶[0052]; EX1002 ¶159. Moreover, part of this *link*, from mobile device 110 to base station 210, is a *wireless link*. Jain FIG. 2.

As an alternative to cellular radio technology, Jain also discloses “the mobile device 110 transmit[ing] packet data using its own connection to the external world

(e.g.,... Wi-Fi).” Jain ¶[0053], claims 13-14. This includes using “WiFi technology” to “wirelessly interface” with financial institutions. Jain ¶[0068], FIG. 5. This use of Wi-Fi involves establishing a *link*, part of which (from mobile device 110f to client 104e) is a wireless. Jain ¶[0068], FIG. 5; EX1002 ¶160.

In Jain, the *distance associated with the proximity condition* is the distance between a mobile device and a nearby POS device, where NFC is used to communicate and perform a financial transaction. See Jain ¶[0023]; EX1002 ¶161. This distance is “10 cm or less.” Jain ¶[0030]. The mobile device and the financial institution (*second device*) communicate using cellular radio technology, traversing intermediary nodes, including a base station. Jain ¶¶[0041]-[0043], FIG. 2. A wireless link to a base station (e.g., the top of a cell tower) is already going to be *greater than a distance* of the NFC wireless link—“10 cm or less.” Jain ¶[0030], FIG. 2.

(iv) 18[c]-[d]

Jain’s mobile device transmits a request (*information*) to the financial institution (*second device*) and receives an activation code (*information*) using cellular radio technology (*wirelessly... over said wireless link*). Jain ¶[0081]. Cellular radio technology *us[es]... licensed frequencies*. EX1002 ¶162.

To the extent Patent Owner argues the cellular radio technology uses unlicensed frequencies, this is also covered. EX1002 ¶163.

(v) 18[e]

As discussed with limitations 18[c]-[d], Jain discloses that the smartphone and transaction card “us[e]... cellular radio technology.” Jain ¶¶[0041]-[0043], [0081]. A POSITA would be motivated to use the most advanced and performant cellular radio technologies such as LTE and WiMAX (*i.e.*, 4G) in addition to the cellular radio technology mentioned in Jain to keep up with ever-evolving technologies that allow for higher data rates. LTE and WiMAX were known to a POSITA as of the ’756 patent’s priority date to be in line to displace older technologies in the near future. EX1002 ¶¶36-37, 40, 164; *see also* EX1045; EX1046. Wi-Max and LTE *us[e]... orthogonal frequency division multiplexing and/or orthogonal frequency division multiple access protocol*. EX1002 ¶164; *see also* EX1045; EX1046.

(vi) 18[f]

This limitation requires that the *establishing* of limitation 18[b] is performed that in response to the *sensing* and *determining* of limitations 14[a] and 14[b], respectively. This is disclosed in Jain. Jain requires completion of authorization process 700, including user authentication steps 734-742 (which include the claimed *sensing* and *determining*) before enabling the mobile device to communicate with the financial institution (*second device*) using cellular radio technology and then using that capability in connection with process 900, including steps 920-926. *See* Jain ¶¶[0072], [0080]-[0081], FIGS. 7, 9. Thus, establishing of a cellular link

between the mobile device and the financial institution (*establishing the link*) is responsive to Jain’s user authentication (*sensing the parameter... satisf[ying] the threshold criterion*). EX1002 ¶165.

B. Ground 2: Dua

1. Background

Dua is prior art under pre-AIA 35 U.S.C. § 102(b), having been published on July 27, 2006, and thus before the earliest effective filing date of the ’756 patent—Nov. 4, 2008. Dua discloses all limitations of the ’756 patent claims, but Petitioner presents Dua as an obviousness reference in the event Patent Owner argues there are differences between Dua and the ’756 patent claims.

Dua was cited during prosecution of the ’756 patent, but was only relied upon for rejections in the prosecution of related patents (the ’015 and ’432 patents) that contain substantially different limitations. 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 ’756 patent claims. EX1008 at 212-213. 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 ’756 patent’s claims do not contain this limitation or similar language. EX1009 at 171. During prosecution of the ’432 patent, Applicants argued, and the examiner

agreed, that Dua’s paragraphs [0026], [0089], and [0495] do not “teach or suggest ‘enabling a mode to communicate... responsive to at least one physiological parameter.’” EX1009 at 253, 275-276. But, in portions of Dua that were seemingly overlooked by the examiner, Dua *does* disclose “biometric technologies” including using a “fingerprint in lieu of a PIN code to authenticate a user to the wallet application.” Dua at 39:9-13, 45:55-58, 45:58-61. This argument, among others, is set forth below.

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

’756 patent claim 1 requires two steps to be performed by a smartphone—a sensing-and-determining step and enabling-and-disabling step. Those steps are broken down in Section VIII.A.1.

Dua discloses the first sensing-and-determining. Dua’s smartphone performs user authentication via fingerprints. *E.g.*, Dua ¶¶[0366], [0414], [0534].

Dua discloses the second enabling-and-disabling step under two theories—the **Card-Issuing Theory** and **External-Storage-Authentication Theory**. Under the **Card-Issuing Theory**, after scanning a valid fingerprint to open the wallet application, the wireless device enables communication with the issuer’s WCM for credit card issuance. Opening the wallet application also disables the lock on the wallet application and security subroutines tracking fingerprint authentication attempts.

Under the **External-Storage Theory**, the wallet application’s credentials are stored in external storage, not on the wireless device. Upon opening the wallet application with a valid fingerprint, the wallet application enables a communication channel with the external storage to retrieve the credentials, and disables the lock function and security subroutines discussed with the **Card-Issuing Theory**.

