

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. IPR2025-00973

U.S. Patent No. 9,462,411

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 9,462,411**

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. MANDATORY NOTICES AND FEES	2
A. Real Party-In-Interest	2
B. Related Matters.....	2
C. Counsel and Service Information	2
D. Payment of Fees	3
E. Requirements for Inter Partes Review	3
III. GROUNDS	3
IV. BACKGROUND	3
A. State of the Art	3
V. '411 PATENT	6
A. Priority Date	6
B. '411 Patent Specification	6
C. Prosecution History (EX1005)	8
VI. PERSON OF ORDINARY SKILL	9
VII. CLAIM CONSTRUCTION	9
VIII. GROUNDS	9
A. Ground 1: Jain (EX1017)	9
1. Background	9
2. Analysis.....	13
B. Ground 2: Dua (EX1018).....	41
1. Background	41
2. Analysis.....	43
C. Secondary Considerations	65
IX. STIPULATION	66
X. CONCLUSION.....	67

EXHIBIT LIST

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

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

EX1034	Near Field Communication - Interface and Protocol (NFCIP-1), Standard ECMA-340 (December 2002)
EX1035	NFC Forum News Conference, NFC Forum (June 5, 2006)
EX1036	Dean A. Gratton, “Developing Practical Wireless Applications”, Elsevier Digital Press (2007)
EX1037	Jacki Katzman, “NFC Forum Unveils Technology Architecture and Announces Initial Specifications and Mandatory Tag Format Support”, NFC Forum, at 3 (June 5, 2006)
EX1038	Exhibit Intentionally Omitted
EX1039	U.S. Pub. No. 2010/0082445
EX1040	Exhibit Intentionally Omitted
EX1041	Exhibit Intentionally Omitted
EX1042	“iPhone Premieres This Friday Night at Apple Retail Stores”, Apple (Jun. 28, 2007), https://www.apple.com/newsroom/2007/06/28iPhone-Premieres-This-Friday-Night-at-Apple-Retail-Stores/
EX1043	Exhibit Intentionally Omitted
EX1044	Exhibit Intentionally Omitted
EX1045	Exhibit Intentionally Omitted
EX1046	Exhibit Intentionally Omitted
EX1047	Near Field Communication - Interface and Protocol (NFCIP-1), Standard ECMA-340 (2nd Edition, December 2004)

LIST OF CHALLENGED CLAIMS

Claim	Limitation
1[pre]	A method comprising:
1[a]	sensing by a smartphone, using a smartphone-based sensor, physiological data associated with a living organism;
1[b]	detecting that a proximity criterion is satisfied between the smartphone and an entity, wherein the entity is not the living organism;
1[c]	selectively communicating by the smartphone using a first air interface of a plurality of air interfaces with which the smartphone is capable of communicating, responsive to the proximity criterion having been detected as being satisfied and responsive to a value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor;
1[d]	refraining from communicating by the smartphone using the first air interface absent said value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor satisfying a criterion, even though the proximity criterion is detected as being satisfied;
1[e]	selectively sending information by the smartphone to one or more other devices and receiving information by the smartphone from the one or more other devices responsive to said value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor satisfying the criterion; and
1[f]	communicating by the smartphone using a second air interface of the plurality of air interfaces with which the smartphone is capable of communicating that differs from the first air interface.
2[pre]	The method according to claim 1, wherein said detecting that a proximity criterion is satisfied between the smartphone and an entity comprises:
2[a]	detecting that a proximity criterion of less than 10 meters in distance is satisfied between the smartphone and the entity;

Claim	Limitation
2[b]	wherein the detecting is performed by the smartphone, by a device that is associated with the entity, by a system that is associated with the smartphone, or a combination thereof.
3[pre]	A smartphone comprising:
3[a]	a processor that is configured to control the smartphone to perform operations comprising:
3[b]	sensing, using a smartphone-based sensor, physiological data associated with a living organism;
3[c]	detecting that a proximity criterion is satisfied between the smartphone and an entity, wherein the entity is not the living organism;
3[d]	selectively communicating using a first air interface of a plurality of air interfaces with which the smartphone is capable of communicating, responsive to the proximity criterion having been detected as being satisfied and responsive to a value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor;
3[e]	refraining from communicating using the first air interface absent said value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor satisfying a criterion, even though the proximity criterion is detected as being satisfied;
3[f]	selectively sending information to one or more other devices and receiving information from the one or more other devices responsive to said value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor satisfying the criterion; and
3[g]	communicating using a second air interface of the plurality of air interfaces with which the smartphone is capable of communicating that differs from the first air interface.

Claim	Limitation
4[pre]	The smartphone according to claim 3, wherein said detecting that a proximity criterion is satisfied between the smartphone and an entity comprises:
4[a]	detecting that a proximity criterion of less than 10 meters in distance is satisfied between the smartphone and the entity.

I. INTRODUCTION

The '411 patent is directed to a smartphone and method for enabling a smartphone to communicate with another device over an air interface based on having satisfied a proximity criterion (*i.e.*, the smartphone is within a certain physical distance from the other device) and sensing some other parameter such as physiological data (*e.g.*, “a blood pressure, a heart rate, a blood content, a physiological state” as disclosed in the specification—*see* EX1001 at 6:4-9).

Patent Owner (“PO”) has broadly interpreted its claims to encompass biometrically secured smartphones that communicate with a payment terminal via NFC to perform a financial transaction. The '411 patent does not, however, disclose any non-obvious technology for performing such transactions. Indeed, using existing cell-phone technology to conduct financial transactions was the subject of intense growth during the early 2000s, with pilot programs and commercial deployments by companies including Nokia, Motorola, Kyocera, and NTT. And short-range wireless communications technologies, such as NFC, had also been developed specifically for use in such applications. The necessary building blocks for mobile payment were not developed by PO; they already existed and were in use. Prior artists had also recognized the need for securing mobile transactions and, thus, taught the use of biometric authentication to avoid unauthorized transactions. PO was not the first to invent any of these building blocks or any of the specific

combinations claimed in the '411 patent. The technology was mature enough to be the subject of multiple patent publications from this timeframe, including the prior art Jain and Dua references relied upon in this Petition.

II. MANDATORY NOTICES AND FEES

A. Real Party-In-Interest

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

B. Related Matters

The '411 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 '411 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 '411 patent is the parent of numerous continuations that led to issued U.S. Patent Nos. 9,832,708, 10,219,199, 10,674,432, 11,770,756, 11,924,743, 11,937,172, and 12,028,793, all also asserted against Petitioner. Petitioner is in the process of filing IPR petitions against these family members.

C. Counsel and Service Information

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

LEAD COUNSEL	BACK-UP COUNSEL
James M. Glass (Reg. No. 46,729) jimglass@quinnemanuel.com QUINN EMANUEL URQUHART & SULLIVAN, LLP 51 Madison Avenue, 22 nd Floor New York, NY 10010 Tel: (212) 849-7000	Ognjen Zivojnovic (Reg. No. 69,516) ogizivojnovic@quinnemanuel.com Benjamin Kleinman (Reg. No. 66,856) benjaminkleinman@quinnemanuel.com QUINN EMANUEL URQUHART & SULLIVAN, LLP 50 California Street, 22nd Floor San Francisco, California 94111 Tel: (415) 875-6600

D. Payment of Fees

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

E. Requirements for Inter Partes Review

Petitioner certifies that the '411 patent is available for *inter partes* review, that Petitioner is not barred or estopped, and that 35 U.S.C. §§315(a)-(b) is inapplicable.

III. GROUNDS

Ground	Basis	Reference	Claims
1	§103	Jain (U.S. Pat. Appl. Pub. No. 2009/0069049)	1-4
2	§103	Dua (U.S. Pat. Appl. Pub. No. 2006/0165060)	1-4

IV. BACKGROUND

A. State of the Art

As the '411 patent recognizes, mobile phones could communicate using a variety of wireless protocols and frequencies that were well known prior to the alleged invention in late 2008. EX1001 at 1:35-61. Indeed, the market for mobile

phones capable of cellular communications was well-established by the 1990s, with the Nokia 3210 released in 1999 eventually selling over 160 million units. EX1002 ¶81. 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. *Id.* So too were phones with Bluetooth capabilities, such as the Nokia 6310 and, again, the Samsung SCH-i730. *Id.*

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 ¶82. 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. *Id.*

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 ¶83. This technology soon spread to the United States, with mobile phone and payment companies teaming up to conduct pilot programs of their own mobile payment software, including a 2006 pilot by Nokia and

MasterCard, a 2007 pilot program by Motorola and Discover, and a 2007 pilot by Kyocera and MasterCard, with companies such as ViVOtech releasing full mobile payment solutions. *See id.*; *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 ¶84. 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 ¶¶84. For example, the mobile phones used for mobile payments in the 2007 Kyocera and MasterCard trial included fingerprint scanners and required biometric authentication. EX1002 ¶¶84; *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. '411 PATENT

A. Priority Date

The '411 patent was filed November 4, 2008, as U.S. Patent Application No. 12/264,711, and does not claim any earlier priority.

B. '411 Patent Specification

The specification assumes familiarity with a “wireless communications device” such as “a wireless terminal, a wireless/mobile phone, a Personal Digital Assistant (PDA), a smart phone, a multi-media device including Global Positioning System (GPS) capability, etc.” EX1001 at 2:60-64; *id.* at 1:35-50. It relies on long-established, generic concepts of computer systems such as “authorization” (5:26-28 et seq.), “sensors” capable of detecting, *inter alia*, physiological input (mentioned only at 5:65-6:9), “short-range communications” (mentioned in the specification only at 8:14-19 and 8:41-50), “air interface[s]” (6:36-52 et seq., with a recitation of then-existing interfaces at 7:3-13), and “communications service[s]” (8:64-66 et seq.). The specification acknowledges that the “adaptivity and mobility aspects of

wireless communications” were already “important in people’s lives” at the time of alleged invention. EX1001 at 1:15-16. It also assumes that mobile phones could act as digital wallets. EX1001 at 1:24-27. The specification does not disclose or purport to disclose new or improved means of sensing (including physiological/biometric sensing) or proximity detection.

The '411 specification describes a “mobile subscriber device” (element 14 in '411 patent Figure 1) that “may be configured to enable one or more modes/functions” of itself or of another device “responsive to a proximity criterion having been satisfied.” EX1001 at 2:60-3:2. The proximity criterion is a measure of how close the wireless device (or the second device) is to an “entity” such as a person, product for sale, or POS terminal. EX1001 at 3:3-17, 3:31-39.

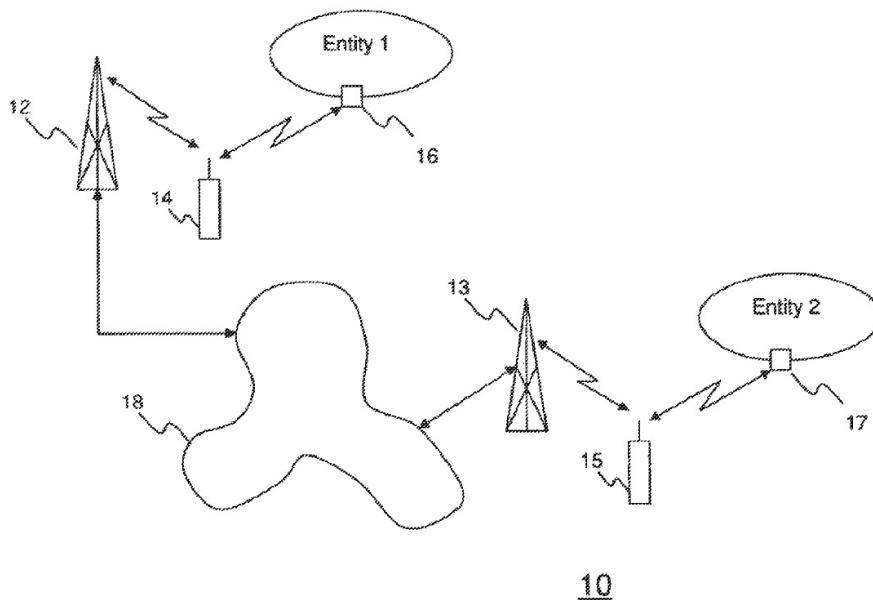


FIG. 1

C. Prosecution History (EX1005)

In prosecution, the Examiner rejected the claims of the '411 patent nine times, primarily on obviousness grounds. EX1005 at 74, 127, 197, 240, 295, 330, 382, 420, 453. Accordingly, the claims were amended substantially including through a final Examiner's Amendment for allowance. EX1005 at 108, 166, 220, 266, 316, 351, 407, 434, 498. Many of the Examiner's rejections were based on the overbroad nature of Applicants' claims. Indeed, even the Applicants acknowledged "the claims are broad" but attempted to excuse the overbreadth by noting "that their filing date of November 4, 2008 is quite early relative to the claimed invention." EX1005 at 410. As evident from the state of the art and Grounds raised herein, November 2008 was far from being "quite early relative to the claimed invention."

Tellingly, Applicants argued for allowance of the claims based on claim 1's sensing of physiological data, only narrowly distinguishing the cited art by arguing that a prior art fingerprint sensor was not "smartphone-based." EX1005 at 484. Applicants also traversed the Examiner's rejections by arguing "the combination of NFC transceiver plus biometric finger sensor did not yet exist in a mobile phone at the time of filing of [U.S. Pub. No. 2007/0197261 ('Humbel')]." EX1005 at 483. Again, these assertions are provably false in view of the state of the art and Grounds presented herein.

VI. PERSON OF ORDINARY SKILL

A person of ordinary skill in the art at the time of the '411 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 ¶74.

