

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. IPR2025-00978

U.S. Patent No. 12,028,793

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 12,028,793**

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. MANDATORY NOTICES AND FEES	1
A. Real Party-In-Interest	1
B. Related Matters.....	1
C. Counsel and Service Information	2
D. Payment of Fees	2
E. Requirements for Inter Partes Review	2
III. GROUNDS	3
IV. STATE OF THE ART	3
V. '793 PATENT.....	6
A. '793 Patent Specification	6
B. Prosecution History (EX1015).....	6
VI. PERSON OF ORDINARY SKILL	7
VII. CLAIM CONSTRUCTION	7
VIII. GROUNDS	7
A. Ground 1: Jain (EX1017)	7
1. Background	7
2. Analysis.....	9
B. Ground 2: Dua (EX1018).....	47
1. Background	47
2. Analysis.....	49
C. Secondary Considerations	71
IX. STIPULATION	71
X. CONCLUSION.....	72

EXHIBIT LIST

Ex.	Description
EX1001	U.S. Patent No. 12,028,793 (“’793 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 ’793 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 Wireless Wallet Consumer Trial”, Kyocera (Oct. 18, 2007), https://americas.kyocera.com/press-releases/press-releases_201503201874.htm
EX1024	U.S. Pub. No. 2005/0137977
EX1025	U.S. Pub. No. 2001/0026632
EX1026	NTT DoCoMo FOMA F900iC Basic Manual
EX1027	Jain et al., “An Identity-Authentication System” (Sep. 1997)
EX1028	U.S. Patent No. 6,957,339
EX1029	Jin et al., “Biohashing: two factor authentication featuring fingerprint data and tokenised random number” (Apr. 27, 2004)
EX1030	Bhargav-Spantzel, “Privacy Preserving Multi-Factor Authentication with Biometrics” (2006)
EX1031	“About NFC Technology”, NFC Forum (Jun. 15, 2006), https://web.archive.org/web/20060615050709/http://www.nfc-forum.org/aboutnfc/about_nfc_technology/
EX1032	Erik Rolf & Viktor Nilsson, “Near Field Communication (NFC) for Mobile Phones” (Aug. 2006)
EX1033	Wall Street Journal, Vivotech (Aug. 12, 2005), https://web.archive.org/web/20060915080521if_/http://www.vivotech.com:80/newsroom/coverage/Videos/Wall_Street_Journal/Wall_Street_Journal.wmv

EX1034	Near Field Communication - Interface and Protocol (NFCIP-1), Standard ECMA-340 (December 2002)
EX1035	NFC Forum News Conference, NFC Forum (June 5, 2006)
EX1036	Dean A. Gratton, “Developing Practical Wireless Applications”, Elsevier Digital Press (2007)
EX1037	Jacki Katzman, “NFC Forum Unveils Technology Architecture and Announces Initial Specifications and Mandatory Tag Format Support”, NFC Forum, at 3 (June 5, 2006)
EX1038	Arumugam et al., “Consumer Electronics Application and Coverage Constraints Using Bluetooth and Proposed Bluetooth Evolution Technologies” (Aug. 2001)
EX1039	U.S. Pub. No. 2010/0082445
EX1040	Information Sciences Institute, RFC 793 Transmission Control Protocol (Sep. 1981), https://datatracker.ietf.org/doc/html/rfc793
EX1041	“Bluetooth Basics”, Bluetooth (Apr. 23, 2006), https://web.archive.org/web/20060423011921/http://www.bluetooth.com/Bluetooth/Learn/Basics/
EX1042	“iPhone Premieres This Friday Night at Apple Retail Stores”, Apple (Jun. 28, 2007), https://www.apple.com/newsroom/2007/06/28iPhone-Premieres-This-Friday-Night-at-Apple-Retail-Stores/
EX1043	“Enabling Fast Wireless Networks with OFDM,” EETimes (February 1, 2001), https://www.eetimes.com/enabling-fast-wireless-networks-with-ofdm/
EX1044	IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999), IEEE Computer Society, June 12, 2007
EX1045	“Getting Base Stations Ready for LTE”, EETimes (April 17, 2007), https://www.eetimes.com/getting-base-stations-ready-for-lte/

EX1046	3rd Generation Partnership Project; Technical Specification Group Radio Access Network; LTE Physical Layer – General Description (Release 8), 3rd Generation Partnership Project, March 2007
EX1047	Near Field Communication - Interface and Protocol (NFCIP-1), Standard ECMA-340 (2nd Edition, December 2004)

LIST OF CHALLENGED CLAIMS

Claim	Limitation
1[pre]	A method comprising:
1[a]	sensing a physiological parameter; then
1[b]	determining whether or not the physiological parameter sensed satisfies a criterion; then
1[c]	responsive to the physiological parameter sensed satisfying the criterion, enabling at least one first function; then
1[d]	while said at least one first function is enabled, responsive to having sensed the physiological parameter and responsive to having determined that the physiological parameter sensed satisfies the criterion, requesting an authorization to establish a function to conduct a financial transaction; then;
1[e]	responsive to the requesting, receiving the authorization to establish the function to conduct the financial transaction; then
1[f]	responsive to receiving the authorization, establishing the function to conduct the financial transaction; and then
1[g]	responsive to satisfying a proximity condition relative to an entity and responsive to sensing the physiological parameter and determining that the physiological parameter sensed satisfies the criterion, using the function that has been established to conduct the financial transaction and conducting the financial transaction by paying for a product;
1[h]	wherein said paying for a product comprises sensing that the proximity condition is satisfied relative to an access point maintained by a vendor at a point of purchase counter, by detecting a short-range signal that is transmitted by the access point, determining that the physiological parameter sensed satisfies the criterion and then, responsive to having sensed that the proximity condition is satisfied relative to the access point and having determined that the physiological parameter sensed satisfies the criterion, paying for the product by selectively sending information to at least one device;

Claim	Limitation
1[i]	wherein said paying for the product by selectively sending information to at least one device comprises selectively and wirelessly transmitting information to the at least one device using unlicensed frequencies; and
1[j]	wherein said paying for a product further comprises deducting/withdrawing an amount of money from an account.
2[pre]	The method of claim 1, wherein said enabling at least one first function comprises enabling the at least one first function and disabling a second function; and wherein the method further comprises:
2[a]	repeatedly sensing the physiological parameter and repeatedly deciding, based on comparing the physiological parameter sensed to the criterion, whether or not to maintain enabled said at least one first function while maintaining disabled said second function; and
2[b]	maintaining enabled said at least one first function while maintaining disabled said second function responsive to deciding that the physiological parameter sensed satisfies the criterion; or
2[c]	disabling said at least one first function and enabling said second function responsive to deciding that the physiological parameter sensed no longer satisfies the criterion.
3[pre]	The method of claim 1,
3[a]	wherein said paying for a product further comprises wirelessly receiving information from at least one device using unlicensed frequencies.
4[pre]	The method of claim 3,
4[a]	wherein said wirelessly transmitting information to the at least one device using unlicensed frequencies and said wirelessly receiving information from at least one device using unlicensed frequencies comprises using unlicensed frequencies over a short-range link in a Time Division Duplex operation; and
4[b]	wherein said selectively and wirelessly transmitting information to the at least one device further comprises selectively and wirelessly transmitting information to the access point maintained by the vendor at