2. Analysis

(a) Claim 1

(i) 1[pre]

Dua discloses a wireless *device*, “such as a mobile telephone.” Dua Abstract, FIGS. 3, 5, 6(a)-8. The wireless device includes phone applications like a “wallet application,” which can be operated to “conduct[] financial... transactions” (*method of operating*). Dua Abstract, ¶¶[0041], [0312]-[0313], [0333]; EX1002 ¶174.

(ii) 1[a]-[c]

Limitations 1[a]-[c] can be grouped into two steps. First, check whether a *parameter* satisfies a *criterion* (*sensing*, *determining*, and *satisfying*) as part of, for example, a biometric scan. Second, if the check is passed, *enabl[e]... a number of functions* where a *number of functions* can be *greater than or equal to one* (’756 Patent, limitation 2[a].), and disable another, different *function*. Dua discloses these requirements under two theories: **Card-Issuing Theory** and **External-Storage Theory**. EX1002 ¶175

Card-Issuing Theory: In Dua, the wallet application must be opened for the wallet application to be issued a credit card. Dua ¶¶[0128]-[0129], [0178], [0180], [0250]. Thus, the “default security setting in the wallet application is that PIN-entry is required before the wallet application can be ‘opened’” or otherwise “allow[s] the user access to the application,” which receives an issued a credit card. Dua ¶¶[0366], [0429]. This understanding is confirmed by additional disclosure in Dua. EX1002 ¶176. **First**, using the wallet application requires authentication because “[d]ata in the wallet application is encrypted and protected with a special wallet PIN code.” Dua ¶¶[0366], [0429]. **Second**, Dua requires user authentication for making significant changes in the wallet application, such as “access[ing] stored credentials and chang[ing] any application settings or preferences.” Dua ¶[0366]. Adding a new credit card is such a change. **Third**, a wallet application can hold many pieces of confidential information. Dua ¶¶[0041], [0055], [0287]-[0288], [0334]. Regardless of how the wallet is opened, the wallet application allows the user to navigate and view the stored credentials and thus needs to be protected. Dua ¶¶[0324]-[0332], [0334], [0366], [0378]; *see also* EX1002 ¶¶176-77.

Further, a feature within a wallet/payment application to add an account or credit cards is well known to a POSITA. EX1002 ¶¶178-80; 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 ¶¶178-80.

At a minimum, requiring PIN entry under these circumstances would be obvious. To ensure security of the other credentials, alongside allowing use of an encrypted wallet application and changes to the wallet application by an authenticated user, a POSITA would retain Dua's "default" user authentication for credit card issuance. Dua ¶[0366]. Indeed, it was well known to require such verification before permitting access to such sensitive functionality. EX1019 ¶[0107], FIGS. 10A-B; EX1002 ¶¶178-80.

Dua teaches that PIN codes can be replaced with fingerprints (*parameter*) scanned by the "wireless device's embedded biometric technologies" (*sensing by the device, using a device-based sensor, a parameter*). Dua ¶¶[0366], [0414]; EX1002 ¶¶181-83. "[F]ingerprint[s]" can be used "in lieu of a PIN code to authenticate a user" (*determining by the device a value of the parameter that is sensed*). Dua ¶¶[0366], [0414], [0534]. For fingerprint-based authentication, the wireless device scans and *determin[es]... [the] value* to compare against the rightful owner's fingerprint value. Dua ¶¶[0366], [0414], [0534]. The scanned *value* can also decrypt the wallet application's data. Dua ¶¶[0050], [0366], [0399], [0429].

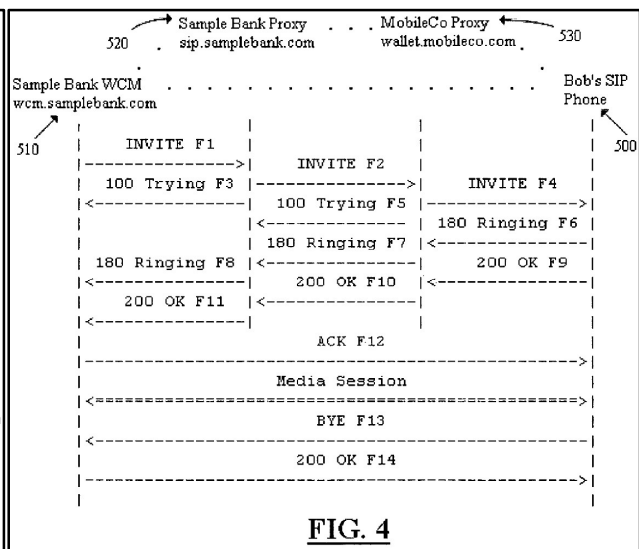
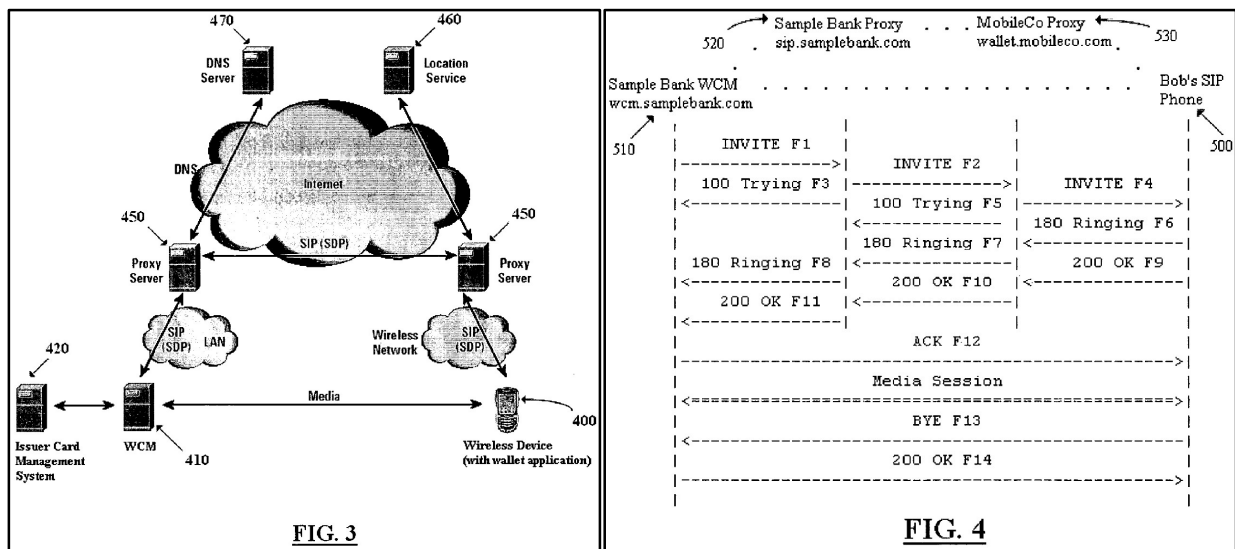
A POSITA would also understand that biometric verification entails a *value... satisfying a threshold criterion*. Or, at a minimum, it would be obvious to