Petitioner's expert, Dr. Almeroth, exceeded this level by the priority date. *Id.* ¶75.

VII. CLAIM CONSTRUCTION

No express constructions are required to find the '411 patent claims invalid. To the extent relevant, Petitioner addresses the plain meaning of certain terms in the analysis for the presented Grounds.

VIII. GROUNDS

A. Ground 1: Jain (EX1017)

1. Background

Jain is prior art under at least pre-AIA 35 U.S.C. § 102(e), having been filed Sep. 5, 2008 and thus before the earliest effective filing date of the '411 patent. Jain discloses all limitations of the '411 patent claims, but Petitioner presents Jain as an obviousness reference in the event Patent Owner argues there are any differences between Jain and the '411 patent claims.

Jain was not considered by the Examiner during prosecution of the '411

patent. *See* EX1002 ¶85.

'411 patent claim 1 recites a set of steps for a smartphone to communicate with other devices when within a certain proximity to an entity and sensing physiological data associated with a living organism. These steps roughly consist of (1) sensing physiological data associated with a living organism (*e.g.*, a user of the smartphone); (2) detecting if the smartphone is in the proximity of some other entity that is not the living organism (*e.g.*, a “store” or “check-out counter in a store”); (3) selectively communicating information to another device (*e.g.*, a payment terminal) if both of the foregoing criterion are met while also refraining from communicating if they are not; and (4) also communicating over a separate “air interface” (*e.g.*, cellular or Wi-Fi).

Jain discloses all of these steps in the context of its systems and methods for, *inter alia*, using a mobile device to “wirelessly execute[] financial transactions with a retail terminal” as illustrated in Fig. 1, below, for example. Jain, ¶¶[0005], [0018]-[0020]; *see also* EX1002 at ¶¶86-91.

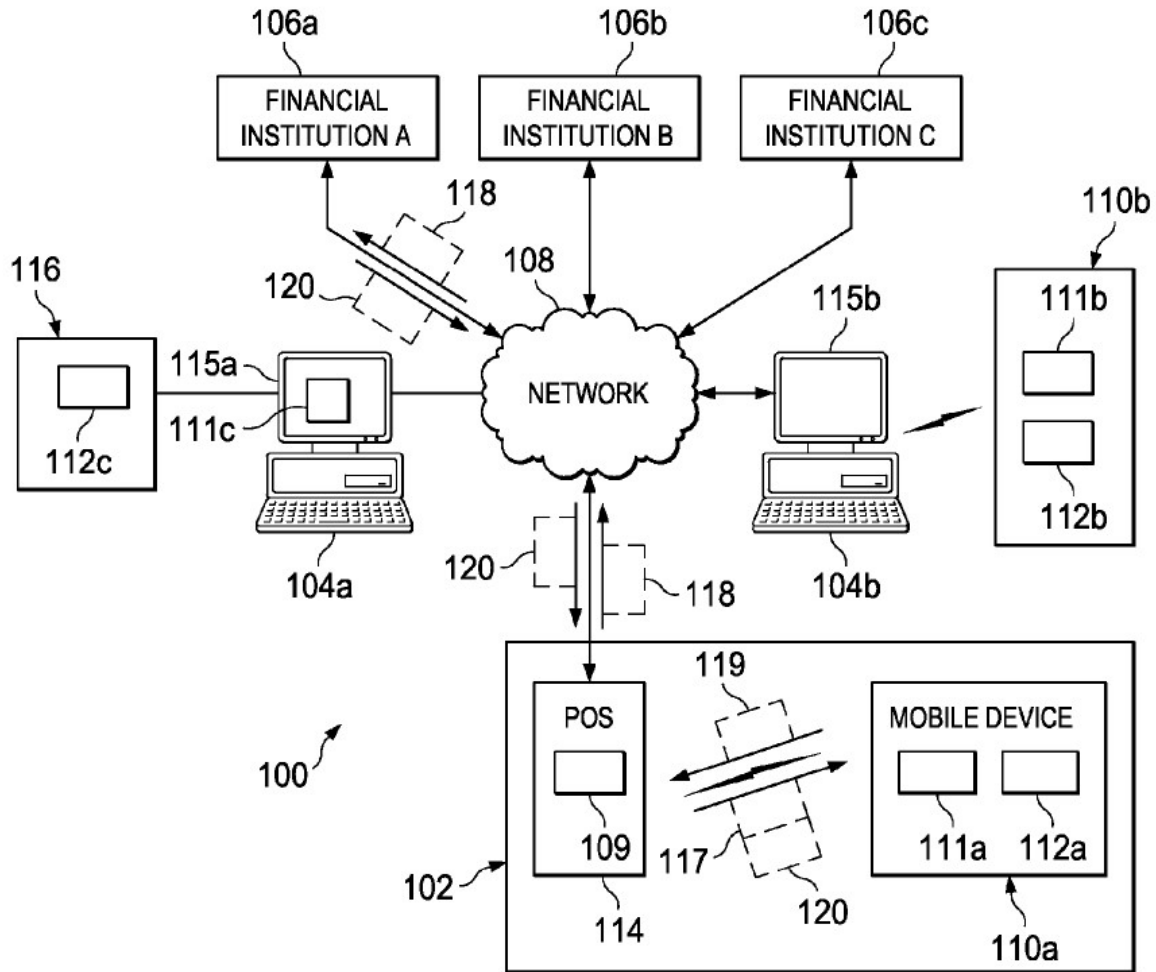


FIG. 1

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

device [110a¹] having a transaction card 112a and a Point of Sale (POS) device 114 that executes transactions with customers.”), Fig. 1 (showing transaction card 112a within mobile device 110a). Jain also describes various methods for activating transaction card 112. *See, e.g.*, Jain Fig. 9, ¶¶[0080]-[0081].

Mobile device 110 may thereafter conduct financial transactions via the same sequence of steps claimed as novel by the '411 patent—*i.e.*: (1) detecting if the mobile device is sufficiently close to a POS terminal to send and receive transaction requests and responses via a short-range NFC signal (*e.g.*, transmissions 117, 119, and 120 in Fig. 1—Jain ¶¶[0023], [0027]); (2) sensing presence of a living organism by prompting the user to authenticate themselves (*e.g.*, by touching a touch screen to input a PIN or through biometrics, such as a fingerprint scan, ¶[0075]), either as part of the claimed first step of setting up the transaction card 112 with mobile device 110 (*e.g.*, Fig. 7B, steps 734-742) or again for individual transactions (*e.g.*, ¶[0029]); and (3) if both conditions are met, communicating with a point-of-sale terminal by sending and receiving transaction requests and responses (*e.g.*, 117, 119, and 120 in Fig. 1) containing information associated with the transaction (*e.g.*, ¶[0027]). Jain also discloses the mobile device 110 having transaction card 112 may separately communicate with financial institutions 106 over a cellular network—not NFC—

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

when “not proximate a retail device, such as the POS device 114 of FIG. 1” (¶[0041]).

2. Analysis

(a) Claim 1

(i) 1[pre]: A method comprising:

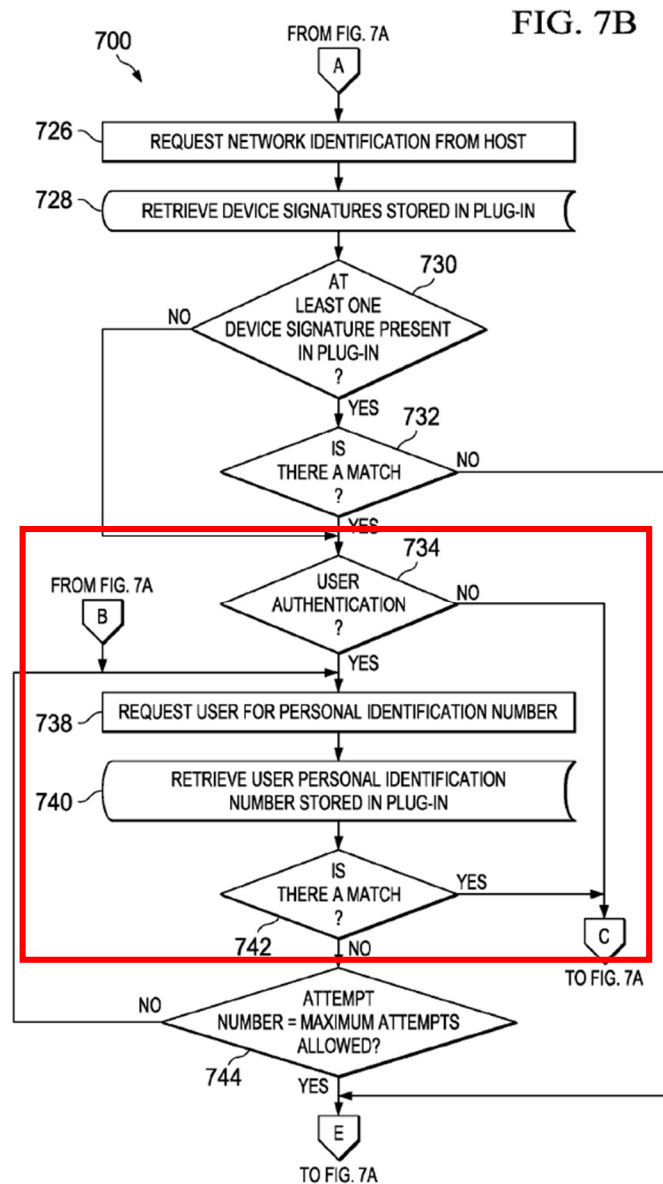
Jain describes a method comprising the steps in the remaining limitations of claim 1. *See infra; see also* Jain at Abstract (“The present disclosure is directed to a system *and method* for interfacing transaction cards with mobile devices. In some implementations, *a method* includes . . .”).

(ii) 1[a]: sensing by a smartphone, using a smartphone-based sensor, physiological data associated with a living organism;

Jain describes at least two scenarios in which physiological data associated with a living organism (*e.g.*, a user of mobile device 110) is sensed by a smartphone-based sensor.

First, before Jain’s mobile device 110 (*e.g.*, “a smartphone” (¶[0018])) can engage in financial transactions it must interface with transaction card 112. Accordingly, Jain discloses a process for “automatically bootstrapping” transaction card 112 to mobile device 110, which includes authenticating a user using a PIN or biometric data (*e.g.*, fingerprint). Jain ¶¶[0072], [0075], Fig. 7B at steps 734-742 (annotated); *see also id.* ¶[0065] (“the CPU 408 may execute one or more authentication processes prior to activating the intelligent card 400 and/or antenna

402 as illustrated in FIG. 7”), ¶[0066] (disclosing user authentication techniques), ¶[0070] (explaining users may add “user authentication” such as through “self-select[ed] PIN authentication to prevent unauthorized use”), Table 1 (“The user can also optionally select a PIN (change Antenna availability to user authentication)”); EX1002 ¶¶94-95.



At step 738, the smartphone requests and receives a user-inputted PIN (*sensing . . . physiological data associated with a living organism*) via the mobile device's touch screen (*sensing by a smartphone, using a smartphone-based sensor*), which a POSITA would understand is a sensor for sensing touch by a living organism, such as a capacitive touch screen. Jain ¶¶[0022], [0075]; EX1042. At step 740, the smartphone retrieves a locally stored PIN. Jain ¶[0075]. Then, at step 742 ("is there a match?"), the smartphone determines whether the user-inputted PIN matches the locally stored PIN, thereby further associating the touch of the touchscreen with a particular living organism. Jain ¶[0075], FIG. 7B. *See also* EX1002 ¶96.

Jain also discloses that rather than "entering a PIN," "the user may be authenticated using . . . biometric information (*e.g.*, fingerprint)" (*physiological data associated with a living organism*). Jain ¶[0075]. Thus, Jain discloses performing steps 738, 740, and 742 in the context of biometric verification, where step 738 senses "biometric information" using a biometric (*e.g.*, fingerprint) sensor (*sensing by a smartphone, using a smartphone-based sensor, physiological data associated with a living organism*), step 740 retrieves locally stored biometric information, and step 742 determines if the sensed biometric information matches the stored biometric information. EX1002 ¶¶97-99.

Accordingly, through this “bootstrapping” process, Jain describes sensing physiological data (touch and/or biometric/fingerprint) of a living organism (user) by a smartphone-based sensor (touch screen and/or biometric/fingerprint sensor).

Further confirming this limitation is met, Patent Owner alleges in its district court infringement contentions that using biometrics to authenticate a user is *prima facie* evidence of limitation 1[a]. EX1016 at 7-12; EX1002 ¶100.

Second, Jain also discloses that during each point-of-sale (“POS”) transaction, a merchant payment terminal may “prompt the user to authorize [the] transaction such as by entering a PIN.” Jain ¶[0029]. This “PIN request” is presented and user information is received via GUI 111 of mobile device 110 (Jain ¶¶[0023]-[0025]), which can include a touch screen (¶[0022]). Authorization via PIN involves or at least obviously involves the same steps as the “bootstrapping” process discussed above. Jain ¶[0075]; EX1002 ¶104. Accordingly, this transactional PIN request similarly requires sensing physiological data of a living organism (*i.e.*, touch associated with a living organism inputting their PIN) using a smartphone-based sensor (*i.e.*, a touch screen). Moreover, just as in the “bootstrapping” implementation, the PIN here too could be replaced with biometric data sensed using a biometric sensor. Jain ¶[0075]; EX1002 ¶108.