Claim	Limitation
	the point of purchase counter and to at least one other device that is predetermined; and further comprises wirelessly receiving information from the access point maintained by the vendor at the point of purchase counter and from at least one other device that is predetermined.
5[pre]	A wireless device that comprises a smartphone and a sensor; wherein the wireless device is configured to perform operations comprising:
5[a]	sensing, by the sensor, a physiological parameter of a user of the wireless device; then
5[b]	determining whether or not the physiological parameter sensed satisfies a criterion; then
5[c]	responsive to the physiological parameter sensed satisfying the criterion, enabling at least one first function of the wireless device; then
5[d]	while said at least one function is enabled, responsive to having sensed the physiological parameter and responsive to having determined that the physiological parameter sensed satisfies the criterion, requesting from a second device an authorization to establish a function to conduct a financial transaction; then
5[e]	responsive to the requesting, receiving from the second device the authorization to establish the function to conduct the financial transaction; then
5[f]	responsive to receiving the authorization, establishing at the wireless device the function to conduct the financial transaction; and then
5[g]	responsive to the wireless device satisfying a proximity condition relative to an entity and responsive to the wireless device sensing the physiological parameter and determining that the physiological parameter sensed satisfies the criterion, using the function that has been established at the wireless device to conduct the financial transaction and conducting the financial transaction by paying for a product;
5[h]	wherein said paying for a product comprises sensing that the proximity condition is satisfied relative to an access point maintained by a vendor at a point of purchase counter, by detecting a short-range signal that is

Claim	Limitation
	transmitted by the access point, determining that the physiological parameter sensed satisfies the criterion and then, responsive to having sensed that the proximity condition is satisfied relative to the access point and having determined that the physiological parameter sensed satisfies the criterion, paying for the product by selectively sending information to at least one device;
5[i]	wherein said paying for the product by selectively sending information to at least one device comprises selectively and wirelessly transmitting information to the at least one device using unlicensed frequencies; and
5[j]	wherein said paying for a product further comprises deducting/withdrawing an amount of money from an account.
6[pre]	The wireless device of claim 5, wherein said enabling at least one first function of the wireless device comprises enabling the at least one first function of the wireless device and disabling a second function of the wireless device; and wherein the operations further comprise:
6[a]	repeatedly sensing the physiological parameter and repeatedly deciding, based on comparing the physiological parameter sensed to the criterion, whether or not to maintain enabled said at least one first function while maintaining disabled said second function; and
6[b]	maintaining enabled said at least one first function while maintaining disabled said second function responsive to deciding that the physiological parameter sensed satisfies the criterion; or
6[c]	disabling said at least one first function and enabling said second function responsive to deciding that the physiological parameter sensed no longer satisfies the criterion.
7[pre]	The wireless device of claim 5, wherein said conducting the financial transaction by paying for a product comprises:
7[a]	establishing by the wireless device a short-range wireless link with the entity;

Claim	Limitation
7[b]	wirelessly transmitting information to the entity using unlicensed frequencies; and
7[c]	wirelessly receiving information from the entity using unlicensed frequencies;
7[d]	wherein said wirelessly transmitting information to the entity and said wirelessly receiving information from the entity comprises using unlicensed frequencies in a time division duplex operation; and
7[e]	wherein said establishing by the wireless device a short-range wireless link with the entity comprises establishing the short-range wireless link with the entity responsive to the wireless device satisfying the proximity condition relative to the entity and responsive to the wireless device sensing the physiological parameter and determining that the physiological parameter sensed satisfies the criterion.
8[pre]	The wireless device of claim 5, wherein said requesting from a second device an authorization to establish a function to conduct a financial transaction and/or said receiving from the second device the authorization to establish the function to conduct the financial transaction comprises:
8[a]	establishing by the wireless device a link with the second device, said link comprising a wireless link;
8[b]	wirelessly transmitting information to the second device over said wireless link using unlicensed and/or licensed frequencies; and
8[c]	wirelessly receiving information from the second device over said wireless link using unlicensed and/or licensed frequencies;
8[d]	wherein said wirelessly transmitting information to the second device and/or said wirelessly receiving information from the second device comprises using a WiFi air interface protocol, an orthogonal frequency division multiplexing air interface protocol and/or an orthogonal frequency division multiple access air interface protocol; and

Claim	Limitation
8[e]	wherein said establishing by the wireless device a link with the second device comprises establishing the link with the second device responsive to the wireless device sensing the physiological parameter and determining that the physiological parameter sensed satisfies the criterion.
9[pre]	The wireless device of claim 5,
9[a]	wherein said using unlicensed frequencies comprises using unlicensed frequencies over a short-range link in a Time Division Duplex operation; and
9[b]	wherein said selectively sending information to at least one device further comprises selectively sending information to the access point maintained by the vendor at the point of purchase counter and to at least one other device that is predetermined; and selectively receiving information from the access point maintained by the vendor at the point of purchase counter and from at least one other device that is predetermined.
10[pre]	The wireless device of claim 5,
10[a]	wherein said paying for a product further comprises wirelessly receiving information from at least one device using unlicensed frequencies.
11[pre]	The wireless device of claim 10,
11[a]	wherein said wirelessly transmitting information to the at least one device using unlicensed frequencies and said wirelessly receiving information from at least one device using unlicensed frequencies comprises using unlicensed frequencies over a short-range link in a Time Division Duplex operation; and
11[b]	wherein said selectively and wirelessly transmitting information to the at least one device further comprises selectively and wirelessly transmitting information to the access point maintained by the vendor at the point of purchase counter and to at least one other device that is predetermined; and further comprises wirelessly receiving information

Claim	Limitation
	from the access point maintained by the vendor at the point of purchase counter and from at least one other device that is predetermined.

I. INTRODUCTION

The '793 patent is directed to performing a “financial transaction” using a “smartphone.” It does not, however, disclose any non-obvious technology for performing such a transaction. Indeed, using existing cell-phone technology to conduct financial transactions was the subject of intense growth during the early 2000s, with pilot programs and commercial deployments by companies including Nokia, Motorola, Kyocera, and NTT. The technology was mature enough to be the subject of multiple patent publications from this timeframe, including the prior art Jain and Dua references relied upon in this Petition.

II. MANDATORY NOTICES AND FEES

A. Real Party-In-Interest

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

B. Related Matters

The '793 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 '793 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 '793 patent is in the same family as U.S. Patents Nos. 9,462,411, 9,832,708, 10,219,199, 10,674,432, 11,770,756, 11,924,743, and 11,937,172, 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 (any additional fees) to Deposit Account No. 50-5708.

E. Requirements for Inter Partes Review

Petitioner certifies that the '793 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)	1-11
2	§103	Dua (U.S. Pat. Appl. Pub. No. 2006/0165060)	1-11

IV. STATE OF THE ART

As the '793 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 1:37-2:6. Indeed, the market for mobile phones capable of cellular communications was well-established by the 1990s, with the Nokia 3210 released in 1999 eventually selling over 160 million units. EX1002 ¶85. Manufacturers added other standardized wireless communication technology to mobile phones by the early 2000s. The first IEEE standard for Wi-Fi (802.11) was published in 1997, and by 2005 phones with both cellular and Wi-Fi communication capabilities, such as the 2005 Samsung SCH-i730, were common. EX1002 ¶85. So too were phones with Bluetooth capabilities, such as the Nokia 6310 and, again, the Samsung SCH-i730. EX1002 ¶85.

Near Field Communication (NFC) was also common at that time, and used RFID technology (*i.e.*, magnetic field induction) to allow short-range wireless communications between devices in close proximity. EX1002 ¶¶86, 121, 125. Examples of mobile phones with integrated NFC capabilities include the 2004

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

EX1002 ¶86.