implement Dua’s teaching of “us[ing] a fingerprint... to authenticate a user” in this manner. EX1021 ¶¶[0040]-[0042]; EX1024 ¶¶[0009], [0025]; EX1025 ¶¶[0044], [0086]-[0092]; EX1026 at 196. Biometric verification ensures that a user’s biometrics matches the rightful owner’s biometrics. This entails storing the rightful owner’s biometrics during setup, and then comparing against the user’s biometrics. EX1002 ¶¶182-84. Specifically, a user’s fingerprint is scanned. A set of features are extracted. And a certain number of features must match between the user’s and rightful owner’s fingerprints. The number of matching features sufficient to authenticate the user is the *threshold criterion*. Otherwise, biometric verification would not serve its central purpose.

Patent Owner makes the same mapping. Patent Owner’s infringement contentions asserts that the Accused Products “sen[se,]... using a device-based sensor such as... a fingerprint scanner... a parameter... associated with the... a user of the device,” and “determin[e]... a value of the parameter, such as... a fingerprint... .” EX1016 at 6, 13; EX1002 ¶185.

After a matching fingerprint is sensed (*responsive to... the parameter... satisfying a threshold criterion*), the wallet application is opened to be issued a credit card. EX1002 ¶186 As part of issuance, the issuer’s wireless credential manager (“WCM”) “authenticate[s] the mobile user’s identity in real-time.” Dua ¶[0180]. The authentication process includes “prompting the user for some

cardholder or account holder authentication information,” and the “user would see such a request... within the wallet application screen.” Dua ¶[0180]. The wallet application establishes a Session Initiation Protocol (“SIP”) communication session (*enabling... a number of functions*) between the wireless device and the issuer’s WCM for this authentication process (*enabling... a number of functions*). Dua ¶¶[0046], [0104], [0128], [0178], FIGS. 3 and 4:



Further, Dua discloses how “[d]ata in the wallet application is encrypted and protected with a... PIN... .” Dua ¶[0366]. Therefore, opening the wallet application, such as for credit card issuance, causes the wallet application data to be decrypted (*enabling... a number of functions*) and disables the encryption function for wallet application data (*disabling... a function*). EX1002 ¶187. For instance, if data in the wallet application is encrypted, opening the wallet application and

allowing “[u]sers [to] scroll through... and select credentials” requires the wallet application data to be decrypted. Dua ¶¶[0371]-[0377].

Successfully opening the wallet application also causes security mechanisms tracking authentication attempts to be disabled. EX1002 ¶188. For instance, “[i]f a user keys in... incorrect biometric identification... three consecutive times, the wallet application will not function.” Dua ¶[0441]. A POSITA would understand that providing a valid fingerprint would disable this security subroutine (*disabling... a function*). Or a POSITA would find it obvious to disable this function because, upon receiving a valid fingerprint, the wireless device must wait an indefinite amount of time until the user is prompted again for a fingerprint.

Opening the wallet application also allows a user to change the wallet application’s settings. See Dua ¶¶[0310], [0324]-[0331], [0351], [0366], [0384]; EX1002 ¶189. For instance, PIN-entry to open the wallet application is a “default security setting,” and could be turned off (*disabling... a function*). Dua ¶[0366]. The settings also “allow users to delete extensions” on the wallet application (*disabling... a function*), (Dua ¶[0310].) where “[e]xtensions... ‘extend’ the capability of the wallet platform by enabling a new set of features... .” Dua ¶[0289]. The mobile device has modifiable “hot buttons,” where a “user could use the ‘Wallet Settings’ functionality in the wallet application to link [a] favorite/preferred credit card to [a hot] button,” (*enabling... a number of functions*) including delinking a

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

Alternatively, Patent Owner’s infringement contentions assert that the “*enabling a number of functions*” limitation is met by “unlocking the smartphone or an application.” EX1016 at 20; EX1002 ¶190. And the “*disabling a function of the smartphone*” limitation is met by “disabling the lock function.” EX1016 at 20.

The same disclosure is found in Dua. The wallet application must be opened for credit card issuance. The “default security setting... is that PIN-entry is required before the wallet application can be ‘opened,’” or otherwise “allow the user access to the application.” Dua ¶¶[0366], [0429]. The wallet application is unlocked (*enabling a number of functions*), and the lock function of the wallet application is disabled (*disabling a function of the smartphone*).