To the extent Patent Owner argues that entry of a PIN via touch screen does not disclose sensing physiological data of a living organism and, further, that Jain

somehow does not disclose replacing entry of a PIN for each transaction with a biometric scan, it would have at least been obvious for a POSITA to replace the disclosed PIN in ¶[0029] with user authentication via biometrics. EX1002 ¶¶104-110. Jain already contemplates using biometrics (*e.g.*, fingerprints) to authenticate users for its initial “bootstrapping” process (Jain ¶[0075], Figure 7), and reusing that software and hardware for individual transactions would not further complicate the system or incur material additional costs. Moreover, Jain itself recognizes that biometrics are an alternative to PINs. In addition, a POSITA would recognize advantages of biometrics over PINs, including that biometrics cannot be forgotten or obtained by a bad actor via, *e.g.*, phishing, and that use of biometrics for authorizing individual transactions would thus further improve system security. Alternatively, a POSITA would also be familiar with two-factor authentication and would both (a) know how to retain PIN authentication while augmenting it with biometric authentication and (b) appreciate that the cost of doing so is warranted because of the extra security it provides for financial transactions. EX1002 ¶¶104-110; EX1028 Abstract; EX1029 Abstract; EX1030. Indeed, requiring biometric authentication before authorization of individual transactions was well known in the art. *See, e.g.*, EX1020 ¶¶[0083]-[0084], [0088], Fig. 14; EX1021 ¶[0052]; *see also* EX1002 ¶¶106-110.

- (iii) **1[b]: detecting that a proximity criterion is satisfied between the smartphone and an entity, wherein the entity is not the living organism;**

After Jain's user authentication process 700 (Fig. 7) and transaction card activation process 900 (Fig. 9) are performed, a user (*living organism*) of Jain's mobile device 110 (*the smartphone*) may execute contactless payment transactions with a nearby merchant and its payment terminal (*an entity, wherein the entity is not the living organism*) using short range signals, such as NFC or "proximity signals." Jain ¶¶[0023], [0029] ("The transaction card 112 may operate active-card-emulation mode to convert the mobile device 110 to a contactless payment device loaded with a financial vehicle (FV) that may be, for example, a credit card, a debit card, a gift card and/or other retail payment product. In this mode, the transaction card 112 may execute payment transactions at any capable retail payment terminal (e.g., POS 114) that accepts contactless payment transactions."); *see also id.* Fig. 1, ¶[0020] (describing POS device 114 as housed at a physical retail location of offline store 102, for example); EX1002 ¶111.

To engage in such transactions, mobile device 110 detects, via its included transaction card 112, that it is proximate the merchant by proximity with the merchant's payment terminal (*i.e.*, POS device 114). For example, mobile device 110 "wirelessly receive[s] a request from the POS device 114 to execute a transaction and/or and provide a response." Jain ¶[0023]; EX1002 ¶¶111-112. A

POSITA would understand that mobile device 110 is only able to process the “request” if it is sufficiently close to POS device 114 to receive and decode the short-range signal corresponding to the request (*detecting that a proximity criterion is satisfied between the smartphone and an entity*). EX1002 ¶¶113-118; EX1034 at 11-12; *see also* EX1036 at 220. Specifically, Jain’s NFC and other short range wireless communication protocols are only effective if there is an underlying signal of sufficient strength detected such that the device and the terminal can communicate using that protocol. EX1002 ¶¶113-118; EX1035 at 4, 36; EX1037 at 3. And that signal strength correlates to proximity and rapidly deteriorates as distance increases. EX1002 ¶114; EX1035 at 4, 36; EX1037 at 3. Accordingly, receipt of a short-range NFC signal corresponds to and teaches detecting that a proximity criterion has been satisfied between the smartphone and an entity (*e.g.*, a retail store of a merchant housing the POS device).

Indeed, Jain further discloses an “active-reader mode” that is activated when “the mobile device 110 is proximate (*e.g.*, 10cm or less) a transmitting terminal.” Jain ¶[0030] (describing mobile device 110 being brought proximate the POS device to trigger a user prompt on the mobile device to authorize a transaction or other communication with the POS). Jain recognizes this mode may require NFC or other short-range communication. *Id.* (“this mode can require special NFC hardware”). Thus, Jain’s mobile device 110 communicates with POS device 114 via NFC by first

detecting it is within a certain proximity to the merchant POS device (*e.g.*, “10 cm or less”), thereby disclosing the ’411 patent’s claimed ***detecting that a proximity criterion is satisfied***. EX1002 ¶119.

Also, Jain teaches that its NFC “wireless connection” is based on “ISO 18092/ECMA 340” standards. Jain ¶¶[0023], [0051], [0018]; EX1002 ¶120. The ECMA-340 Interface and Protocol Standard for NFC² explains that an NFC “transaction” requires an “initialization” (described in ECMA-340 §11) and then a “data exchange” (described in §12). EX1047 at §4.26, §10, Figure 5; EX1002 ¶121. ECMA-340 specifies two devices (“Initiator” and “Target”) and two communication modes (“Passive” and “Active”). EX1047 §1, §4.1, §4.7, §4.17, §4.23, §7; EX1002 ¶122. But it does not matter whether Jain’s POS device or mobile device is the “Initiator” or “Target,” or what communication mode they use: every combination results in Jain’s mobile device (*smartphone*) detecting a ***proximity criterion is satisfied*** and then establishing a short-range link used for subsequent

² ECMA 340 is a well-known communications standard that defined NFC. EX1002 ¶121. This standard was publicly available and known to a POSITA even at the time of Jain’s filing, and thus predates the earliest priority date of the challenged patent. *Id.* Exhibit 1047 is a true and correct copy of the 2nd edition of “ECMA-340,” which was publicly available as of December 2004 and not updated again until June 2013. *Id.*; <https://ecma-international.org/publications-and-standards/standards/ecma-340/>. This version was also published as “ISO 18092” cited in Jain. *Id.* The disclosures of ECMA-340 referenced here are found in both the 1st edition (released December 2002) and the 2nd edition. *Id.*; compare EX1047 with EX1034.

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.” EX1047 §10. Then, the “Initiator” sends one or more commands (e.g., ALL_REQ, SENS_REQ, and/or ATR_REQ) and receives one or more responses (e.g., SENS_RES and/or ATR_RES). EX1047 §§11.2.1.16-17, §11.2.1.23, §11.3.2, §§12.2-.3, Figures 13, 24-25; EX1002 ¶123. Thus, regardless of what mode is used and which of Jain’s devices is the Initiator or Target, the Target device detects a sufficiently strong field from the Initiator (*proximity criterion is satisfied*), and the Initiator device detects that a Target is within its field by receiving a response to a command from the Target (*proximity criterion is satisfied*). This exchange of commands and responses results in selection of a particular “Target” and attributes/parameters for further communication with the same, thereby establishing a short-range link. EX1047 §7, §§11.2.1.24-25, §12, §12.1, Figures 22, 24-25; EX1002 ¶124-125. After this link is established, the Initiator and the Target communicate using ECMA-340’s data exchange protocol. EX1047 Figures 5, 23, and 24. This includes transmission of Jain’s transaction request 117, transaction response 119, and authorization response 120. EX1002 ¶¶121-126.

Moreover, Patent Owner alleges in its district court infringement contentions that the use of NFC to conduct financial transactions with a POS terminal is *prima facie* evidence of limitation 1[b]. EX1016 at 12-15; EX1002 ¶127.

At a minimum, it would be obvious to a POSITA that Jain's smartphone detects proximity to a POS device of a merchant before attempting to engage in a transaction or otherwise communicate. To ensure communications are successful and not wasted signaling (which wastes battery life), and further to avoid the security risk of indiscriminately transmitting sensitive financial information over the air, there must first be a determination that Jain's smartphone is near the merchant and the merchant POS before attempting a payment transaction. EX1002 ¶¶112-118. Otherwise, the NFC communication fails or, worse, sends information to unintended recipients. Such implementations were well-known to a POSITA. For example, EX1020 teaches using NFC to limit the range at which communication may take place between devices. EX1020 ¶¶[0041], [0063] [0041]. EX1020 further teaches using this ability to detect proximity with a Wi-Fi hotspot before connecting to it. EX1020 ¶[0073] ("The [identifying information] may be used by the device 10 to indicate that the device is located within communication range of the hot spot 169."). A POSITA would be motivated and able to use Jain's NFC "request" or ECMA-340's commands and responses in the same manner to detect proximity with a merchant and its POS device before communicating with it. EX1002 ¶¶112-118, 120-126.

- (iv) **1[c]: selectively communicating by the smartphone using a first air interface of a plurality of air interfaces with which the smartphone is capable of communicating,**

responsive to the proximity criterion having been detected as being satisfied and responsive to a value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor;

As an initial matter, Jain discloses a plurality of air interfaces over which the mobile device 110 having transaction card 112 may communicate: (1) a first air interface for short-range communications (*e.g.*, contactless transactions) with POS device 114; and (2) a second air interface for cellular and other communications with a cellular network, for example. Jain ¶¶[0021], [0023], [0027], [0030], [0041]-[0044], [0046]-[0048], and Fig. 2; EX1002 ¶128.

Jain discloses that its *first air interface* may utilize “NFC (*e.g.*, ISO 18092/ECMA 340), ISO 14443 type A/B, ISO 15693, Felica, MiFARE, Bluetooth, Ultra-wideband (UWB), Radio Frequency Identifier (RFID), contactless signals, proximity signals, and/or other signals compatible with retail payment terminals.” Jain ¶[0022]; *see also* Jain ¶[0030] (recognizing need for “special NFC hardware”); EX1002 ¶129. This *first air interface* (yellow) between mobile device 110 with transaction card 112 (*smartphone*, in red) and a POS device (*entity*, in green) is shown in Jain’s Figure 1 (annotated):

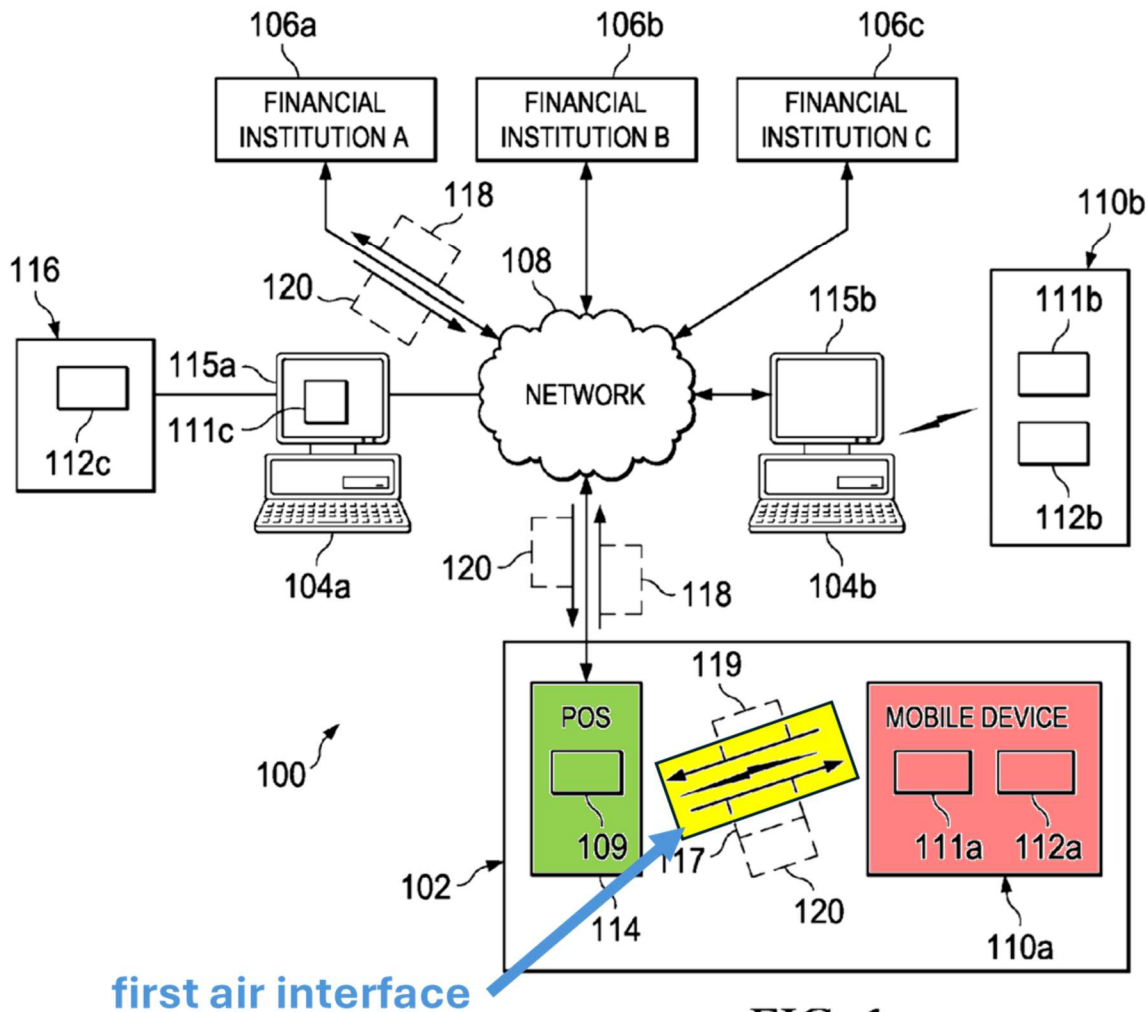
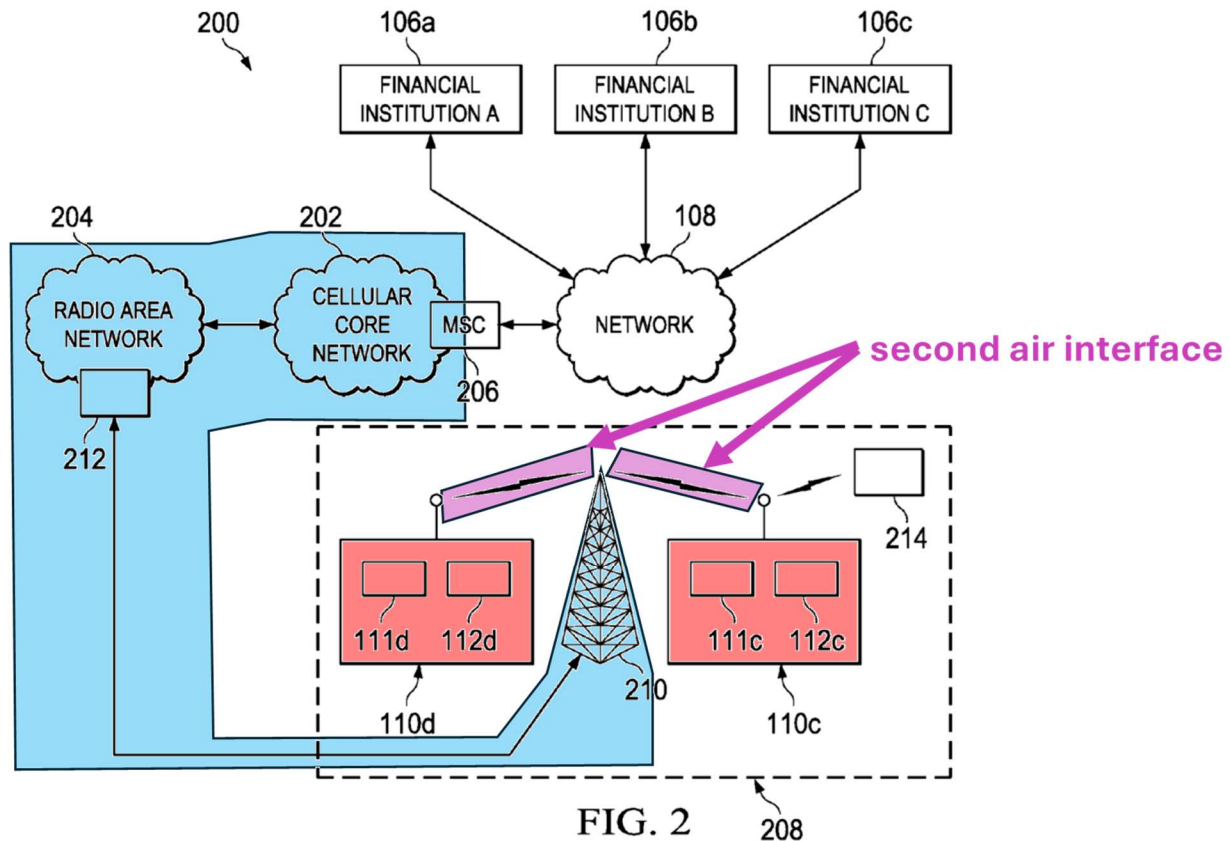