Manufacturers quickly deployed applications leveraging these additional smartphone capabilities, including mobile payment. Mobile payment technology was commercially deployed as early as 2004 in Japan with NTT Docomo's support of the Sony FeliCa chip for mobile phones coupled with Osaifu-Keitai ("Wallet Mobile") software. EX1002 ¶87. This technology soon spread to the United States, with mobile phone and payment companies teaming up to conduct pilot programs of their own mobile payment software, including a 2006 pilot by Nokia and MasterCard, a 2007 pilot program by Motorola and Discover, and a 2007 pilot by Kyocera and MasterCard, with companies such as ViVOtech releasing full mobile payment solutions. EX1002 ¶87; *see also* EX1022:



See also screenshots from EX1033:



As mobile phones evolved into smartphones and were increasingly used for sensitive activities (*e.g.*, financial transactions) and to store sensitive user data (*e.g.*, payment account information), mobile phone security received industry attention. EX1002 ¶88. One security mechanism that gained popularity in the early 2000s was biometric authentication. By the early 2000s, fingerprint scanners were routinely integrated into mobile phones, such as the 2000 SAGEM MC 959, 2003 Fujitsu F505i, 2004 Pantech GI100, and 2007 Toshiba G500 and G900. EX1002 ¶88. For example, the mobile phones used for mobile payments in the 2007 Kyocera and MasterCard trial included fingerprint scanners and required biometric authentication. EX1002 ¶88; *see also* EX1023 **Error! Hyperlink reference not valid.**(describing Kyocera trial of “mobile payment technology” from ViVOtech with “biometric security, with fingerprint scanners from Atrua Technologies for transactional security on the test handsets”).

V. '793 PATENT

A. '793 Patent Specification

The specification assumes familiarity with a “wireless communications device” such as “a wireless terminal, a wireless/mobile phone, a Personal Digital Assistant (PDA), a smart phone, a multi-media device including Global Positioning System (GPS) capability, etc.” EX1001 at 1:58-2:6, 3:16-25. It relies on long-established, generic concepts of computer systems such as “authorization” (5:48-50), “sensors” capable of detecting, inter alia, physiological input (mentioned only at 6:17-34), “short-range communications” (mentioned in the specification only at 8:29-34 and 8:56-65), “air interface[s]” (6:62-63, with a recitation of then-existing interfaces at 7:21-31), and “communications service[s]” (9:10). The specification acknowledges that the “adaptivity and mobility aspects of wireless communications” were already “important in people’s lives” at the time of alleged invention. EX1001 at 1:37-38. It also assumes that mobile phones could act as digital wallets. EX1001 at 1:47-50. The specification does not disclose or purport to disclose new or improved means of sensing (including physiological/biometric sensing) or proximity detection. EX1002 ¶¶38-39.

B. Prosecution History (EX1015)

The Examiner rejected the claims of the '793 patent just once, for obviousness-type double patenting, which was overcome by submitting a terminal disclaimer. EX1002 ¶42.

VI. PERSON OF ORDINARY SKILL

A person of ordinary skill in the art at the time of the '793 patent ("POSITA") had at least a Bachelor of Science in electrical engineering, computer engineering, or similar fields and at least two years of practical experience in the field of secure wireless communication applications. More education can supplement for less practical experience, and vice versa. EX1002 ¶¶77-79.

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

VII. CLAIM CONSTRUCTION

No express constructions are required to find the '793 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 '793 patent. Jain discloses all limitations of the '793 patent claims, but Petitioner presents Jain as an obviousness reference in the event Patent Owner argues there are differences between Jain and the '793 patent claims.

Jain was not considered by the Examiner during prosecution of the '793 patent.

While each limitation is addressed in the “Analysis” section below in detail, given the repetitive and nonsequential nature of the '793 patent's claim language, below is a short, non-limiting overview of Ground 1:

'793 patent claim 1 can be divided into two parts: first establishing a function to conduct a financial transaction, and then conducting such a financial transaction. Establishing the function to conduct a financial transaction consists of (1) determining if a physiological (e.g., biometric) parameter meets a criterion; (2) if the criterion is met, enabling a function; and (3) using that function to request and then receive authorization to establish the function to conduct a financial transaction. Jain discloses the same sequence by (1) performing user authentication via PIN or biometrics (*e.g.*, Fig. 7B, steps 734-742); (2) if user is authorized, updating device signatures to enable cellular communications with a financial institution (*e.g.*, Fig. 7A, step 714); and (3) using the cellular communications to request and receive an activation code from the financial institution (*e.g.*, Fig. 9, steps 920-926).

'793 patent claim 1 also requires then conducting a financial transaction, which consists of (1) detecting if the smartphone is in proximity of an access point; (2) determining if the criterion is satisfied (according to Patent Owner, this criterion is satisfied by the claimed “first step” and no further determining is required); and

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

2. Analysis

(a) Claim 1

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

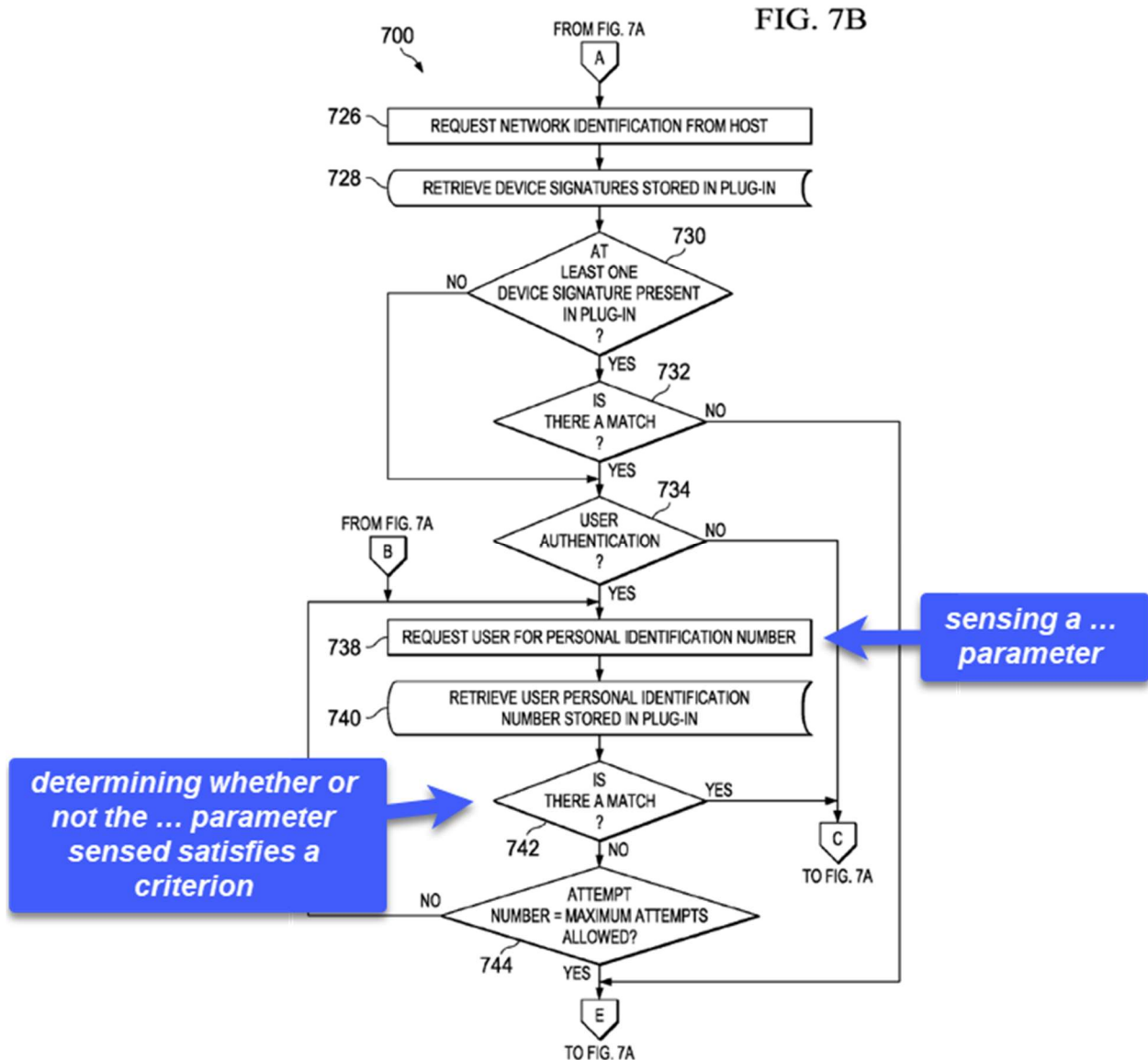
Jain discloses a method for authenticating (Jain ¶¶[0072]-[0075], Fig. 7), activating (Jain ¶¶[0080]-[0081], Fig. 9), and then using a transaction card in a mobile device to conduct a financial transaction (Jain, Abstract, ¶¶[0019], [0023], [0027]-[0029]). EX1002 ¶95.