External-Storage Theory: Dua discloses an embodiment where the wallet application stores 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]. Because the credentials are stored in external storage, opening the wallet application causes credentials to be retrieved from the external storage for viewing and use. Dua ¶[0495]. Therefore, retrieval of credentials from the external storage is only possible

after performing fingerprint authentication. Dua ¶¶[0353]-[0354], [0366], [0429]; *see also* EX1002 ¶191. As addressed above in connection with the **Card-Issuing Theory**, Dua’s requirement that the user provide a fingerprint for authentication to open the wallet application discloses or at least renders obvious the claimed *sensing... a parameter, determining... a value, and satisfying a threshold criterion*. EX1002 ¶191.

After opening the wallet application, retrieval of credentials requires establishing a connection with the external storage, the wallet application authenticating itself to the external storage, and credential transmission back to the wallet application. Dua ¶¶[0491]-[0492], [0495]. “[W]henver the wallet application is launched[,]... a real-time connection is initiated between the wallet application and... [external] storage” by “utiliz[ing] SIP” (*enabling... a number of functions*). Dua ¶¶[0494]-[0495]; EX1002 ¶192. The “real-time connection” includes “encrypt[ion] [for] all messages between the wallet application and the storage service,” where “[n]ew communication keys can be dynamically generated for each communication session” (*enabling... a number of functions*). Dua ¶¶[0493], [0495].

As addressed above in connection with the **Card-Issuing Theory**, opening the wallet application, such as for viewing and using credentials, causes the wallet application data to be decrypted (*enabling... a number of functions*). EX1002

¶193. Further, when the wallet application uses external storage, the wallet application only holds retrieved credentials and data temporarily. Dua ¶[0495]. The wallet application’s function for encrypting (*see* Dua ¶[0366].) and permanently storing received credentials and data is disabled (*disabling a function of the smartphone*). *See* Dua ¶[0495].

Also as addressed above in connection with the **Card-Issuing Theory**, opening the wallet application via fingerprint authentication also allows a user to change the settings of the wallet application. *See* Dua ¶¶[0310], [0324]-[0331], [0351], [0366], [0384]; EX1002 ¶194. For instance, several settings can be turned off (*disabling... a function*), such as the PIN-entry to open the wallet application (Dua ¶[0366].), “delet[ing] extensions” (Dua ¶[0310].), de-linking credentials from hot buttons (*see* Dua ¶[0392].), and designating a credential for PIN-less use (Dua ¶[0367].).

Similar to the **Card-Issuing Theory**, Dua’s external storage embodiment follows Patent Owner’s contentions. EX1002 ¶195. Patent Owner contends that the “*enabling a number of functions*” and “*disabling a function of the smartphone*” limitations are met by “unlocking the smartphone or an application” and “disabling the lock function,” respectively. EX1016 at 20. In Dua, opening the wallet application via fingerprint authentication causes the wallet application to be

unlocked (*enabling a number of functions*), and the lock function of the wallet application is disabled (*disabling a function of the smartphone*).

(iii) 1[d]

As discussed with limitations 1[a], Dua discloses several possible biometric inputs—a fingerprint, iris, voiceprints, facial recognition, and/or hand geometry (*parameter... sensed using the device-based sensor... compris[ing]... a physiological state*). See Dua ¶¶[0366], [0414], [0534]; EX1002 ¶196.

(iv) 1[e]

Dua discloses wireless device as a *smartphone*—a “handheld device, such as a mobile telephone,” “capable of wirelessly connecting to the internet” and phone applications like a “wallet application.” Dua Abstract, ¶¶[0041], [0049]-[0051], [0287]-[0288], FIGS. 3, 5, 6(a)-8; EX1002 ¶197.

(b) Claim 2

(i) 2[pre]

See Claim 1, *supra*; EX1002 ¶198.

(ii) 2[a]

As discussed with limitation 1[c], Dua discloses enabling one or more (*a number... greater than or equal to one*) functions. EX1002 ¶199.

(c) Claim 3

(i) 3[pre]

See Claim 1, *supra*; EX1002 ¶200.

(ii) 3[a]-[b]

Claim 3 identifies additional steps to be performed after enabling the claimed *number of functions*, as addressed with limitation 1[c]. EX1002 ¶¶ 201-202. The first of these additional steps is *requesting by the device from a second device an authorization to enable a function for conducting a financial transaction by the device*. The second of these additional steps is, *responsive to the requesting, receiving by the device from the second device the authorization to enable the function for conducting the financial transaction*. Dua discloses these two steps under the **Card-Issuing Theory** and **External-Storage Theory**.

Card-Issuing Theory: Dua discloses the wireless device *requesting... from* the issuer's WCM (*second device*) a credential (*e.g.*, credit card) (*authorization to... conduct... a financial transaction*). EX1002 ¶203. Specifically, after opening the wallet application, the "issuer's system will authenticate the... user's identity... to ensure that the [user]... is... the person that requested the digital credential." Dua ¶[0180]. The "authentication process [is]... accomplished by... the issuer system prompting the user for some cardholder... information," where the "user would see such a request for information within the wallet application." Dua ¶[0180]. The credential-issuance request asks for a "special code or PIN that was mailed to the user in advance of the issuance." Dua ¶[0180].

The wireless device's wallet application then sends the "special code or PIN" to the WCM (*requesting by the device from the second device an authorization to enable a function for conducting a financial transaction by the device*). This response is for user authentication, "ensur[ing] that the [user]... is in fact the person that requested the digital credential." Dua ¶[0180]. And "[s]ubsequent to... validating the user's identity[,]" (*responsive to the requesting*) "the WCM 510 will transmit the credential to the wallet application" (*receiving... the authorization to enable the function for conducting the financial transaction*). Dua ¶[0180]; EX1002 ¶¶204-205.