FIG. 1

Jain also discloses a *second air interface* (discussed in more detail below in connection with limitation 1[f])—meaning it has a *plurality of air interfaces*—that may be with a radio access network that provides access to the cellular network (and its associated infrastructure, including base station 210, macrocell 208, base station controller 212, etc.) using “Advanced Mobile Phone Service (AMPS), GSM standards, Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), IS-54 (TDMA), General Packet Radio Service (GPRS), Enhanced Data

Rates for Global Evolution (EDGE), or proprietary radio interfaces.” Jain ¶¶[0043], [0044]; EX1002 ¶130. This *second air interface* (purple) between mobile device 110 with transaction card 112 (*smartphone*, in red) and infrastructure of a cellular network provider (blue) is shown in Jain’s Figure 2:



The mobile devices 110a, 110c, and 110d in Figs. 1 and 2 (annotated in red) are the same mobile device 110 having smartcard 112 discussed herein. Jain ¶¶[0017] (“Like reference symbols in the various drawings indicate like elements.”), ¶¶[0027] (discussing a mobile device that is in proximity-based communication with POS device 114 per FIG. 1, and stating “[i]n some implementations, the financial

institution 106 may transmit the authorization response 120 to the mobile device through a cellular core network (see FIG. 2)').

Moreover, Patent Owner alleges in its district court infringement contentions that a cellular smartphone that supports NFC is *prima facie* evidence of the claimed plurality of air interfaces of limitation 1[c]. EX1016 at 15-20; EX1002 ¶131.

Jain also discloses that mobile device 110 *selectively* communicates over the first air interface (*e.g.*, NFC or other short-range communication protocol) with POS device 114 based on and responsive to the proximity detection of 1[b] and physiological data sensed in 1[a].

Specifically, as explained above with respect to limitation 1[b], mobile device 110 can only engage in contactless payments with POS device 114 when it detects it is proximate the merchant and its POS device 114 (*e.g.*, “10cm or less”) (*responsive to the proximity criterion having been detected as being satisfied*). See *supra* § VIII.A.2(a)(iii); Jain ¶¶[0023], [0029], [0030]; EX1002 ¶¶111-126, 133. For example, Fig. 1 (annotated below) illustrates that communications between mobile device 110a and POS device 114, including transaction request 117, transaction responses 119, and authorization response 120, occur when both are in proximity such as when the mobile device is proximate to and inside the store 102 (Jain ¶[0019])— notably, by contrast, mobile device 110b (blue) is not inside store 102

communicate with POS 114:



FIG. 1

biometric/fingerprint scan (*responsive to a value of the physiological data*)

associated with a living organism that was sensed by the smartphone using the smartphone-based sensor). See *supra* § VIII.A.2(a)(ii); Jain ¶¶[0022]-[0025], [0029], [0065], [0066], [0072], [0075], Table 1, Fig. 7B at steps 734-742; EX1002 ¶¶93-110, 134.

Once both criteria (proximity and physiological data) are met, mobile device 110 having transaction card 112 may then communicate transaction information to POS device 114 over NFC or other short-range communication medium (*selectively communicating by the smartphone using a first air interface of a plurality of air interfaces with which the smartphone is capable of communicating*), and the POS device may then complete the transaction with a corresponding financial institution. Jain ¶¶[0036] (“In illustrated implementation, the POS 114 can wirelessly receive encrypted transaction information [e.g., routing number, account number, transaction amount, credit-card number, etc.] from the transaction card 112 and electronically send the information to one or more of the financial institutions 106 for authorization.”); see also Jain ¶¶[0028] (“The GUI 109 may present a series of screens or displays to the user to, for example, accept a transaction and enter security information such as a PIN.”), [0029] (“a merchant terminal may detect the presence of a host device with the transaction card 112 and prompt the user to authorize a transaction such as by entering a PIN”); EX1002 ¶135.

Thus, Jain's communication of transaction information from the mobile device to the POS terminal is a *selective* communication because it is not performed unless the proximity and physiological data criteria are both met.

Indeed, Patent Owner alleges in its district court infringement contentions that using a smartphone to conduct a financial transaction via NFC after having authenticated the user and bringing the phone proximate a payment terminal is *prima facie* evidence of limitation 1[c]. EX1016 at 15-16; EX1002 ¶136.

- (v) **1[d]: refraining from communicating by the smartphone using the first air interface absent said value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor satisfying a criterion, even though the proximity criterion is detected as being satisfied;**

As explained above with respect to limitations 1[a] and 1[c], mobile device 110 does not communicate with POS device 114 unless its user has been authenticated—first as part of initial bootstrapping but also for each individual transaction—by entry of a PIN on the mobile device touch screen or through biometric/fingerprint scan (*refraining from communicating by the smartphone using the first air interface absent said value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor satisfying a criterion*). See *supra* §§ VIII.A.2(a)(ii), VIII.A.2(a)(iv);

Jain ¶¶[0022]-[0025], [0029], [0065], [0066], [0072], [0075], Table 1, Fig. 7B at steps 734-742; EX1002 ¶¶137-138.

Thus, even if Jain's mobile device 110 having transaction card 112 is brought proximate a merchant and its corresponding POS device 114 to "wirelessly receive a request from the POS device 114 to execute a transaction" (Jain ¶[0023]), the mobile device will refrain from communicating with POS device 114 using the first air interface unless and until the user authenticates and authorizes the transaction (such as by entering a PIN or through biometric authentication). Jain ¶¶[0024], [0028], [0029], [0066].

Jain even discloses turning the NFC antenna off if an incorrect PIN is detected (which a POSITA would understand would include an incorrect biometric scan where biometrics are employed). For example, as shown in annotated Figs. 7A and 7B, below, Jain teaches an authentication loop in which a user may be asked to enter their PIN (steps 734 and 736) when a transaction card is first inserted into the mobile device (step 702) and the antenna is turned off (step 722) if the number of attempts to enter the correct PIN exceeds some threshold (steps 738-744) and thus the device refrains from communicating using the transaction card:

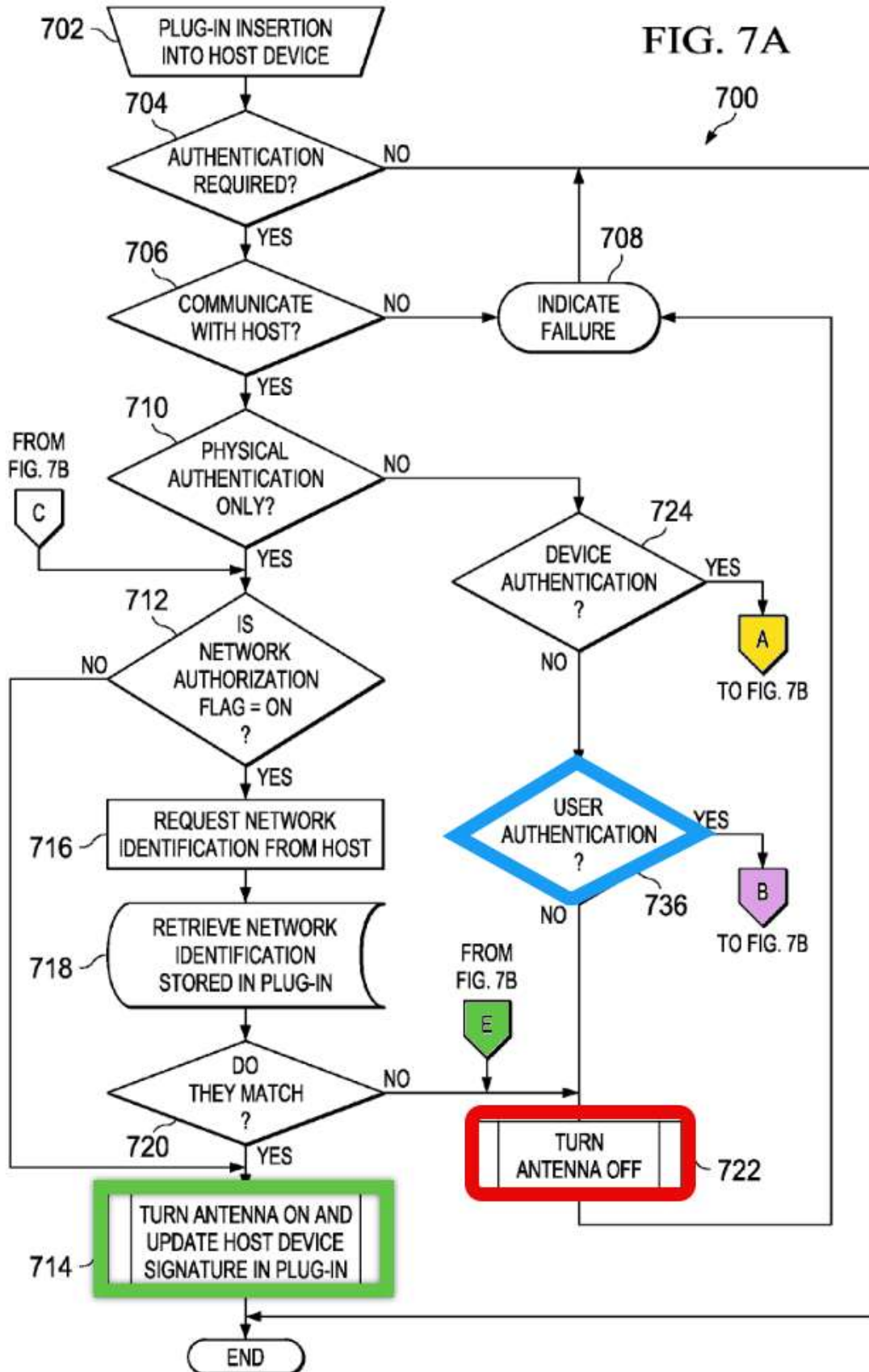
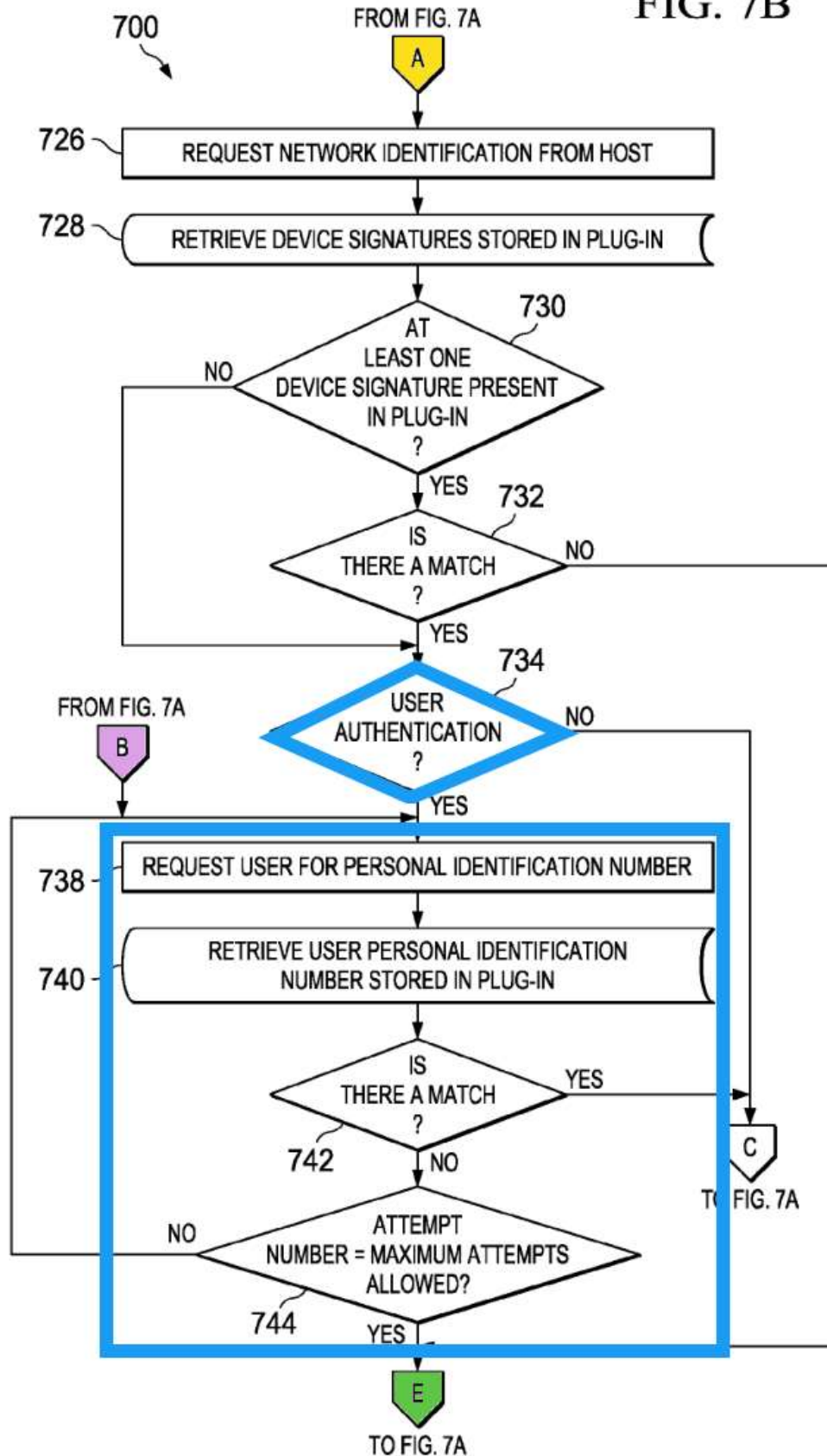