(ii) 1[a]: *sensing a physiological parameter; then*

(iii) 1[b]: *determining whether or not the physiological parameter sensed satisfies a criterion; then*

The claim begins with a prerequisite to establishing the function to conduct a financial transaction: *determining* if a *physiological parameter* satisfies a *criterion*. Jain discloses this prerequisite in steps 734-742 of Fig. 7B. Specifically, Jain

discloses an authentication process for “automatically bootstrapping” transaction card 112 to mobile device 110, which includes authenticating a user using a PIN number or biometrics (*e.g.*, fingerprint) (*physiological parameter*). Jain ¶¶[0072], [0075], Fig. 7B (annotated); EX1002 ¶¶96-97.



At step 738, the smartphone receives a PIN (*sensing a ... parameter*) via the mobile device’s touch screen. Jain ¶¶[0022], [0075]. At step 740, the smartphone

retrieves a locally stored PIN. Jain ¶[0075]. Then, at step 742 (“is there a match?”), the mobile device *determin[es]* whether the user-inputted PIN matches the locally-stored PIN (*whether or not the ... parameter sensed satisfies a criterion*). Jain ¶[0075], Fig. 7B. *See also* EX1002 ¶98.

Jain also discloses that rather than “entering a PIN... the user may be authenticated using... biometric information (*e.g.*, fingerprint).” Jain ¶[0075]. Thus, Jain discloses performing steps 738, 740, and 742 in the context of biometric verification, where step 738 senses “biometric information” using a biometric sensor (*sensing a physiological parameter*), step 740 retrieves locally stored biometric information, and step 742 determines if the sensed biometric information matches the stored biometric information (*determining whether or not the physiological parameter sensed satisfies a criterion*). EX1002 ¶¶99-100.

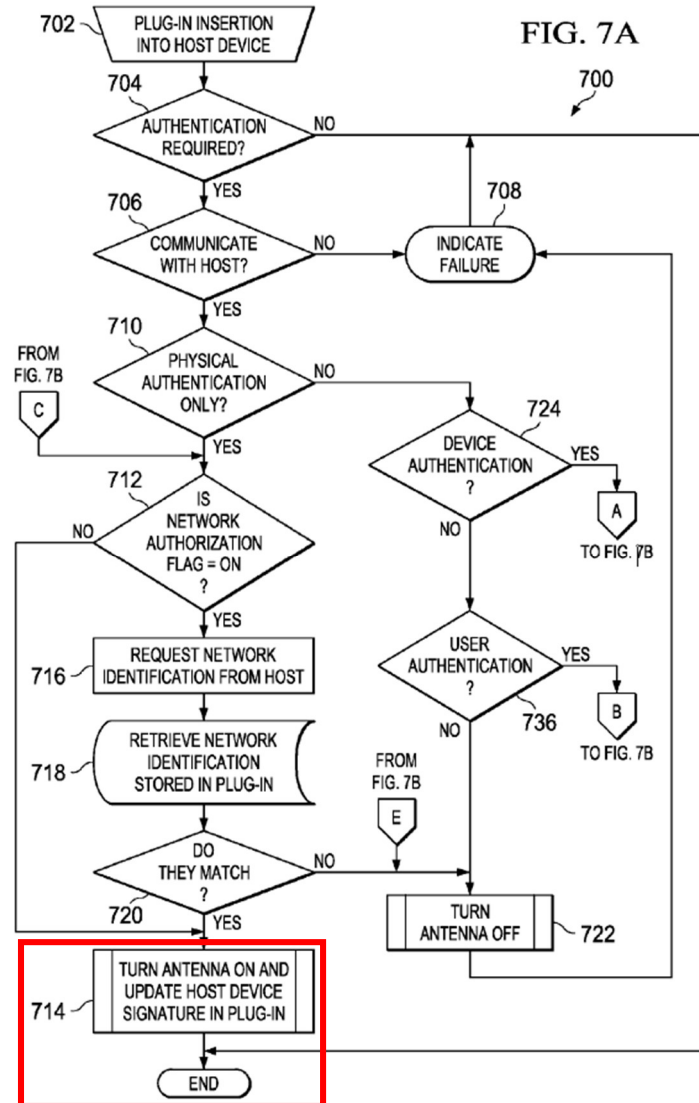
Further confirming this limitation is met, Patent Owner alleges in its infringement contentions in the district court litigation that the use of biometric verification is itself sufficient to show the claimed *sensing* and *determining*. EX1016 at 12-19; *see also* EX1002 ¶101.

At a minimum, it would be obvious to implement Jain’s teaching of “authentication using... biometric information” in this manner, and a POSITA would be well aware of such implementations. *See* EX1021 ¶¶[0040]-[0042]; EX1024 ¶[0009], [0025]; EX1025 ¶[0044], [0086]-[0092]; EX1026 at 28-29, 196;

EX1027 at 1370-73. The purpose of biometric authentication is to ensure biometric information of a current user matches the biometric information of the rightful owner of the device. This entails first storing the biometric information of the rightful owner during a setup stage and then comparing that stored biometric information to the biometric information of a current user sensed via a sensor. The claimed “*criteria*” requires that the stored and sensed biometric information sufficiently correlate such that there is adequate confidence that the current user is the device’s owner. Otherwise, biometric information authentication would not serve its central purpose. EX1002 ¶¶102-104.

- (iv) 1[c]: *responsive to the physiological parameter sensed satisfying the criterion, enabling at least one first function; then*

The next limitation is a second prerequisite to establishing the function to conduct a financial transaction: after *determining* the *criterion* is satisfied, the claims require *enabling at least one first function*. Jain discloses this limitation. In response to authenticating the user in steps 738-744 of Fig. 7B (claimed *determining*), Jain process 700 returns to step 712 (label C in both figures) and proceeds to step 714: “turn antenna on and update host device signature in plug-in” (claimed *enabling*). Jain ¶¶[0072]-[0075], Fig. 7A (annotated). *See also* EX1002 ¶¶105-107.