Because the wallet application's response with the "special code or PIN" results in the issued credit card, which is authorization to execute financial transactions with an account, the transmission of the PIN code and reception of the credit card constitutes *requesting* and *receiving... authorization to enable the function for conducting the financial transaction*, respectively. Indeed, in its infringement contentions, Patent Owner asserts that receiving an issued credit card for conducting financial transactions is sufficient to show "requesting an *authorization* to establish a function to conduct a financial transaction." EX1016 at 42,44-46,51-54; EX1002 ¶206.

The wallet application's *request*[] to the WCM occurs *while said number of functions [are] enabled*, where the *enabled* functions are mentioned with the

discussion of limitation 1[c]—establishment of a communication channel with the WCM, authentication process with the WCM, decrypted credentials and wallet application data, and unlocked wallet application. EX1002 ¶207. Because the *request* is submitted over a communication channel between the wireless device and WCM, the *request* is submitted *while* the communication channel and transmission is *enabl[ed]*. Similarly, because the *request* is part of the WCM’s authentication procedures, the wallet application has already *enabl[ed]* the WCM’s authentication subroutine. EX1002 ¶¶208-209.

In order for the user to engage with the authentication subroutine, the user has opened, and is operating within, the wallet application. “PIN-entry is [used] before the wallet application can be ‘opened,’” and the wallet application’s *request* occurs from the user responding to the “issuer system prompting the user” “within the wallet application.” Dua ¶[0180]. Thus for the user to respond to the prompt and submit the request, the wallet application has to be unlocked, and the wallet application data decrypted for the wallet application to be used. EX1002 ¶210.

External-Storage Theory: Dua discloses the wireless device *requesting... from* the external storage (*second device*) a credential (*e.g., credit card*) (*authorization to... conduct... a financial transaction*). EX1002 ¶211. “Whenever the wallet application is launched on the device and a user logs in with his valid PIN, a real-time connection is initiated between the wallet application and the storage

service. The wallet application automatically authenticates itself and gains access to the stored credentials” (*requesting... authorization to enable a function for conducting a financial transaction by the device*). Dua ¶[0495]. The wallet application automatically authenticates itself to the external storage by transmitting a “username/password” associated with the wallet application. Dua ¶[0492]. And access to the storage area allows for requests to retrieve credentials. Dua ¶¶[0491]-[0492], [0495]. From the external storage the “credential information is securely transmitted to the wireless device and temporarily made available for use by the wireless device” (*receiving... the authorization to enable the function for conducting the financial transaction*). Dua ¶[0495].

Because a request to the external storage results in retrieval and allowed use of a credential, this constitutes *requesting* and *receiving... authorization to enable the function for conducting the financial transaction*, respectively. *See also* EX1016 at 42. Indeed, in its infringement contentions, Patent Owner asserts that receiving a credit card for conducting financial transactions is sufficient to establish “request[] an *authorization* to establish a function to conduct a financial transaction.” EX1016 at 42,44-46,51-54; EX1002 ¶212.

The wallet application’s *request*[] to the external storage occurs *while said number of functions [are] enabled*, where the *enabled* functions are mentioned with the discussion of limitation 1[c]—establishment of a communication channel with

the external storage, decrypted wallet application data, and unlocked wallet application. EX1002 ¶213. Because the wallet application “automatically authenticat[ing] itself” to the external storage occurs over a communication channel with the external storage, said *request*[] is submitted *while* the communication channel is *enabl[ed]*. EX1002 ¶214.

Separately, in order for the wallet application to establish a communication channel for automatic authentication, the user has already opened, and operated within, the wallet application. “[W]henver the wallet application is launched... with [a] valid PIN,” the “wallet application automatically authenticates itself [to the external storage] and gains access the stored credentials.” The wallet application is unlocked *while* the wallet application automatically authenticates itself (*requesting... authorization*). EX1002 ¶216.

Further, automatic authentication means transmitting a “username/password” to the external storage. *See* Dua ¶¶[0492], [0495]. Thus, the username/password is data in the wallet application. *See* Dua ¶¶[0492], [0495]. The wallet application also has data regarding “headers for information in storage,” which allows a user to see what credentials are stored and select credentials to retrieve. Dua ¶[0494]. “Data in the wallet application is encrypted and protected with a special wallet PIN set by the wireless device owner... .” Dua ¶[0366]. “The PIN may serve as a decryption key... .” Dua ¶[0399]; *see also* Dua ¶¶[0180], [0366], [0429]. In order to transmit

the username/password, and select credentials to be retrieved, the username/password and header data must be decrypted *while... requesting* retrieval of a credential. Dua ¶[0495]; EX1002 ¶215.

(iii) 3[c]

Limitations 3[a]-[b] discussed *requesting* and *receiving* under the **Card-Issuing Theory** and **External-Storage Theory**. EX1002 ¶217. The *requesting* results in the wallet application *receiving* a credential. Upon receiving the credential (*responsive to the receiving*), the wireless device can use the “credential... to conduct... transactions via... a short range wireless link with a point-of-sale terminal” (*enabling at the device the function for conducting the financial transaction*). Dua Abstract.

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

credential is issued to the wallet application (*responsive to receiving the authorization, enabling... the function for conducting the financial transaction*).

EX1002 ¶218.

External-Storage Theory: Credentials retrieved from external storage are used by the wallet application to conduct financial transactions. A retrieved “credential... is... temporarily made available for use by the device’s RFID interface.” Dua ¶[0495]. In other words, after retrieving the credential (*responsive to receiving the authorization*), the functionalities for transmitting the credential—a wireless device’s “integrated RFID chip” and NFC implementations—to a POS terminal are *enabl[ed]* (*enabling... the function for conducting the financial transaction*). Dua Abstract, ¶[0495]; EX1002 ¶219.