FIG. 7B



See also Jain ¶[0024] (“In some implementations, the transaction card 112 may selectively switch the antenna between an on and off state in response to one or more events. The one or more events may include . . . detection of incorrect PIN entered by the user . . . [and] [i]n some implementations, the transaction card 112 may request user identification such as a PIN, a user ID and password combination, biometric signature, and/or others.”), ¶[0061] (disclosing “antenna control function 320 [that] may activate/deactivate the antenna 322 [which ‘may be a short range wireless antenna’] in response to, for example, successful authentication”), ¶[0066] (“In case of a successful [PIN] match, the antenna 402 may be activated.”), Table 1 (“The user can also optionally select a PIN (change Antenna availability to user authentication)”); EX1002 ¶¶139-140.

Jain also discloses fraud control mechanisms whereby transaction card 112 disables transactional communications (*e.g.*, “execute a command to block . . . the transaction card 112”) if it detects “an operational violation” such as the transaction card 112 being moved from an authorized mobile device 110 to a different mobile device 110. Jain ¶[0026]. A POSITA would understand that a failed user authentication qualifies as an operational violation or at least would have been obvious to include as a violation, particularly since Jain already recognizes that “detection of incorrect PIN entered by the user” qualifies as a violation that triggers

disabling use of the transaction card antenna. Jain ¶¶[0024], [0061], [0065], [0066]; EX1002 ¶141.

Thus, a POSITA would understand that Jain's mobile device 110 having transaction card 112 will turn the NFC antenna off or otherwise disable transactional communications absent the value of a correct PIN (or biometric) being sensed: it refrains from communicating with POS device 114 under such circumstance even though the proximity criterion may be satisfied. EX1002 ¶142.

Consistent with this, Patent Owner alleges in its district court infringement contentions that requiring a smartphone to authenticate its user via biometrics before it is allowed to conduct a financial transaction via NFC, even though the phone may be proximate a payment terminal, is *prima facie* evidence of limitation 1[d]. EX1016 at 20-22; EX1002 ¶143.

- (vi) **1[e]: selectively sending information by the smartphone to one or more other devices and receiving information by the smartphone from the one or more other devices responsive to said value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor satisfying the criterion; and**

As explained above with respect to limitations 1[a] and 1[c], Jain discloses that mobile device 110 communicates with POS device 114 (*one or more other devices*) by sending transaction responses 119 (*selectively sending information by the smartphone to one or more other devices*) and receiving authorization responses

120 (*receiving information by the smartphone from the one or more other devices*) responsive to a user's authentication via PIN or biometric (*responsive to said value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor satisfying the criterion*). See *supra* §§ VIII.A.2(a)(ii), VIII.A.2(a)(iv); Jain ¶¶[0022]-[0025], [0029], [0065], [0066], [0072], [0075], Table 1, Fig. 7B at steps 734-742; EX1002 ¶144.

For example, responsive to user authentication (through initial bootstrapping and for each transaction), “transaction card 112 may transmit one or more transaction responses 119 identifying information associated with a payment account” to POS device 114. Jain ¶[0027]. POS device 114 may then use said information to “transmit a request 118 to authorize a transaction to the financial institution 106.” *Id.* Financial institution 106 may then authorize the transaction and “transmit an authorization response 120” to POS device 114, which “may transmit the response 120 to the to the transaction card 112” where “[t]he transaction response 120 may include, for example, a receipt presentable to the user through the GUI 111 a.” *Id.* All these transmissions to and from mobile device 110 having transaction card 112 (*the smartphone*) are *selective* communications because they are responsive to the user authentication via PIN/biometric (*i.e.*, they are not sent absent authentication). EX1002 ¶145.

The transmissions are further *selective* because they are only sent to a specific POS device 114 in response to transaction request 117 from that device.³ Jain ¶[0027]. For example, Jain discloses mobile device 110 having transaction card 112 may be instructed “to transmit data using its wireless connection with, for example, *the POS 114*”—not some other device. Jain ¶¶[0054], [0057] (describing selective communications directed to POS device 114, including encrypted data). “In addition, the data may be encrypted by the transaction card 112 prior to transmission using, for example, keys and encryption capability stored within the security module.” *Id.*; see also ¶¶[0025] (identifying public and private key encryption schemes supported by transaction card 112), [0036] (“the POS 114 can wirelessly receive encrypted transaction information from the transaction card 112”). A POSITA would understand encrypted communications with a specific POS device 114 prevents other devices from accessing the transaction information and is, thus, a selective communication to a specific device (the device having the correct decryption key). EX1002 ¶¶146-147.

³ To the extent Patent Owner argues that this limitation also requires *selectively* “receiving information” in addition to “selectively sending,” then Jain discloses that for all the same reasons that sending data to POS device 114 is selective. Specifically, receiving authorization response 120 only occurs in an authenticated transaction and is only received from POS device 114. In other words, mobile device 110 does not receive data from other devices with which it is not engaged in a transaction while it is conducting a transaction with POS device 114. EX1002 ¶148.

Indeed, Patent Owner alleges in its district court infringement contentions that using a smartphone to submit a financial transaction to a POS terminal and receive a confirmation from the POS terminal responsive to user authentication (via “a fingerprint, facial recognition, or iris”) is *prima facie* evidence of limitation 1[e]. EX1016 at 22-26; EX1002 ¶149.

- (vii) **1[f]: communicating by the smartphone using a second air interface of the plurality of air interfaces with which the smartphone is capable of communicating that differs from the first air interface.**

As explained above with respect to limitation 1[c], mobile device 114 has a plurality of wireless interfaces, including a second air interface with a radio access network that provides access to a cellular network and its associated infrastructure, such as base station 210, microcell 208, and base station controller 212 (*communicating by the smartphone using a second air interface of the plurality of air interfaces with which the smartphone is capable of communicating*), all of which are separate from the NFC interface used for short-range communications (*that differs from the first air interface*). See § VIII.A.2(a)(iv), *supra*; Jain ¶¶[0043], [0044]; EX1002 ¶¶150-151; *see also* Fig. 2 (annotated):

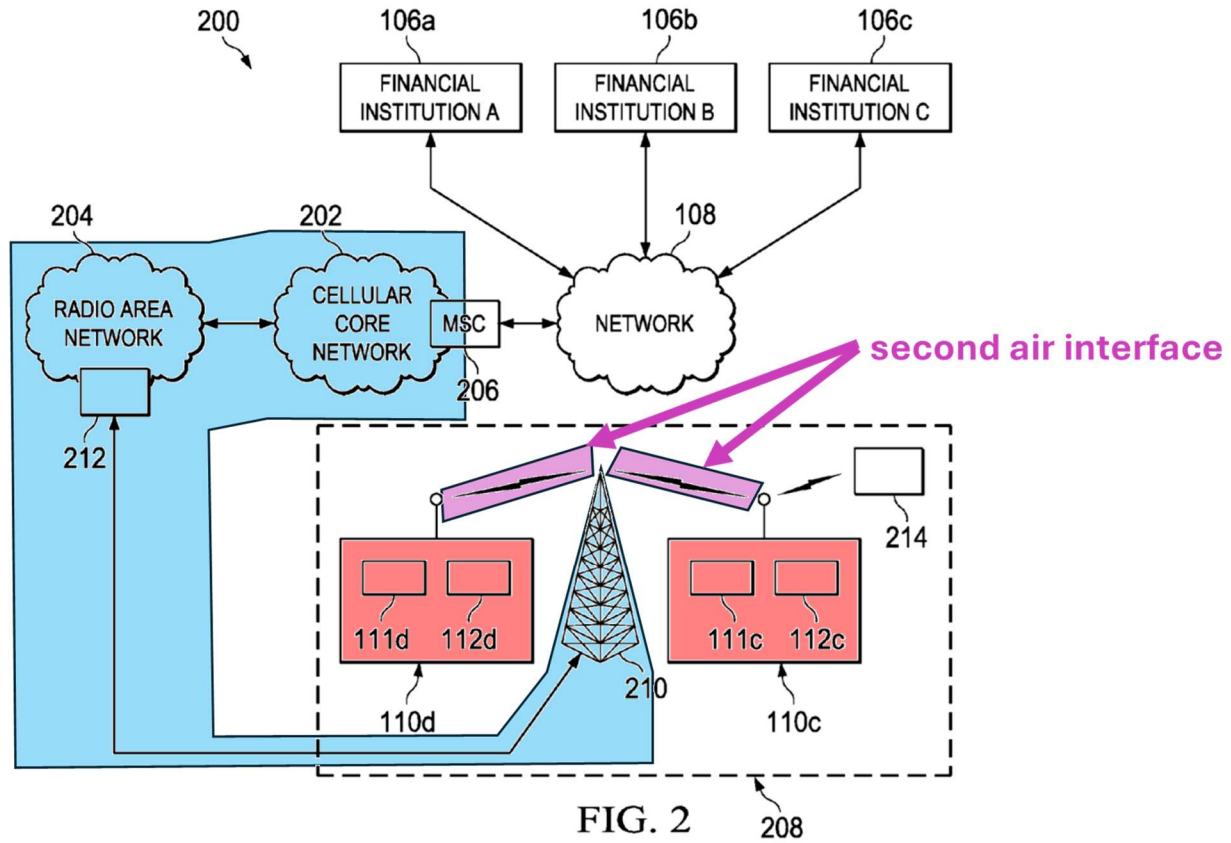


FIG. 2

For example, Jain describes the mobile device 110 may wirelessly communicate with a financial institution “using the cellular core network 202” separate from any NFC communication with a POS terminal by noting “the financial institutions 106 may transmit information to the transaction card 112 without requiring a POS terminal being proximate to the card 112.” Jain ¶[0046].

Moreover, Patent Owner alleges in its district court infringement contentions that a smartphone that can communicate over a cellular data network in addition to NFC is *prima facie* evidence of limitation 1[f]. EX1016 at 26-27; EX1002 ¶152.

(b) Claim 2

- (i) 2[pre]: The method according to claim 1, wherein said detecting that a proximity criterion is satisfied between the smartphone and an entity comprises:**

See limitation 1[b], *supra*.

- (ii) 2[a]: detecting that a proximity criterion of less than 10 meters in distance is satisfied between the smartphone and the entity;**

Jain discloses that the short-range communication occurs at a range of “10 cm or less” (Jain ¶[0030]) or between 10 cm and 50 cm (Jain ¶[0045]). Thus, when Jain detects the proximity criterion is met at those ranges, as addressed above with respect to limitation 1[b], Jain is *detecting that a proximity criterion of less than 10 meters in distance is satisfied between the smartphone and the entity*. EX1002 ¶154. Also, that range is consistent with what a POSITA knows about NFC: it has an effective range of about 10 cm. *See* EX1002 ¶154; EX1032 §8.