Once the host-device signature is updated in step 714 to match the host device, the transaction card completes the bootstrap operation and can communicate with the host, which includes using the host's cellular radio technology; otherwise, the "host device is rejected, bootstrap is aborted and the card 400 is returned to the mode it was before being inserted into the device." Jain ¶[0065]. Only after bootstrapping/authentication (Figure 7) is complete can activation (Figure 9) begin, which includes communicating with a financial institution "using cellular radio

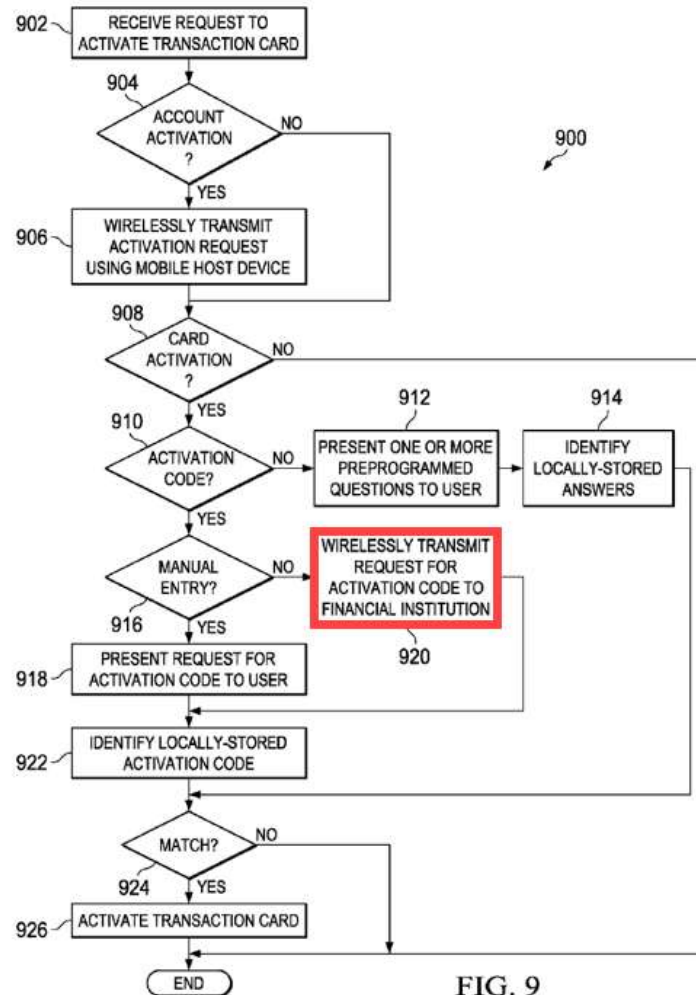
technology of the host device.” Jain ¶¶[0065], [0072] (“an intelligent card may execute one or more authentication procedures prior to activation.”), [0081]. Thus, successful authentication as part of “automatically bootstrapping” (Jain ¶[0072]) allows mobile device 110 to engage in the cellular radio communication with a financial institution as part of process 900 (*enabling at least one first function*). See also EX1002 ¶¶108-111.

- (v) 1[d]: *while said at least one first function is enabled, responsive to having sensed the physiological parameter and responsive to having determined that the physiological parameter sensed satisfies the criterion, requesting an authorization to establish a function to conduct a financial transaction; then*
- (vi) 1[e]: *responsive to the requesting, receiving the authorization to establish the function to conduct the financial transaction; then*
- (vii) 1[f]: *responsive to receiving the authorization, establishing the function to conduct the financial transaction; and then*

Finally, with the claimed *determining* and *enabling* complete, claim 1 recites *requesting* and *receiving authorization* to engage in a *financial transaction*. And thereby *establishing the function to conduct the financial transaction*.

In Jain, after the user is authenticated by PIN or biometrics and while the host device signature allows the mobile device 110 with transaction card 112 to communicate with a financial institution, Jain’s mobile device 110 then performs “method 900 for activating a wireless transaction system” with the financial

institution. Jain ¶[0080]. During step 920 of this method, mobile device 110 “wirelessly transmits a request for the activation code using the cellular radio technology” (*requesting an authorization*) to the financial institution. Jain ¶[0081], Fig. 9 (annotated). *See also* EX1002 ¶¶112-114.



In response to the request of step 924, mobile device 110 receives an activation code (*receiving the authorization*) from the financial institution. The received activation code is then checked against a stored activation code (retrieved at step 922). Jain ¶[0081]. If the activation codes match, “the transaction card is

activated” at step 926. Jain ¶[0081]. This “activation process may include activating the transaction card and/or financial account” (Jain ¶[0026]), which allows the transaction card to then perform payments with the associated financial account by “signifying activation of the financial vehicle carried on the card” (Jain ¶[0071]) (*establishing the function to conduct the financial transaction*). See also EX1002 ¶¶115, 118. For additional disclosure on how the *function to conduct the financial transaction* is established and used in Jain, see discussion of limitations 1[g]-[j].

Thus, step 920 and 924 are performed in order to “activat[e] the transaction card and/or financial account.” Jain ¶[0026]. Because the matching “activation code” is required to enable that card to perform financial transactions (*establish a function to conduct a financial transaction*), a matching “activation code” is an *authorization to conduct a financial transaction*. This mirrors Patent Owner’s infringement contentions, where Patent Owner asserts that “adding credit card” is sufficient to show *requesting* and *receiving* an *authorization to establish a function to conduct a financial transaction* and then *establishing* that function. EX1016 at 26-45. See also EX1002 ¶¶113-117.

A POSITA would further understand that the financial institution would not provide a matching activation code if the smartphone is not authorized to perform payment services with the financial institution. This understanding is supported by step 924, which compares the activation code received by the financial institution

with a locally stored activation code to determine “[i]f the locally stored information matches the provided” activation code. Jain ¶[0081]; Fig. 9; EX1002 ¶117. This step (indeed, the entire requirement for an activation code) would be superfluous if receipt of a matching activation code did not serve an *authorization* function. EX1002 ¶¶113-117.

At a minimum, such an implementation was well known and would have been obvious, as evidenced by numerous references describing similar processes. *See, e.g.,* EX1019 ¶¶[0145]-[0146] (describing “verification process” whereby information is “transmitted to the corresponding credit card provider” so the provider can confirm the information is “valid” and “confirm the identi[ty] of the user by transmitting one or more verification codes” to the user device, thereby “ensur[ing] that only the authorized user or users will receive the verification code”). A POSITA would be motivated to treat Jain’s matching activation code as an authorization (and not provide the same if the transaction card is unauthorized) in order to improve system security and guard against fraudulent transaction cards. Indeed, if Jain’s system returned a matching activation code every time, including in response to requests from fraudulent transaction cards, there would be no reason to implement steps 920-924 of Jain’s process 900. *See also* EX1002 ¶118.

(viii) 1[g][i]: *responsive to satisfying a proximity condition relative to an entity and*

After the claimed *establishing the function*, claim 1 requires *using* the same.

Before getting to the actual *using*, claim 1 defines two prerequisites that have to be met. The first of those is *satisfying a proximity condition relative to an entity*.

In Jain, after completing authentication process 700 (Fig. 7) and activation process 900 (Fig. 9), Jain's mobile device 110 can execute contactless payment transactions with a nearby POS device (*entity*) using short range signals, such as NFC or "proximity signals." Jain ¶[0023]. The mobile device first "wirelessly receive[s] a request from the POS device 114 to execute a transaction and/or and provide a response." Jain ¶[0023]. A POSITA would understand that Jain's mobile device 110 is only able to processes the "request" if sufficiently close to POS device 114 to actually receive and decode the short-range signal corresponding to the request (*responsive to satisfying a proximity condition relative to an entity*). EX1002 ¶¶119-21; EX1034 at 11-12; *see also* EX1036 at 220. Specifically, Jain's NFC and other short range wireless communication protocols are only effective if there is an underlying signal of sufficient strength is detected such that the device and the terminal can communicate using that protocol. EX1002 ¶¶119-21, 123-125; EX1035 at 4, 36; EX1037 at 3. That signal strength rapidly deteriorates as distance increase. EX1002 ¶120; EX1035 at 4, 36; EX1037 at 3. Indeed, Jain itself recognizes that NFC communication requires proximity of "10 cm or less." Jain ¶[0030]. Accordingly, for Jain's mobile device to receive a request from the POS device

received via NFC and process it as such, the mobile device and POS device must be sufficiently close, which a POSITA would understand corresponds to ***satisfying a proximity condition relative to an entity*** (e.g., the device is within a range of “10 cm or less” to the POS device, Jain ¶[0030]).