(d) Claim 4

(i) 4[pre]

See Claim 3, *supra*; EX1002 ¶220.

(ii) 4[a]

Claim 4 continues to build on claim 3, which in turn builds on claim 1. Thus, claim 1 recites steps for enabling the claimed *number of functions*, claim 3 recites steps for using those functions to enable a *function for conducting a financial transaction*, and claim 4 then recites steps for engaging in a financial transaction. Engaging in this financial transaction requires two prerequisites—*satisfying a*

proximity condition relative to an entity; and *sensing the parameter... satisfies the threshold criterion*—before finally *paying for a product*. EX1002 ¶221.

Satisfying a proximity condition: Dua discloses the wireless device using a “credential... to conduct... transactions via... a short range wireless link with a point-of-sale terminal” (*conducting by the device the financial transaction*). The short-range wireless link is created through communications by the wireless device’s “integrated RFID chip” and using the Near-Field-Communications (“NFC”) protocol (*using by the device the function of conducting the financial transaction*). Dua ¶¶[0016], [0315].

Establishing and using the short-range wireless link to execute the transaction is *responsive to the device satisfying a proximity condition relative to* the POS terminal. EX1002 ¶¶222-23. Because the short range wireless link between the wireless device and point-of-sale reader includes NFC, the connection and subsequent transaction only occurs if (*responsive to*) the wireless device is in “close proximity” to the point-of-sale terminal and can thus detect its NFC communications (*the device satisfying a proximity condition relative to an entity*). Dua Abstract, ¶¶[0016], [0318]. NFC and other short range wireless communication protocols are only effective if there is an underlying signal of sufficient strength such that the device and the terminal can communicate using that protocol. EX1002 ¶¶223-28. Signal strength attenuates with increasing distance. EX1002 ¶¶223-24. Indeed, in

its infringement contentions in the district court litigation, patent owner also asserts use of short range communications—specifically, use of NFC—is sufficient to show *the device satisfying a proximity condition relative to an entity*. EX1016 at 61, 316-17. Thus, when Dua is able to communicate with the POS terminal using NFC, the wireless device has *detected that a proximity condition is satisfied* (e.g., Dua Abstract, ¶¶[0041], [0314]-[0315], [0382], [0395]) by receiving and decoding a short-range NFC signal from the POS device.

In addition, it would be obvious to a POSITA that Dua’s wireless device would detect proximity to the POS terminal based on a signal from the POS terminal. Dua’s wireless device has to establish a peer-to-peer communication session with the POS terminal over NFC. Dua ¶[0016], Claims 33,36,50. Dua contemplates NFC communication sessions transferring a significant amount of data, such as encryption keys and several credentials, “requir[ing] the user to hold the wireless device in front of the reader for a longer period of time while the processing... takes place.” Dua ¶[0359]. As explained by Dua, the smartphome and POS communicate using short range signals, such as near-field communication (NFC) or proximity signals. *See* Dua Abstract, ¶¶[0016], [0041], [0314]-[0315], [0382], [0395]. Short-range signal communications are dependent on proximity between the two devices communicating. EX1002 ¶¶224-25. To ensure communications will be successful and not just wasted signals and wasted user time, Dua’s wireless device first needs

to detect it is near the POS prior to proceeding with a payment transaction with the POS device. In addition, transmitting sensitive financial information when there is no bona fide POS in proximity poses a security risk. As such, it would have been obvious for a POSITA to configure the smartphone to first detect that it is proximate to Dua's POS device prior to attempting short-range signal communication to prevent the error condition of a smartphone sending short-range signals with a POS device that is too far or to the wrong device, *e.g.* a fraudulent device. EX1002 ¶¶226-28. Indeed, such implementations were well-known to a POSITA. EX1020 ¶¶[0041], [0063], [0073].

Sensing the parameter: As discussed with limitations 1[a]-[c], Dua discloses fingerprint authentication to open the wallet application under the **Card-Issuing Theory** and **External-Storage Theory** as *sensing, determining, and satisfying a threshold criterion*. EX1002 ¶¶229-30. Because the fingerprint authentication to open wallet application for card issuance or credential retrieval under the **Card-Issuing Theory** or **External-Storage Theory**, respectively, is a prerequisite to later navigating, selecting, and using the issued or retrieved credentials, (*See* Dua ¶¶[0371], [0378], [0384].) fingerprint authentication is also a prerequisite to the wallet application establishing an NFC connection and executing transactions with a POS terminal (*responsive to the device sensing the parameter and determining*

the value that is associated with parameter that is sensed satisfies the threshold criterion).

Even if the claims require an additional transaction-specific *sensing*, *determining*, and *satisfying*. EX1002 ¶231. Dua discloses this. Dua discloses that transactions can be made after a valid fingerprint. The “default security setting in the wallet application is that PIN-entry is required before” (*responsive to*) “any credentials [are] transmitted to an external device,” including “inputting a PIN before RF communication can be enabled,” such as for an NFC connection and transaction with a POS terminal. Dua Abstract, ¶¶[0366], [0395]; *see also* Dua ¶¶[0368], [0377]. PINs can be replaced with fingerprints. Dua ¶¶[0366], [0414], [0414].

Paying for a product: Dua discloses the wireless device using a “credential... to conduct... transactions via... a short range wireless link with a point-of-sale terminal” (*conducting... the financial transaction*). EX1002 ¶¶231-32. The executed transaction entails *paying for a product*, such as groceries or train tickets. *See* Dua ¶¶[0352]-[0353].

The short-range wireless link is created through communications by the wireless device’s “integrated RFID chip” and using the Near-Field-Communications (“NFC”) protocol (*using... the function of conducting the financial transaction*), which makes the transaction *responsive to the* wireless device being within

proximity relative to the POS terminal, as discussed above. Dua ¶¶[0016], [0315]. EX1002 ¶233. Further, the short range wireless link only occurs after the fingerprint authentication process (*responsive to the... parameter... satisf[ying] the threshold criterion*), also discussed above.