- (iii) 2[b]: wherein the detecting is performed by the smartphone, by a device that is associated with the entity, by a system that is associated with the smartphone, or a combination thereof.**

As set out above for limitation 1[b], *the detecting is performed by the smartphone, by a device that is associated with the entity, by a system that is associated with the smartphone, or a combination thereof* (mobile device 110 with transaction card 112 and/or POS device 114). Moreover, given how NFC operates, a POSITA would understand that the mobile device, POS terminal, or both, must

perform the detecting, not least because one must be the NFC-340 Initiator and the other must be the NFC-340 Target. EX1002 ¶¶155-156.

(c) **Claim 3**

(i) **3[pre], 3[a]**

As explained *supra*, Jain discloses a smartphone having a processor that is configured to and does control the smartphone to perform the claimed process steps and capabilities. *See also* Jain at ¶[0021] (“As used in this disclosure, the mobile devices 110 are intended to encompass cellular phones, data phones, pagers, portable computers, SIP phones, *smart phones*, personal data assistants (PDAs), digital cameras, MP3 players, camcorders, *one or more processors within these or other devices*, or any other suitable processing devices capable of communicating information with the transaction card 112.”); EX1002 ¶¶157-158.

(ii) **3[b] – 3[g]**

The remaining limitations of claim 3 are substantively identical to claim 1 and merely remove the references in claim 1 to claim steps being performed “by a smartphone,” as claim 3 separately recites the smartphone in 3[pre]/3[a]. Accordingly, Jain discloses a smartphone with a processor that implements the claimed capabilities for the same reasons provided above with respect to claim 1. *See supra* § VIII.A.2(a), where limitations 3[b]-[g] map to limitations 1[a]-1[f], respectively; EX1002 ¶159.

(d) Claim 4

Claim 4 is substantively identical to claim 2, limitations 2[pre] and 2[a]. Accordingly, Jain discloses 4[pre] and 4[a] for the same reasons as 2[pre] and 2[a], respectively. *See supra* § VIII.A.2(b)(i)-(ii); EX1002 ¶160.

B. Ground 2: Dua (EX1018)

1. Background

Dua is prior art under at least pre-AIA 35 U.S.C. § 102(b), having been published July 27, 2006—more than a year before the earliest effective filing date of the '411 patent. Dua discloses all limitations of the '411 patent claims, but Petitioner presents Dua as an obviousness reference in the event Patent Owner argues there are any differences between Dua and the '411 patent claims.

Dua was *cited* during prosecution of the '411 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 '411 patent claims. EX1008 at 207, 208. The '432 patent claims required “independent of performing said first transaction, receiving by the smartphone a communications service from a wireless network, using a second air interface that differs from the first air interface,” whereas the '411 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.

Like Jain, Dua discloses systems and methods for using a mobile telephone (*i.e.*, smartphone) to conduct wireless transactions with a POS terminal by: (1) detecting if the mobile device is sufficiently close to the POS reader/terminal of a merchant to conduct a transaction (*e.g.*, Dua ¶¶[0041], [0315]], [0352]-[0355], [0380], [0383]); (2) sensing presence of a living organism through user authentication via, *e.g.*, biometrics (physiological data) (*e.g.*, ¶¶[0366], [0384], [0395], [0414]); and (3) if both conditions are met, transmitting stored payment credentials to the merchant POS terminal to perform the transaction. Dua refrains from communicating the credentials to the POS reader/terminal in the absence of both criteria (*i.e.*, authentication and proximity), and discloses that the mobile telephone may separately communicate over a cellular network to access the Internet. Dua ¶[0041]. *See also* EX1002 ¶¶161-168.

2. Analysis

(a) Claim 1

(i) 1[pre]

Dua describes a method comprising the steps in the remaining limitations of claim 1. *See infra; see also* Dua at Abstract (“A novel system and methodology for conducting financial and other transactions using a wireless device. . . . Credentials are ultimately supplied to a handheld device such as a mobile telephone via a wireless network. The user holding the credential may then use the handheld device to conduct the authorized transaction or set of transactions via, for example, a short range wireless link with a point-of-sale terminal.”), ¶¶[0041], [0312]-[0313], [0333]; EX1002 ¶¶169-170.

(ii) 1[a]

Dua discloses a wireless device, which includes a *smartphone*. Dua Abstract, FIGS. 3, 5, 6(a)-8. The wireless device includes a “handheld device, such as a mobile telephone,” “capable of wirelessly connecting to the internet” and with applications like a “wallet application.” Dua Abstract, ¶¶[0041], [0049]-[0051], [0287]-[0288], FIGS. 3, 5, 6(a)-8; *see also* EX1002 ¶170.

Dua further discloses its wireless device (*smartphone*) sensing a user’s fingerprint (*sensing . . . physiological data associated with a living organism*) with the “wireless device’s embedded biometric technologies,” which involves biometric sensors (*using a smartphone-based sensor*). Dua ¶¶[0366], [0414], [0534]

(disclosing additional types of user physiological data that may be sensed, including “iris, voiceprints, facial recognition, and hand geometry”). In particular, the wallet application on Dua’s wireless device scans for “fingerprint[s] in lieu of a PIN code to authenticate a user.” Dua ¶¶[0366], [0414], [0534]. And the scanned fingerprint can also be used to decrypt wallet application data. Dua ¶¶[0050], [0366], [0399], [0429]. *See also* EX1002 ¶171.

Alternatively, Dua discloses a PIN to secure the wallet application and data. For example, Dua’s wallet application must be opened so it can be provisioned with a credit card and, thus, requires authentication via PIN. Dua ¶¶[0128]-[0129], [0178], [0180], [0250], [0366]. Engaging in a financial transaction with a POS terminal also requires entry of the PIN. Indeed, “[t]he default security setting in the wallet application is that PIN-entry is required before the wallet application can be ‘opened’ and any credentials transmitted to an external device.” Dua ¶[0366]; *see also* ¶¶[0384], [0395] (requiring “the user to input a PIN before RF communication can be enabled”). Even accessing the Dua wallet application may require entry of a PIN. Dua ¶[0429] (“The data stored inside the wireless device is encrypted and protected with the wallet PIN code (or other biometric security information), which is used to allow the user access to the application.”). Securing access to the wallet application makes sense, as it can hold credit card and other sensitive, confidential information. Dua ¶¶[0041], [0055], [0287]-[0288], [0334]. The wallet application

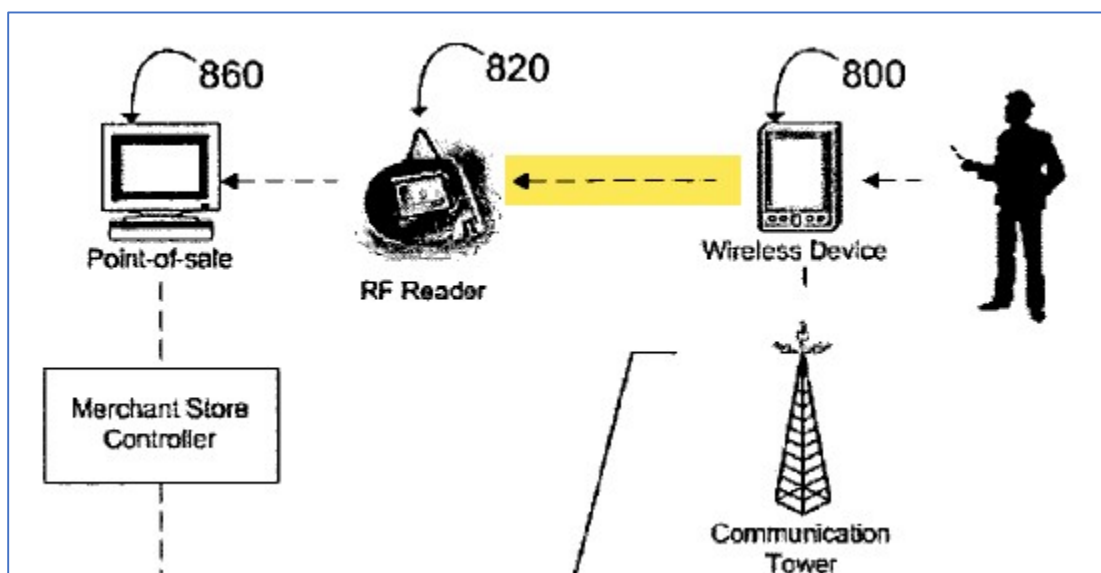
allows the user to navigate, view, and select the stored credentials for transmission and thus needs to be protected. Dua ¶¶[0324]-[0332], [0334], [0366], [0378], [0384]. *See also* EX1002 ¶¶172-178.

For Dua's PIN entry, the wireless device receives a PIN after it is typed in the smartphone keyboard or touchscreen. *E.g.*, Dua ¶[0414] ("PINs can be entered directly into the user's wireless device 800"). As explained above with respect to Jain (*see* § VIII.A.2(a)(ii), *supra*), a POSITA would understand that such a keyboard or touchscreen is as a sensor for sensing touch (*e.g.*, capacitive touch screen) and, thus, senses touch associated with a living organism. Dua ¶¶[0366], [0384], [0395], FIGS. 1, 3, 6(a), 8, FIG. 9; EX1042. The entered PIN code is then used to decrypt data or otherwise matched against a validation PIN code stored on the wallet application, thereby validating the user's identity. Dua ¶¶[0050], [0366], [0399], [0429]; *see also* EX1002 ¶177.

Accordingly, Dua expressly discloses sensing a PIN but also biometric data such as a fingerprint. EX1002 ¶¶165-171. Further confirming this limitation is met, Patent Owner alleges in its district court infringement contentions that using biometrics to authenticate a user is *prima facie* evidence of limitation 1[a]. EX1016 at 7-12; EX1002 ¶179.

(iii) 1[b]

A purpose of Dua is to facilitate transactions and other communications between a wireless device and a merchant POS reader/terminal “via, for example, a short range wireless link” Dua ¶[0026], Abstract (“The user holding the credential may then use the handheld device to conduct the authorized transaction or set of transactions via, for example, a short range wireless link with a point-of-sale terminal.”), ¶[0041] (“Wireless device 200 also preferably has an integrated *short-range communication capability* for transmitting confidential information and exchanging other data between the wallet application and *an external reader that is in proximity to the wireless device*”). The annotated excerpt of Figure 8, below, illustrates the short-range link (highlighted in yellow) between Dua’s wireless device 800 (*the smartphone*) and an RF reader 820 of a merchant POS terminal 860 (*an entity, wherein the entity is not the living organism*).



See also Dua ¶[0405] (“point of sale terminal 860, via RF reader 820 can be used to capture and transmit an electronic credential from a wireless device”); EX1002 ¶¶180-182.

Dua discloses that the consumer wireless device must be “in close proximity to a reader device” to communicate and engage in a “proximity transaction.” Dua ¶[0315]. “For example, a wireless device loaded with a wallet application, that also has an integrated RFID chip can simply be waved slowly *in close proximity* to a reader device to facilitate a transaction.” *Id.*; see also ¶¶[0321], [0355], [0371]. Dua also discloses the RFID chip can be an NFC chip—thus disclosing NFC transactions. *Id.* ¶[0016] (“Wireless devices with integrated RFID proximity chips or Near Field Communication (NFC) technology may also provide users the ability to transfer information to a reader device.”); see also EX1002 ¶¶180-184.

A POSITA would further understand that short-range RFID/NFC links are established responsive to *detecting that a proximity criterion is satisfied between the smartphone and an entity*. EX1002 ¶184. Specifically, Dua’s RFID and NFC communications are only effective if there is an underlying signal of sufficient strength detected such that the device and the terminal can communicate. *Id.*; EX1035 at 4, 36; EX1037 at 3. And that signal strength correlates to proximity and rapidly deteriorates as distance increases. EX1002 ¶177; EX1035 at 4, 36; EX1037 at 3. A POSITA would thus understand RFID and NFC links have a range of up to

~3m and ~10cm, respectively. EX1002 ¶184; EX1035 at 36; EX1037 at 3 (“NFC operates... over a typical distance of a few centimeters.”); *see also* Dua ¶[0009] (disclosing range of “typically two to three inches” for unpowered cards). Accordingly, receipt of a short-range RFID or NFC signal (by either the wireless device or the POS reader) corresponds to and teaches detecting that a proximity criterion has been satisfied between the smartphone and an entity (*e.g.*, a retail store of a merchant housing the POS device). EX1002 ¶185.

Dua further discloses that in some embodiments, if “the device is not placed in proximity of the reader” for a set time (*e.g.*, “30 seconds”), the wallet application on the wireless device “will disable RF communication and the application may shutdown or go into its normal dormant state.” Dua ¶¶[0383], [0384]. This requires the device (*smartphone*) to detect whether it is proximate to the reader of the merchant’s POS terminal (*entity*), otherwise it would not know to shut down RF communication. EX1002 ¶¶186-187.