In addition, the claimed ***satisfying a proximity condition*** also occurs earlier in Jain’s NFC exchange, prior to sending payment information. Jain teaches that its NFC “wireless connection” is based on the “ISO 18092/ECMA 340” standards. Jain ¶¶ [0051], [0018], [0023]. The ECMA 340 Interface and Protocol Standard for NFC¹

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

explains that an NFC “transaction” requires an “initialization” (described in section 11 of the standard) and then a “data exchange” (described in section 12 of the standard). EX1047 at §4.25, §10, Figure 5. The standard specifies two devices (“Initiator” and “Target”) and two communication modes (“Passive” and “Active”). EX1047 §1, §4.1, §4.16, §7. However, it does not matter whether Jain’s POS device or mobile device is the “Initiator,” with the other being the “Target,” or what communication mode they use: every combination results in Jain’s mobile device (*smartphone*) ***satisfying a proximity condition*** and then establishing a link that is used for subsequent communications. Specifically, in both modes, an “Initiator” device “shall activate its RF field” and a “Target” device then “shall be activated by the RF field of the Initiator.” EX1047 at §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, Figure 13, Figures 24-25. Thus, regardless of what mode is being used and which device in Jain is the Initiator and which device is the Target, the Target device detects a sufficiently strong field from the Initiator (***satisfying a proximity condition***), and the Initiator device detects that a Target is within its field by receiving a response to a command from the Target (***satisfying a proximity condition***). In addition, this exchange of commands and responses results in the selection of a particular “Target” and attributes/parameters for further

communication with the same, thereby establishing a link between the Initiator and the Target, which is addressed in more detail in the next limitation. EX1047 §11 and Figure 13 (describing parameters). 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.

At a minimum, it would have been obvious to implement Jain's NFC communications in this manner, because that is the exchange taught by the NFC standard cited in Jain and a POSITA would be motivated to implement the standard rather than define a proprietary approach to simplify design, allow for use of commercially available NFC hardware and software, minimize the need for trial and error, and maximize interoperability with standard-compliant reader/POS systems and mobile devices.

Further confirming this limitation is met, Patent Owner alleges in its infringement contentions in district court litigation that the use of NFC is itself sufficient to show *responsive to satisfying a proximity condition relative to an entity*. EX1016 at 46. *See also* EX1002 ¶122.

In addition, it would be obvious to a POSITA that Jain's smartphone would first detect it is proximate to the POS device (*satisfying a proximity condition*) based on a signal from the POS device (e.g., a "request," Jain ¶[0023], or earlier commands

and responses exchanged as part of implementing ECMA 340) prior to communicating with that POS device. To ensure communications would be successful and not wasted signaling, and further to avoid the security risk of indiscriminately transmitting sensitive financial information, Jain's smartphone first needs to detect it is near the POS device prior to proceeding with a payment transaction with the POS device. EX1002 ¶¶120-25. Otherwise, the NFC communication would fail. Indeed, such implementations were well-known to a POSITA. For example, EX1020 discloses and leverages NFC to limit the range at which communication may take place. EX1020 ¶[0041], [0063] [0041]. Indeed, in the context of Wi-Fi, EX1020 even more explicitly discloses using the ability to receive such signals as an indication of proximity. Jain ¶[0073] ("The [identifying information] may be used by the device 10 to indicate that the device is located within communication range of the hot spot 169."). A POSITA would be motivated and able to use Jain's "request" or ECMA 340's commands and responses in the same manner. EX1002 ¶¶120-25.

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

signaling, and further to avoid the security risk of indiscriminately transmitting sensitive financial information, Jain's smartphone first needs to detect it is near the POS device prior to proceeding with a payment transaction with the POS device. EX1002 ¶¶120-25. Otherwise, the NFC communication would fail. Indeed, such implementations were well-known to a POSITA. For example, EX1020 discloses and leverages NFC to limit the range at which communication may take place. EX1020 ¶[0041], [0063] [0041]. Indeed, in the context of Wi-Fi, EX1020 even more explicitly discloses using the ability to receive such signals as an indication of proximity. Jain ¶[0073] ("The [identifying information] may be used by the device 10 to indicate that the device is located within communication range of the hot spot 169."). A POSITA would be motivated and able to use Jain's NFC "request" or ECMA 340's commands and responses in the same manner. EX1002 ¶¶120-25.

(ix) 1[g][ii]: *responsive to sensing the physiological parameter and determining that the physiological parameter sensed satisfies the criterion,*

The second prerequisite in claim 1 to *using* the claimed *function to conduct the financial transaction* is *sensing the physiological parameter and determining that the physiological parameter sensed satisfies the criterion*.

According to Patent Owner, limitation 1[g][ii] does not impose any new requirement relative to limitations 1[a] and 1[b]: the same sensing of *the* at least parameter and determining it meets *the* criterion prior to establishing the function to

conduct the financial transaction is also a prerequisite to then **using** that function. Compare EX1016 at 46-49 with EX1016 at 56-59 (pointing to the same “fingerprint unlock” and similar security functionality for both limitations). See EX1002 ¶¶126-127.

Even if the claims require an additional transaction-specific **sensing** and **determining**, Jain discloses or renders this limitation obvious. For example, Jain discloses that during payment, the merchant terminal may “prompt the user to authorize a transaction such as by entering a PIN.” Jain ¶[0029]. Jain further discloses that this “PIN request” is presented and user information is received via GUI 111 of mobile device 110. Jain ¶[0023]-[0025]. See EX1002 ¶128.

Jain’s disclosure of authorizing individual transactions via PIN also renders obvious doing so via biometrics (**sensing ... and determining**). Jain already contemplates using biometrics (*e.g.*, fingerprints) for its user authorization process (Jain ¶[0075], Figure 7), and reusing that software and hardware for individual transactions would not further complicate the system or incur material additional costs. EX1002 ¶128. Moreover, Jain itself recognizes that biometrics are a good alternative to PINs. In addition, a POSITA would recognize advantages of biometrics over PINs, including that biometrics cannot be forgotten or obtained by a bad actor via, *e.g.*, phishing, and that use of biometrics for authorizing individual transactions would thus further improve system security. Alternatively, POSITA

would also be familiar with two-factor authentication and would both (a) know how to retain PIN authentication while augmenting it with biometric authentication and (b) appreciate that the cost of doing so is warranted because of the extra security it provides for financial transactions. EX1002 ¶129; 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 ¶¶103-104, 127-29. In addition, for the reasons discussed above in connection with limitation 1[a]-[b], Jain discloses or at least renders obvious that implementing biometric authorization would entail the claimed *sensing* and *determining*.

- (x) 1[g][iii]: *using the function that has been established to conduct the financial transaction and conducting the financial transaction by paying for a product;*

After *establishing the function to conduct the financial transaction* (limitations 1[a]-[f]), and after the prerequisites related to *a proximity condition* (limitation 1[g][i]) and *the physiological parameter* (limitation 1[g][ii]) are met, claim 1 then requires using the *function to pay for a product*.

Jain discloses using mobile phone 110 with an authenticated and activated transaction card 112 to “wirelessly execute[] financial transactions with a retail terminal,” at for example an “offline store” that “sell[s] goods and/or services at a

physical location (e.g., a brick-and-mortar store).” Jain, Abstract, ¶¶[0019], [0020], [0023], [0027]-[0029]. *See also* EX1002 ¶¶130-31.