(e) **Claim 5**

(i) **5[pre]**

See Claim 3, *supra*; EX1002 ¶234.

(ii) **5[a]**

Card-Issuing Theory: After card issuance, Dua discloses the issuer’s WCM (*second device*) “authentica[ting] a mobile user’s identity in real-time during a transaction.” Dua ¶¶[0180], [0250]; EX1002 ¶¶235-36. “[I]ssuers may issue a credential to a wireless device, require the wallet PIN with every transaction, but also prompt the user for an issuer PIN” either on the POS terminal or wallet application. Dua ¶[0402]. One “type of PIN verification scheme” includes over-the-air or “OTA PIN verification,” where the “WCM... can... handle over-the-air PIN verification for electronic credentials... .” Dua ¶¶[0404], [0406].

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

“WCM... is used to deliver a PIN request to [the] wireless device... and to receive a user-input response from [the] wireless device.” Dua ¶[0405]. Because the authorization for the transaction is withheld until the “PIN... validation,” and because the “WCM... deliver[s] [the] PIN request... and... receive[s] [the] user-input response,” the WCM’s over-the-air PIN verification is *a function for conducting the financial transaction*. EX1002 ¶237.

Additionally, an account must have “OTA PIN verification turned on” (*enabling... a function*), (Dua ¶[0406].) which occurs with credential issuance to a wallet application. See Dua ¶¶[0406], [0408], [0413]; EX1002 ¶238.. Issued “credential[s]... [are] labeled by an issuer as using over-the-air... PIN verification credential issuance.” Dua ¶[0413]. In order to label an issued credential as such, “[t]here must be a valid E.164 mobile phone number in the account record in order to enable OTA PIN verification,” (Dua ¶[0408].) where an E.164 phone number is previously provided through the wireless device. See Dua ¶[0056].

External-Storage Theory: Dua discloses the wireless device setting up the external storage to store and provide access to credentials and transaction receipts. “[T]he wallet application registers an external wallet storage service as an ‘extension’ within the wallet application on the wireless device.” Dua ¶[0491]. For instance, “[d]uring the storage setup process, the storage server will establish a valid username/password for the wallet application to automatically access the storage

area.” Dua ¶[0492]. Then, “[t]he user is then free to use the wallet menu to select stored credentials or profiles to facilitate a transaction” (*function for conducting the financial transaction*). Dua ¶[0495]. Further, “even electronic receipts... are stored in the external storage service, and made available for use by the wireless device” (*function for conducting the financial transaction*). Dua ¶[0495]. Because providing access to credentials used in transactions and because executing a transaction includes receiving and storing receipts, setting up the external storage for the wallet application *enabl[es]... function[s] for conducting... financial transaction[s]*. EX1002 ¶239.

(f) Claims 6-16

Claims 6-16 are substantively identical to claims 1-5. Claims 6-10 are directed to “[a] device that is configured to perform operations,” whereas claims 1-5 are directed to “[a] method of operating a device.” This distinction is immaterial since Dua discloses both methods and systems. Dua Title; EX1002 ¶240.

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

directed to a “wireless device,” and discloses both methods and systems. Dua Title, Abstract; EX1002 ¶241.

(g) Claim 17

(i) 17[pre]

See Claim 14, *supra*; EX1002 ¶242.

(ii) 17[a]

Dua discloses the wireless device *establishing* “*a short range wireless link with [a]*” point-of-sale terminal (*entity*) for “conduct[ing] [a]... transaction,” such as *paying for a product*. Dua Abstract, ¶¶[0352]-[0353]. “The wallet application... support[s] peer-to-peer connectivity to a device in close proximity,” such as “[c]onnectivity between the wireless device and... POS terminal.” Dua ¶[0318]. And “[c]onnectivity could initially be established by exchanging encryption key” (*establishing by the wireless device a short range wireless link*). Dua ¶[0318]; EX1002 ¶243.

Similar to Jain, Dua’s wireless device and POS terminal communicate over an NFC connection, which establishes a wireless link. *See supra*, Section VIII.A.2.g. Patent Owner agrees that the use of NFC is sufficient to show *establishing... a short-range wireless link*. EX1016 at 309-10.

(iii) 17[b]-[d]

Dua discloses a wireless device *wirelessly transmitting* credential *information* to a point-of-sale terminal (*entity*). Dua Abstract, ¶¶[0352]-[0353]. In

response, the point-of-sale terminal transmits to the wireless device an indication of a “successful transmission of credentials to [the] reader” after a transaction is complete (*wirelessly receiving information from the entity*). Dua ¶¶[0364]-[0365]; *see also* Dua ¶¶[0015], [0041], [0293]. The transmission between the wireless device and point-of-sale terminal is done with short range wireless communication, including NFC and Bluetooth (*using unlicensed frequencies and time domain duplex protocol*). Dua Abstract, ¶¶[0016], [0318]; EX1002 ¶¶244-49.

NFC uses unlicensed frequencies, such as the 13.56 MHz ISM band. EX1002 ¶¶244-49. Patent Owner, in its infringement contentions, admits as much, alleging that NFC *us[es] unlicensed frequencies and time domain duplex protocol*. EX1016 at 310-13; EX1002 ¶¶244-49. Bluetooth also *us[es] unlicensed frequencies and a time domain duplex protocol*. A POSITA would have known these things too. *See* EX1032 at 21 (describing NFC as a “half... duplex system”); EX1002 ¶¶244-49.