Dua also discloses an embodiment in which the payment credential used for mobile transactions is issued to a consumer by bringing “his wireless device in proximity of an RFID reader, which will send a command to the wallet application signifying that it is going to receive a new credential via Bluetooth” and thereafter “exchang[ing] encryption keys via RF in order to establish a secure Bluetooth connection.” Dua ¶[0321]. In this embodiment, before the wireless device can

engage in any POS transaction or communicate with the RFID reader to exchange encryption keys, it must receive a command from the RFID reader. A POSITA would understand that transmission and receipt of the command comprises detecting proximity with the RFID reader of the issuer. EX1002 ¶188. Indeed, a POSITA would understand the issuer RFID reader does not indiscriminately broadcast commands, it sends a command specifically to the wallet application of a proximate wireless device and, as such, must detect proximity with the device. *Id.*

Also, Dua teaches that its short-range communications protocol may be NFC. Dua ¶[0016]. Dua, like Jain, was filed after publication of the 2nd edition of the ECMA standard and before release of the 3rd edition. A POSITA would thus understand that Dua's references to NFC refer to implementing the ECMA 340 standard, 2nd edition. EX1002 ¶¶189-192. Moreover, as explained above in connection with Jain, regardless of what NFC mode is being used and which device in Dua is the Initiator and which device is the Target, both devices detect whether *a proximity criterion* has been satisfy, establish a link, and then use that link to exchange data. This includes transmission of Dua's credential data. At a minimum, it would have been obvious to implement Dua's NFC communications this way. EX1002 ¶192. Dua tells a POSITA to look to "ISO/IEC 14443" RF proximity standard (Dua ¶[0013]), which would motivate a POSITA to also look to the

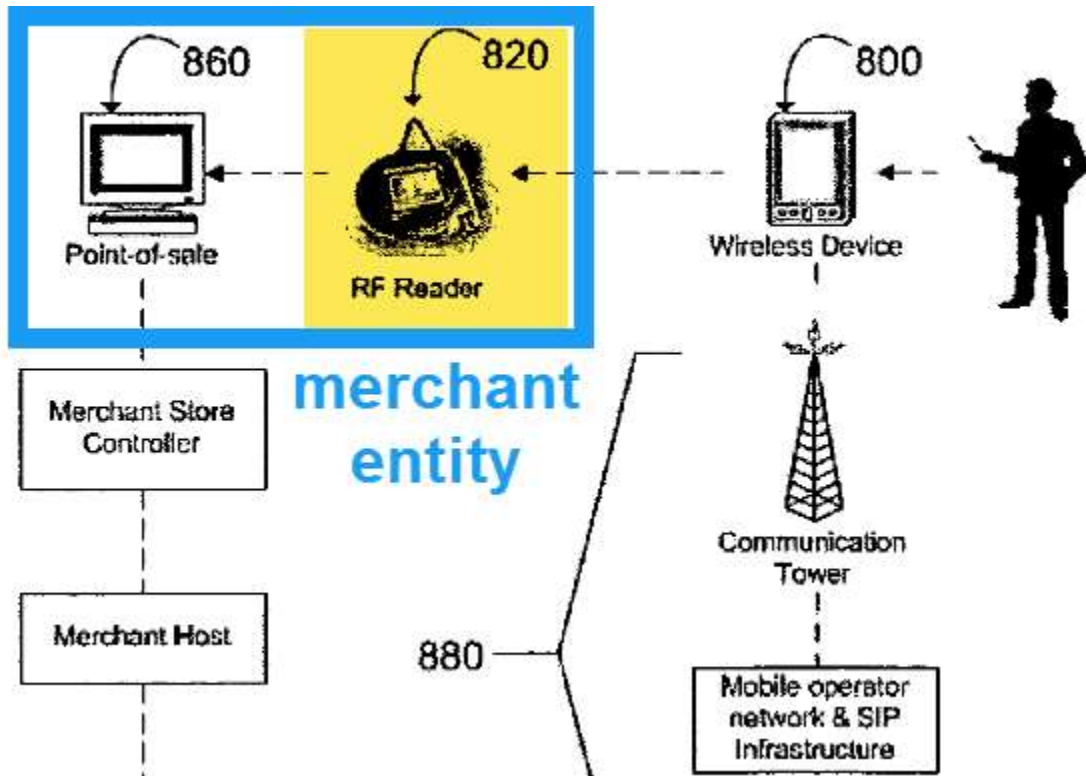
standard for NFC, as would the benefits of implementing a standard discussed above in connection with Jain. EX1002 ¶192; *see also* EX1002 ¶126.

Thus, Dua's embodiments are further evidence of limitation 1[b] and are consistent with a POSITA's understanding that the wireless device (*smartphone*) must detect it is proximate the reader of a merchant POS terminal (*entity*), or *vice versa*, before communicating, because the short-range link between the wireless device and reader/POS terminal requires proximity. EX1002 ¶193.

Indeed, Patent Owner alleges in its district court infringement contentions that the use of NFC to conduct financial transactions with a POS terminal is *prima facie* evidence of limitation 1[b]. EX1016 at 12-15; EX1002 ¶194.

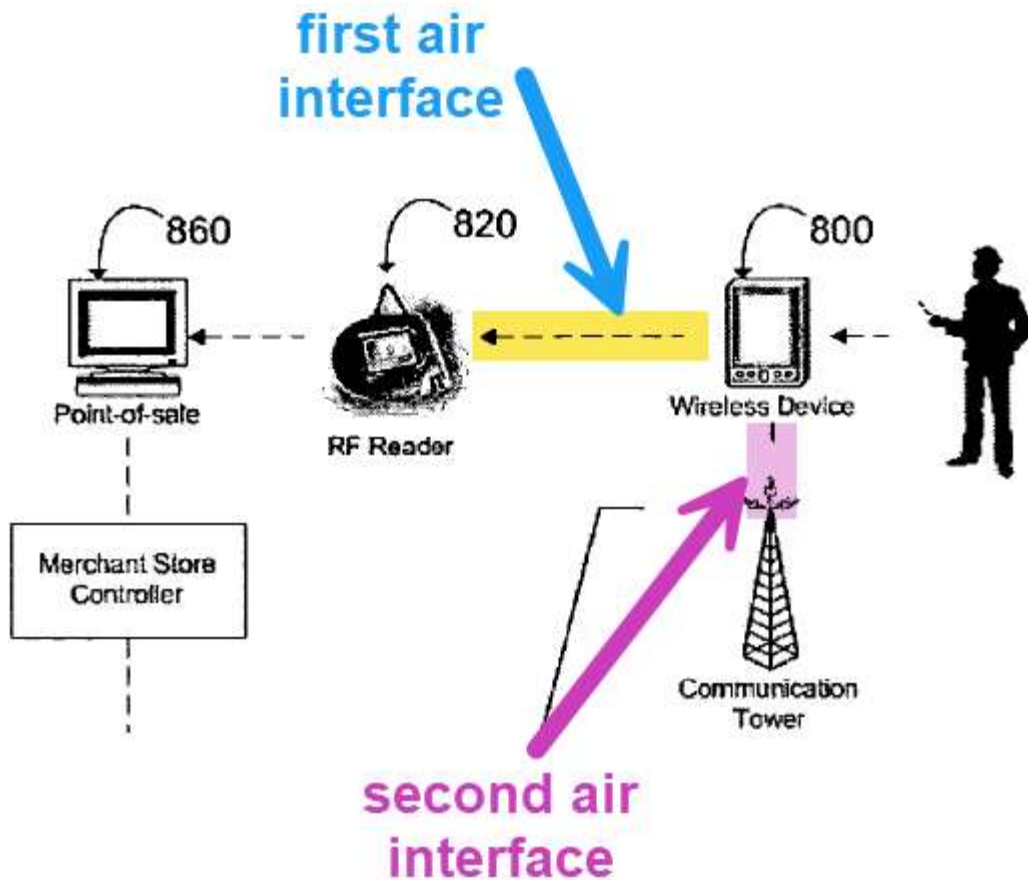
At a minimum, it would be obvious to a POSITA that Dua's smartphone detects proximity to a POS device of a merchant (or *vice versa*) before attempting to engage in a transaction or otherwise communicate. To ensure communications are successful and not wasted signaling (which wastes battery life), and further to avoid the security risk of indiscriminately transmitting sensitive financial information over the air, there must first be a determination that Dua's smartphone is near the merchant and the merchant POS before attempting a payment transaction. EX1002 ¶195. Otherwise, the short-range communication fails or, worse, sends information to unintended recipients. Such implementations were well-known to a POSITA. For example, EX1020 teaches using NFC to limit the range at which communication

may take place between devices. EX1020 ¶[0041], [0063] [0041]. EX1020 further teaches using this ability to detect proximity with a Wi-Fi hotspot before connecting to it. EX1020 ¶[0073]. A POSITA would be motivated and able to use Dua's wireless device in the same manner to detect proximity with a merchant and its POS device before communicating with it. EX1002 ¶196. A POSITA would be motivated and able to use ECMA-340's commands and responses in the same manner. EX1002 ¶¶189-192. Indeed, given Dua's disclosure of NFC, a POSITA would also understand it would have at least been obvious to use Dua's wireless device as an NFC Target and to use NFC passive communications mode, whereby the wireless device detects the RF field generated by the RF reader/POS terminal when the wireless device is proximate the reader/terminal of the merchant POS entity *(detecting that a proximity criterion is satisfied between the smartphone and an entity)* and thereafter engages in further communications, such as a financial transaction. EX1002 ¶197; *see also* Dua Fig. 8, excerpted and annotated below (showing wireless device 800 proximate RF reader 820 of merchant POS 860).



(iv) 1[c]

As an initial matter, Dua discloses a *plurality of air interfaces* over which the wireless device may communicate: (1) a first air interface for short-range communications (*e.g.*, contactless transactions) with RFID/NFC readers at a point of sale; and (2) a second air interface for cellular and other communications with a cellular network, for example. Dua ¶¶[0015]-[0018], [0044], [0051], [0409], Fig. 1 (element 155), Fig. 8 (excerpted and annotated, below; see also element 880):



Dua explains that “[t]he capability of wireless devices has been augmented by their ability to connect to the Internet and also to exchange data over short ranges with other wireless devices or readers.” Dua ¶[0015]. Dua goes on to identify some of those short-range protocols as various IEEE 802.11 Wi-Fi protocols, Bluetooth, IrDA (infrared), RFID, and NFC. Dua ¶[0016]; *see also* Dua ¶[0018] (referring to “short-range data transmission capability of wireless devices”), ¶[0041] (“Wireless device 200 also preferably has an integrated short-range communication capability...”), ¶[0383] (similar). Dua thus discloses *a first air interface*. EX1002 ¶¶ 198-199.

Moreover, Dua's wireless device may be a cell phone. *E.g.*, Dua ¶[0015]. A POSITA would understand a cell phone makes and receives voice calls and exchanges data over a cellular network. EX1002 ¶200. Dua also discloses using cellular networks, which Dua calls a "mobile operator network," for data communications. *See, e.g.*, Dua ¶¶[0044], [0051], [0409], Fig. 1 (element 155), Fig. 8 (element 880). And Figs. 1 and 8 both show the wireless device connecting to the mobile operator network via a cell tower. Dua thus discloses ***a plurality of air interfaces with which the smartphone is capable of communicating.*** EX1002 ¶¶198, 200.

Indeed, Patent Owner alleges in its district court infringement contentions that a cellular smartphone that supports NFC is *prima facie* evidence of the claimed plurality of air interfaces of limitation 1[c]. EX1016 at 15-20; EX1002 ¶201.

Dua also discloses that its wireless device ***selectively*** communicates over the first air interface (*e.g.*, RFID, NFC, or other short-range communication protocol) with an RFID/NFC reader of the merchant POS terminal based on and responsive to the proximity detection of 1[b] and physiological data sensed in 1[a]. EX1002 ¶202.

First, as explained above with respect to limitation 1[b], Dua discloses its wireless device engages in contactless payments with a merchant POS terminal when proximity with the merchant and its POS terminal's RFID/NFC reader is detected (***responsive to the proximity criterion having been detected as being***

satisfied), or at least renders such proximity detection obvious. *See supra* § VIII.B.2(a)(iii); Dua ¶¶[0315], [0321], [0352]-[0355], [0371]; EX1002 ¶203. Indeed, Dua even discloses an embodiment that shuts down the wallet application and disables RF communications if proximity with the merchant POS terminal is not detected for a set time. Dua ¶¶[0383], [0384]. Thus, subsequent proximity-based payment transactions (and selective communications related thereto) are based on and responsive to detecting proximity with the RF reader of the merchant POS terminal for a set time. EX1002 ¶204.

Additionally, as explained with respect to 1[b], Dua also discloses an embodiment in which a payment credential used for mobile transactions is issued to a consumer by bringing “his wireless device in proximity of an RFID reader [of an issuer], which will send a command to the wallet application signifying that it is going to receive a new credential via Bluetooth” and thereafter “exchang[ing] encryption keys via RF in order to establish a secure Bluetooth connection.” Dua ¶[0321]. In this embodiment, proximity between the wireless device and “an issuer’s site” (the *entity*) by detecting proximity with the issuer’s RFID reader according to transmission and receipt of the command from the reader (*detecting proximity*)—*i.e.*, the RFID reader detects proximity in order to send a command, and the wireless device detects proximity by receiving the command. The wireless device then communicates with the reader to “exchange encryption keys via RF” (*selectively*

communicating)—this is a selective communication because it is based on having detected proximity and is also directed to a specific RFID reader (it is not an indiscriminate broadcast). *Id.* Moreover, subsequent wireless device transactions using the acquired credential (*e.g.*, “digital debit card”) are also selective communications, as they only occur after and are thus responsive to: (1) the initial proximity detection with the credential issuer and its RFID reader; and (2) subsequent proximity detection with a merchant and its RFID reader (*supra* § VIII.B.2(a)(iii)). *See also* EX1002 ¶¶205-206.

Second, as explained above with respect to limitation 1[a], Dua’s wireless device also does not communicate with a POS terminal unless its user has been authenticated—both as part of initial credential acquisition and each individual transaction—by entry of a PIN on the wireless device touchscreen or through biometric/fingerprint scan (*responsive to a value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor*). *See supra* § VIII.B.2(a)(ii); Dua ¶¶[0366], [0384], [0395], [0414]; EX1002 ¶207.