- (xi) 1[h]: ... *sensing that the proximity condition is satisfied relative to an access point maintained by a vendor at a point of purchase counter, by detecting a short-range signal that is transmitted by the access point ... and then ... paying for the product by selectively sending information to at least one device;*

Limitation 1[h] for the most part just repeats the requirements of limitation 1[g] and only further specifies that (1) the *satisfying* is “*relative to an access point maintained by a vendor at a point of purchase counter*” and implemented by “*detecting a short-range signal that is transmitted by the access point*”; and (2) the *paying* is done by *selectively sending information to at least one device*.

The first new requirement is addressed above in connection with limitation 1[g][i], since the POS device in Jain is *an access point maintained by a vendor* (e.g., an offline store selling produce), where the location of the POS (point-of-sale) device is the *point of purchase counter*, and the request or ECMA 340 message used to perform the *detecting* is a *short-range signal* (e.g., an NFC signal). Jain ¶[0020], [0023], [0029]; *see also* EX1002 ¶¶132-134.

For the second new requirement, Jain discloses that its mobile device, in response to a request from the POS device, generates a transaction response 119 identifying information associated with a payment account (*information*) and

send[s] the transaction response 119 to the nearby POS device 114 (*at least one device*).² Jain ¶¶[0027], [0029]. This sending is *selective* because it only occurs if the mobile device is sufficiently close to the POS device 114 and the user has authorized the purchase. *See supra* limitations 1[g][i]-[ii]. *See also* EX1002 ¶¶133-134.

(xii) 1[i]: ... *selectively and wirelessly transmitting information to the at least one device using unlicensed frequencies; and*

The only additional requirement of limitation 1[i] is that the “information” of limitation 1[h] is sent *wirelessly using unlicensed frequencies*. Jain meets this requirement by transmitting information to the POS device (*at least one device*) “using short range signals such as NFC (*e.g.*, ISO 18092/ECMA 340), ... proximity signals, and/or other signals compatible with retail payment terminals (*e.g.*, POS 114).” Jain ¶[0023]; *see also* EX1002 ¶¶135-36.

NFC used the 13.56 MHz ISM band, which is unlicensed. EX1002 ¶137; EX1031; EX1032 at 2. Patent Owner, in its infringement contentions, admits as much, alleging that “the wireless short-range communications link used by NFC is

² According to Patent Owner’s infringement contentions, the claimed *access point* and claimed *at least one device* can be one and the same device. EX1016 at 56, 70 (pointing to “the point-of-sale device” or “terminal” for both limitations).

based upon the unlicensed 13.56 MHz frequency.” EX1016 at 70; EX1002 ¶138.

Bluetooth also used unlicensed frequencies. EX1002 ¶139; EX1041.

(xiii) 1[j]: *wherein said paying for a product further comprises deducting/withdrawing an amount of money from an account.*

Jain discloses that when paying for products, the smartphone sends transaction information corresponding to credit, debit, or bank accounts. Jain ¶¶[0025], [0029], [0036]. Payments using such accounts, particularly debit accounts and bank accounts, constitute *deducting / withdrawing an amount of money from an account*. As explained, “[t]he financial institution 106 may be a credit card provider, a bank, an association (*e.g.*, VISA), a retail merchant (*e.g.*, Target), a prepaid/gift card provider, an internet bank, and/or others.” Jain ¶[0039]. During a transaction, the financial institution “may identify an account number (*e.g.*, bank account, debit-card number) and associated verification information (*e.g.*, PIN, zip code) and determine funds available to the account holder.” Jain ¶[0039]. Jain also explains that the merchant “POS 114 may receive an indication that a transaction amount has been accepted or declined for the identified account and/or request additional information from the transaction card.” Jain ¶[0036]; *see also* EX1002 ¶¶140-41.

(b) Claim 2

(i) 2[pre][i]

Claim 2, *supra*.

(ii) 2[pre][ii]

First, Jain’s smartphone bootstrapping/authentication process enables the mobile device 110 to communicate with the financial institution using cellular radio technology. *See* limitations 1[c]. Even after the mobile device is able to communicate with the financial institution using cellular radio technology (***enabling first function***), the mobile device remains unable to engage in payment transactions (***disabling a second function***) because the transaction card is not yet activated. Jain ¶[0081]. Only once activation process 900 in Fig. 9 is also complete can the mobile device engage in financial transaction (***second function***). EX1002 ¶¶143-144.

Second, Jain meets this limitation by ***enabling a first function*** (enabling mobile device 110 to communicate with the financial institution using cellular radio technology in connection with process 900) and ***disabling a second function*** (mode the transaction card was in before being inserted into the device). In its infringement contentions, Patent Owner argued that limitation 2[a] is met by “enabling a first function (unlocking the [] smartphone or application) while disabling a second function (locking the Samsung smartphone or application).” EX1016 at 73-81. Similarly, Jain’s authorization process 700 (Fig. 7) must be completed before turning on the antenna and updating the host device signature (step 714) to enable cellular communication with the financial institution (***enabling a first function***), as described in connection with process 900. Jain ¶[0073]. Jain also describes a “mode it was before being inserted into the device,” which is capable of “automatically

bootstrapping an intelligent card in response to at least insertion into a host device” (*second function*). Jain ¶[0065], [0072]. Completing process 700, thereby turning on the antenna and updating the host signature to enable cellular communication with the financial institution (*enabling a first function*) causes the system to no longer be in this pre-insertion mode with associated capabilities (*disabling a second function*), as evidenced by Jain’s disclosure that, if process 700 fails, the “host device is rejected, bootstrap is aborted and the card 400 is **returned** to the mode it was before being inserted into the device.” Jain ¶[0065] (emphasis added). EX1002 ¶¶145-47.

(iii) 2[a]

Limitation 2[a] performs the steps of limitations 1[a]-1[c] *repeatedly* and based on the result of the claimed *sensing* and *determining* decides whether to maintain the *first function* and keep the *second function disabled*.

As discussed above in connection with limitation 2[pre][ii], in Jain, the *first function* corresponds to use of radio communication with the financial institution in connection with process 900 and the *second function* corresponds either to the capability to engage financial transactions or the mode the transaction card was in before being inserted into the device. *See also* EX1002 ¶148-149, 153. Either way, it would be an obvious security measure to repeatedly perform Jain’s user authentication process in steps 734-742 of process 700 (*repeatedly sensing the at*

least one parameter and repeatedly deciding), such as prompting for a PIN or biometric, when, for example, sufficient time has passed, there is network delay, or there was a change to the smartphone with potential security implications. EX1002 ¶¶150-151. Requiring re-authorization and re-activation under those circumstances would help prevent fraud. EX1002 ¶151. With this obvious modification, the other claim elements also fall into place.

First, to further ensure security, the activation process 900 of Fig. 9 would also need to be repeated, leaving the mobile device unable to perform financial transactions until that re-activation is complete (*while maintaining disabled said second function*). EX1002 ¶152.

Second, as discussed above in connection with limitation 2[pre][ii], Jain discloses *enabling a first function* (enabling mobile device 110 to communicate with the financial institution using cellular radio technology in connection with process 900) and *disabling a second function* (the mode the transaction card was in before being inserted into the device) based on whether process 700 (including user authorization steps 734-742) is successfully completed. Jain ¶[0065] (teaching, if process 700 is unsuccessful, “returned to the mode [the transaction card] was before being inserted into the device”); EX1002 ¶153. If steps 734-742 are repeated, then the same *enabling* and *disabling* would occur after each repetition. *See also* EX1016

at 73-81 (accusing analogous repetition of locking or unlocking device based on user authentication).

(iv) 2[b]

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

As discussed re 2[pre][ii] and 2[a] above, Jain *maintain[s] enabled* the ability to engage in cellular communications with a financial institution as part of activation process 900 (*first function*) while *maintain[s] disabled* the card's payment services (*second function*) until that activation process 900 is complete, even after deciding that the smartphone user is still authorized. EX1002 ¶¶154-55.