(iv) 17[e]

As discussed with limitations 17[pre]-[a], Dua discloses or renders obvious that *paying for a product comprises establishing... a short-range wireless link*. As discussed with limitation 4[a], Dua discloses or renders obvious that *paying for a product*, including *establishing* an NFC connection between the wireless device and POS terminal, is *responsive to the device satisfying a proximity condition relative*

to an entity and responsive to the device sensing the parameter... satisfies the threshold criterion. EX1002 ¶250.

(h) Claim 18

(i) 18[pre]

See Claim 14, *supra*; EX1002 ¶251.

(ii) 18[a]

Limitation 18[a] repeats language found in claim 14, also found in limitations 3[a]-[c] and addressed above. EX1002 ¶252.

(iii) 18[b]

Dua discloses the wireless device establishing connections with the WCM and external storage through SIP. “The... SIP architecture... establish[es] direct communication between... WCM and wallet application... for... transferring... credentials” (*establishing by the wireless device a link with the second device*). Dua ¶¶[0128], [0178], FIGS. 3-4. A “real-time connection is initiated between the wallet application and the storage service” by “utiliz[ing] SIP” (*establishing by the wireless device a link with the second device*). Dua ¶¶[0494]-[0495]. A SIP-established connection can entail servers and various communication protocols such as cellular wireless technology (*e.g.*, “2.5G” and “3G”) and “Wi-Fi” (*wireless link*). Dua ¶[0104], FIG 3. These connections occur over a greater distance than the “short range wireless link” established with NFC (*distance that is greater than a distance associated with the proximity condition*). EX1002 ¶¶253-54.

(iv) 18[c]-[d]

As discussed with limitation 18[b], Dua discloses the wireless device communicating with the WCM and external storage using cellular wireless technology (*e.g.*, “2.5G” and “3G”) and “Wi-Fi,” including card-issuance/automatic authentication procedures (*wirelessly transmitting information to the second device over said wireless link*) and receiving credentials (*wirelessly receiving information from the second device over said wireless link*). See Dua ¶¶[0104], [0495]. Cellular wireless technology 2.5G, 3G, and WiFi *us[e] unlicensed and/or licensed frequencies*. EX1002 ¶255.

(v) 18[e]

As discussed with limitations 18[c]-[d], Dua discloses the wireless device using Wi-Fi or cellular technology to communicate with the WCM and external storage, including “GSM/GPRS, CDMA2000, W-CDMA, EDGE, HDR, 1xRTT, UMTS, IMT-2000, 802.11a, 802.11b, 802.11g... or other relevant protocols developed hereinafter.” Dua ¶¶[0041], [0104]. WiFi protocols “802.11a” and “802.11g” *us[e]... orthogonal frequency division multiplexing*. Dua ¶[0041]; EX1002 ¶256; EX1043; EX1044.

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

to the 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 '756 patent, were known to a POSITA to be in line to displace older technologies in the near future. EX1002 ¶257; EX1045; EX1046. Wi-Max and LTE *us[e]... orthogonal frequency division multiplexing and/or orthogonal frequency division multiple access protocol*. EX1002 ¶257.

(vi) 18[f]

As discussed with limitation 1[c], Dua discloses *establishing the link with the second device responsive to... the parameter... satisf[ying] the threshold criterion*.

Under the **Card-Issuing Theory** and **External-Storage Theory**, scanning a valid fingerprint causes the wireless device to open the wallet application and establish a connection with WCM and external storage, respectively. EX1002 ¶¶258-59.

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 '756 patent. EX1002 ¶¶260-61. Additionally, there was no long felt, unresolved need met by the '756 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 ¶262. Further, the vast number of contactless payment systems and trials of those systems before the '756 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. Even if any secondary factors weighing in favor of non-obviousness did exist, they do overcome the strength of the obviousness analysis. *See* EX1002 ¶¶261-262.

IX. STIPULATION

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

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

Simply put, if the review is instituted, Petitioner does not at this time intend to present prior art invalidity based on patents or printed publications (beyond as evidence of operation of system prior art) in district court and instead intends to go to trial based on system prior art, including the system prior art described above in Section IV ("State of the Art"). However, district court litigation is still in its early stages, Petitioner has not yet received all documents responsive to subpoenas issued to the companies responsible for the prior art systems, and Patent Owner has not yet

fully disclosed its validity contentions. As such, Petitioner cannot at this time exclude the possibility that it may rely on patents or printed publications that are not the basis of the Grounds set forth herein to address discrete gaps in its discovery into prior art systems (*e.g.*, if Petitioner is unable to obtain discovery into how Kyocera implemented biometric verification, it may need to rely on printed publications to render those limitations obvious). But aside from this minor reservation of rights pertaining to secondary references, Petitioner intends to bifurcate its invalidity case: invalidity grounds based on patents and printed publications will be litigated in this IPR, and invalidity grounds based on prior art systems will be litigated in district court.

X. CONCLUSION

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

Date: May 23, 2025

Respectfully submitted,

By: /s/ James Glass

James M. Glass

Counsel for Petitioner

CERTIFICATION UNDER 37 C.F.R. § 42.24

Under the provisions of 37 C.F.R. § 42.24, the undersigned hereby certifies that the word count for the foregoing Petition for *inter partes* review (excluding the table of contents, table of authorities, mandatory notices, certificate of service or word count, and appendix of exhibits or claim listing) totals 13,559 words, which is within the word limit allowed under 37 C.F.R. § 42.24(a)(i).

Date: May 23, 2025

/s/ James Glass

James Glass (Reg. No. 46729)

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 42.6(e), 42.105(a), the undersigned hereby certifies service on the PO of a copy of this Petition and its respective exhibits at the official correspondence address for the attorneys of record for the '756 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 23, 2025

/s/ James Glass

James Glass (Reg. No. 46729)