Accordingly, once both criteria (proximity and physiological data) are met, Dua’s wireless device can communicate information to a merchant POS terminal (*selectively communicating by the smartphone using a first air interface of a*

plurality of air interfaces with which the smartphone is capable of communicating) for conducting a transaction. EX1002 ¶208.

Thus, Dua's communication of transaction information from the wireless device to the issuer or merchant POS terminal is a *selective* communication because it is not performed unless the proximity and physiological data criteria are both met.

Indeed, Patent Owner alleges in its district court infringement contentions that using a smartphone to conduct a financial transaction via NFC after having authenticated the user and bringing the phone proximate a payment terminal is *prima facie* evidence of limitation 1[c]. EX1016 at 15-16; EX1002 ¶209.

(v) 1[d]

As explained above with respect to limitations 1[a] and 1[c], Dua's wireless device does not communicate with POS terminals/readers unless its user has been authenticated—first as part of initial credential acquisition but also for each individual transaction with a credential—by entry of a PIN on the phone touchscreen or through biometric/fingerprint scan (*refraining from communicating by the smartphone using the first air interface absent said value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor satisfying a criterion*). See *supra* §§ VIII.B.2(a)(ii), VIII.B.2(a)(iv); Dua ¶¶[0128]-[0129], [0178], [0180], [0250], [0366], [0384], [0395], [0414], [0534]; EX1002 ¶210.

Thus, even if Dua’s wireless device is brought proximate a merchant or issuer and their corresponding POS terminal, the wireless device and wallet application will refrain from communicating with the POS terminal using the first air interface unless and until the user opens the wallet application and selects a credential for transmission, both of which require entering a PIN or through biometric authentication. *E.g.*, Dua ¶[0366] (“The default security setting in the wallet application is that PIN-entry is required before the wallet application can be ‘opened’ and any credentials transmitted to an external device.”); *cf.* ¶[0395] (disclosing embodiment in which RF communication is not enabled unless the user inputs their PIN); *see also* EX1002 ¶211.

Indeed, Patent Owner alleges in its district court infringement contentions that requiring a smartphone to authenticate its user via biometrics before it is allowed to conduct a financial transaction via NFC, even though the phone may be proximate a payment terminal, is *prima facie* evidence of limitation 1[d]. EX1016 at 20-22; EX1002 ¶212.

(vi) 1[e]

As explained above with respect to limitations 1[a] and 1[c], Dua’s wireless device communicates with issuers and merchants and their respective POS readers/terminals responsive to a user’s authentication via PIN or biometric. *See supra* §§ VIII.B.2(a)(ii), VIII.B.2(a)(iv); EX1002 ¶213. Dua also discloses

selectively sending information to a particular POS reader/terminal and receiving information from that reader/terminal as part of such communications.

For example, Dua requires a user to enter a PIN (or biometric) “before the wallet application can be ‘opened’ and any *credentials transmitted to an external device*” such as a POS reader/terminal (*responsive to said value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor satisfying the criterion*). Dua ¶¶[0366], [0384]. Once authenticated, the user “will be required to pre-select all the credentials he wants to *transmit to a reader* prior to placing his device in proximity of the reader during a transaction” and “the wallet application is ready to *transmit the credential(s)* via its RFID interface.” Dua ¶¶[0371]-[0378]. “When the wireless device is placed in proximity to the reader, the selected credential(s) are automatically *transmitted* by the RFID chip in the wireless device to the reader” (*selectively sending information by the smartphone to one or more other devices*). *Id.*; see also ¶[0320] (“credential data is transmitted from the wireless device to a merchant”). EX1002 ¶¶214-215.

Dua also discloses the wireless device *receiving* information from the reader/terminal. Indeed, Dua expressly discloses “*bi-directional* exchange of data” between the wireless device and POS readers/terminals—meaning the wireless device will not only send information to the POS but will also receive information

from it. ¶[0318]. For example, (1) a POS reader/terminal may send a prompt to the “wireless device for various types of preferences, questions, or other data input in sequence” (¶[0319]), (2) “during a transaction—a point-of-sale device may establish secure connectivity with the user's wireless device and poll it for a list of user-defined payment methods that the user can select from using the user-interface of the POS system” (¶[0317]), and (3) the wireless device and POS reader/terminal may “exchang[e] encryption keys via RFID” (¶[0318])—all of which teach *receiving information by the smartphone from the one or more other devices*. EX1002 ¶¶216-217.

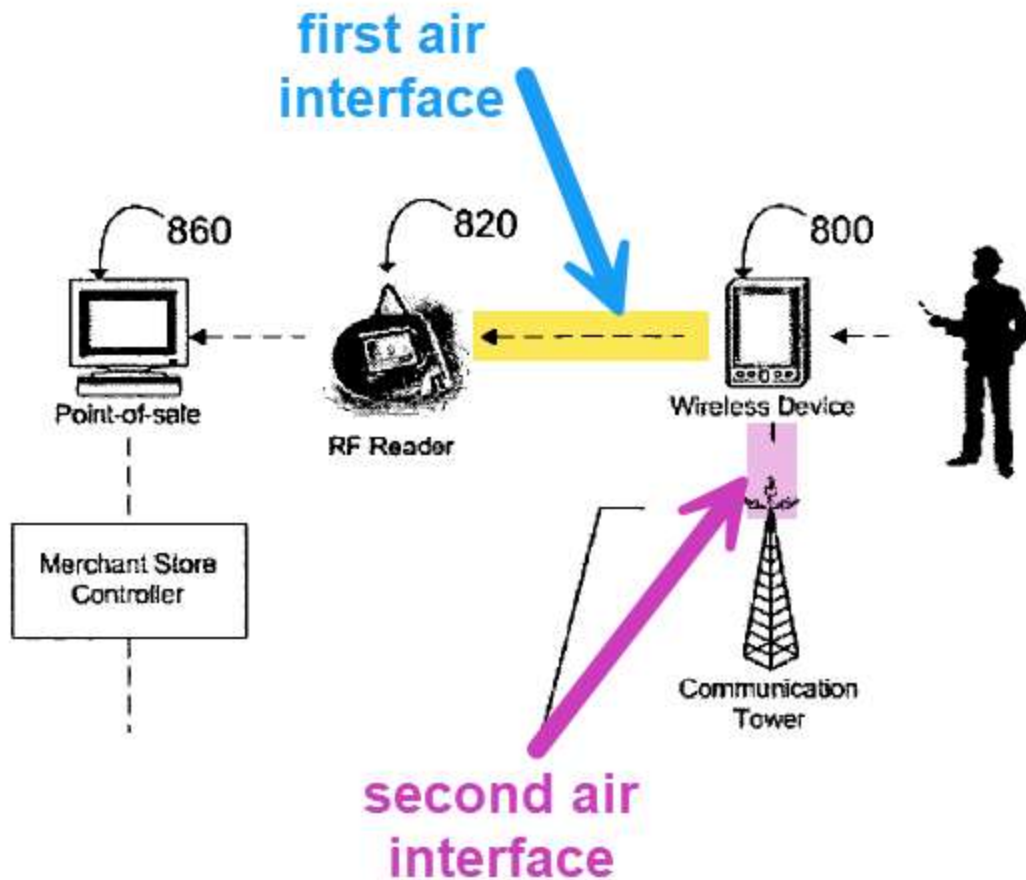
Dua also discloses an embodiment in which a user presses a “hot button” to send a pre-selected payment method and credentials matching a particular POS reader’s “reader key” to that specific reader (*selectively sending*), “provided that the reader sent the key in its initial communication with the wireless device” (*receiving*). ¶[0393]; *see also* ¶[0353]. These communications are also responsive to user authentication, as pressing the hot button “may prompt the user to input a PIN before RF communication can be enabled.” ¶[0395]. In sum, the user pushes a button and is prompted to enter a PIN before RF communication is enabled (*responsive to said value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor satisfying the criterion*) after which the wireless device receives a reader key from the reader/terminal

(receiving information by the smartphone from the one or more other devices) and, in response, transmits a payment method and corresponding credential for that specific reader/terminal (*selectively sending information by the smartphone to one or more other devices*). EX1002 ¶¶218-219.

Indeed, Patent Owner alleges in its district court infringement contentions that using a smartphone to conduct a financial transaction with a POS terminal and receive a confirmation from the POS terminal responsive to user authentication (via “a fingerprint, facial recognition, or iris”) is *prima facie* evidence of limitation 1[e]. EX1016 at 22-26; EX1002 ¶220.

(vii) 1[f]

As noted above, Dua’s wireless device may be a cell phone. *E.g.*, Dua ¶[0015]. A POSITA would understand that a cell phone can make and receive voice calls and exchange data over a cellular network. EX1002 ¶2221. Dua also discloses using cellular networks for data communications. Dua refers to a cellular network as a “mobile operator network.” *E.g.*, Dua ¶¶[0044], [0051], [0409]; *see also* Fig. 1 (element 155) and Fig. 8 (element 880), both of which show the wireless device connecting the mobile operator network via a cell tower. Dua thus discloses the wireless device communicating *using a second air interface . . . that differs from the first air interface*. EX1002 ¶222.



For example, Dua discloses that its wireless device and “wallet application is designed to facilitate transactions in a proximity, personal, and remote environment using the device's short-range *or long-range transmission capability*.” Dua ¶[0333]; *see also* ¶[0323] (“In a remote-or online--environment, transactions are conducted with a remote server *over a wireless network*” and can include “online purchases,” “banking,” and “downloading digital content”). Dua expressly distinguishes the long-range transmissions over a wireless network from short-range communications with a POS reader/terminal. *E.g.*, Dua ¶[0026] (explaining that “credentials are ultimately supplied to a handheld device such as a mobile telephone

via a wireless network” and separately referring to and, thus, distinguishing “a short range wireless link with a point-of-sale (POS) terminal”). For example, Dua discloses a feature by which a Wireless Credential Manager (WCM) can remotely wipe the wallet application of a stolen wireless device over a mobile operator’s wireless network—*not* the first air interface. Dua ¶¶[0454], [0455] (explaining this feature requires the wireless device to “have signal to the wireless network”). *See also* EX1002 ¶¶223-225.

Moreover, Patent Owner alleges in its district court infringement contentions that a smartphone that can communicate over a cellular data network in addition to NFC is *prima facie* evidence of limitation 1[f]. EX1016 at 26-27; EX1002 ¶226.

(b) Claim 2

(i) 2[pre]

See limitation 1[b], *supra*.

(ii) 2[a]

As noted with respect to limitation 1[b], Dua discloses that the effective range of unpowered RFID smartcards is “typically two to three inches” for unpowered cards. Dua ¶[0009]. These are the cards that are included in Dua’s wireless device. Also, that range is consistent with what a POSITA knows about NFC: that under ideal circumstances, NFC is considered to have an effective range of about 10 cm. *See* EX1002 ¶228, EX1032 §8; *see also* Jain ¶¶[0030], [0045]. Consistent with what is set forth above with respect to limitation 1[b] and 2[a], Dua thus discloses

detecting that a proximity criterion of less than 10 meters in distance is satisfied between the smartphone and the entity.

(iii) 2[b]

As set out above for limitation 1[b], *the detecting is performed by the smartphone, by a device that is associated with the entity, by a system that is associated with the smartphone, or a combination thereof* (Dua’s device and/or POS terminal). Given how NFC operates, a POSITA would understand that the mobile device, POS terminal, or both, must perform the detecting, not least because one must be the NFC-340 Initiator and the other must be the NFC-340 Target. EX1002 ¶¶229-230.

(c) Claim 3

(i) 3[pre], 3[a]

As explained *supra*, Dua discloses a smartphone having a processor that is configured to and does control the smartphone to perform the claimed process steps and capabilities. *See also* Dua ¶[0315] (“a wireless device loaded with a wallet application, that also has an integrated RFID chip”), ¶[0384] (referring to “the wireless device’s operating system”); EX1002 ¶¶231-232.

(ii) 3[b] – 3[g]

The remaining limitations of claim 3 are substantively identical to claim 1 and merely remove the references in claim 1 to claim steps being performed “by a smartphone,” as claim 3 separately recites the smartphone in 3[pre]/3[a].

Accordingly, Dua discloses a smartphone with a processor that implements the claimed capabilities for the same reasons provided above with respect to claim 1. *See supra* § VIII.B.2(a), where limitations 3[b]-[g] map to limitations 1[a]-1[f], respectively; *see also* EX1002 ¶233.

(d) Claim 4

Claim 4 is substantively identical to claim 2, limitations 2[pre] and 2[a]. Accordingly, Dua discloses 4[pre] and 4[a] for the same reasons as 2[pre] and 2[a], respectively. *See supra* § VIII.B.2(b)(i)-(ii); EX1002 ¶234.

C. Secondary Considerations

Any secondary considerations further weigh in favor of obviousness and do not overcome the strong showing of obviousness. First, Patent Owner has not practiced the claimed invention, evidencing a lack of commercial success for any product practicing the '411 patent. EX1002 ¶236. Additionally, there was no long felt, unresolved need met by the '411 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 ¶237. Further, the vast number of contactless payment systems and trials of those systems before the '411 patent's priority date indicates that many within the market observed the desirability of such systems and were concurrently working towards implementing them. *See* §§ IV.A, VIII. Even if any secondary factors weighing in

favor of non-obviousness did exist, they do overcome the strength of the obviousness analysis. *See* EX1002 ¶¶236-237.

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 12,406 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 '411 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
apederson@carlsoncaspers.com

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

Date: May 23, 2025

/s/ James Glass

James Glass (Reg. No. 46729)