Alternatively, as discussed re 2[pre][ii] and 2[a] above, Jain *maintain[s] enabled the first function* (enabling mobile device 110 to communicate with the financial institution using cellular radio technology in connection with process 900) *while maintaining disabled the second function* (the mode the transaction card was in before being inserted into the device) based on deciding that the smartphone user is still authorized. EX1002 ¶156.

(v) 2[c]

Alternatively, Jain discloses limitation 2[c] when it disables cellular communications with the financial institution by returning to the mode the transaction card was in before being inserted into the device when the user is not

authenticated responsive to the ***repeatedly sensing*** (Jain ¶[0065]), similar to Patent Owner’s theory of locking and unlocking the smartphone’s screen. EX1016 at 73-81; *see also* EX1002 ¶¶157-178.

(c) **Claim 3**

(i) **3[pre]**

Claim 1, *supra*.

(ii) **3[a]**

Jain discloses, as part of conducting a financial transaction, receiving first a transaction request 117 (***information***) and an authorization response 120 containing a transaction receipt (***information***) from POS device 114 (***at least one device***) using NFC or Bluetooth. Jain ¶[0023], [0025], [0027], Fig. 1. The authorization response with the transaction receipt (***information***), as well as requests for transaction histories (***information***), can also be received from the financial institution using either cellular communication or Wi-Fi. Jain ¶[0027], [0041], [0046], [0053], [0068], Fig. 5. EX1002 ¶160.

Jain’s NFC, Bluetooth, and Wi-Fi all use ***unlicensed frequencies***. Jain ¶[0023]. According to Patent Owner, “NFC communications”—which includes the NFC communications disclosed in Jain—use “***unlicensed frequencies***.” EX1016 at 70 (emphasis added); EX1032 at 2; EX1002 ¶¶161-64. Same is true for Bluetooth and Wi-Fi. EX1002 ¶163; *see also* EX1038 at 1; EX1043; EX1044.

(d) Claim 4

(i) 4[pre]

Claim 3, *supra*.

(ii) 4[a]

Limitation 4[a] requires that the wireless transmitting and receiving of limitations 1[h] and 3[a] be done using ***unlicensed frequencies over a short-range link in a Time Division Duplex operation***.

Jain teaches the sending and receiving of limitations 1[h]-[i] and 3[a] is done via NFC, Bluetooth, or Wi-Fi. Jain ¶[0023], *see also* EX1002 ¶166-67. According to Patent Owner, “NFC communications”—which includes the NFC communications disclosed in Jain—use “***unlicensed frequencies... in a Time Division Duplex operation***.” EX1016 at 100 (emphasis added); EX1032 at 21 (describing NFC as a “half... duplex system”); EX1002 ¶168. Bluetooth and Wi-Fi also use ***unlicensed frequencies in a Time Division Duplex operations***. EX1002 ¶¶169-70; *see also* EX1038 at 1; EX1044 at 251.

(iii) 4[b]

Limitation 4[a] mostly repeats the requirements of limitations 1[h]-[i] and 3[a] but further adds that the information of limitations 1[h]-[i] and 3[a] is transmitted to and received from ***the access point maintained by the vendor at the point of purchase counter*** and adds the further requirement of transmitting information to

and receiving information from ***at least one other device that is predetermined***. Jain discloses both limitations.

In the discussion above for limitations 1[h]-[i] and 3[a], the claimed ***information*** is already transmitted to and received from Jain's POS device (***access point***).

Jain also discloses sending the transaction response 119 identifying information associated with a payment account to the POS device 114 (***access point***), which is then forwarded to the financial institution (***at least one other device that is predetermined***). Jain ¶¶[0027], [0029]; *see also* EX1002 ¶173. Jain's mobile device also receives the authorization response with the transaction receipt from the POS terminal (***access point***) that was originally sent by the financial institution (***one other device that is predetermined***). Jain ¶[0027]; *see also* EX1002 ¶¶171-73.

Also, Patent Owner's infringement contentions rely on the theory that the accused devices "send[s] information (e.g., a transaction-specific dynamic digital token) to the access point maintained by the vendor at the point of purchase counter (the point-of-sale terminal, which includes an access point) and to at least one other device that is predetermined (a base station)." EX1016 at 102-103. Applying this theory to Jain, Jain's smartphone also transmits data to and receives a transaction receipt from numerous intermediary devices, including network 108, GSM core network 202, RAN 204, MSC 206, Base Station Controllers (BSC) 212, Base

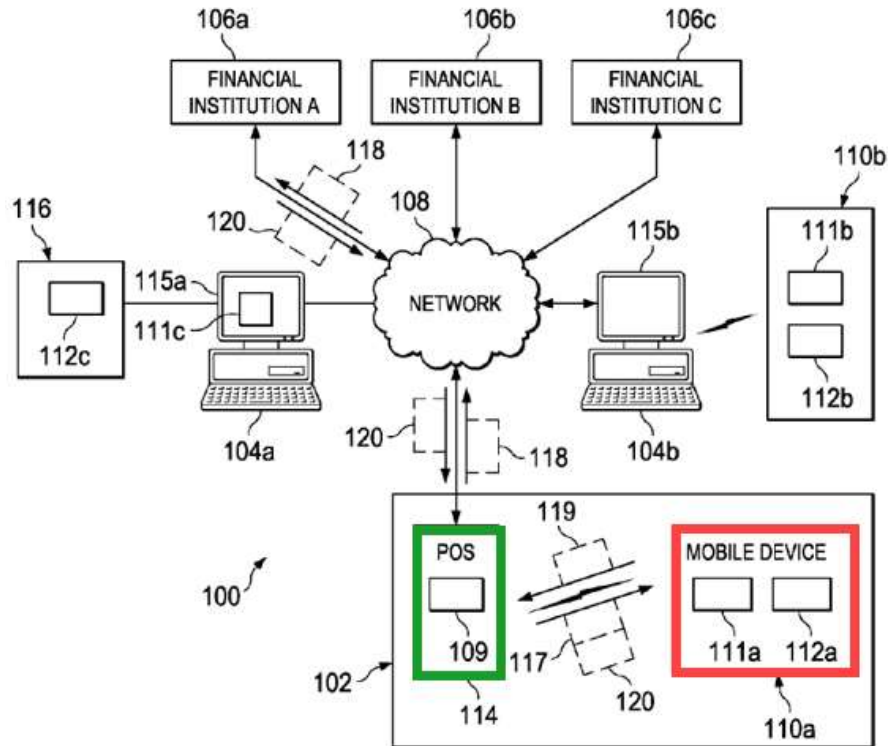
Stations (BS) 210, and/or client 115 (*one other device that is predetermined*) on the way to/from the financial institution. Jain ¶[0044]; Figs. 1-2, 5; EX1002 ¶173.

Finally, to the extent Patent Owner argues the claimed *transmitting* and *receiving* to/from the *one other device that is predetermined* cannot be via the claimed *access point*, Jain also discloses that such communication (including authorization responses and requests for transaction history) can bypass the POS device by using the cellular core network or Wi-Fi. Jain ¶[0027], [0046]; *see also* limitation 3[a], EX1002 ¶174.

(e) Claim 5

Claim 5 is substantively identical to claim 1 and only further adds that the steps of claim 1 be implemented by *a wireless device that comprises a smartphone and a sensor* and that the *authorization* is requested and received from *a second device*. See EX1002 ¶175.

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



For example, Jain’s Figure 1 shows a customer’s mobile device 110a with transaction card 112a and GUI 111a (red box) wirelessly executing transactions with a nearby POS device 114 (green box). Jain ¶[0019]. The mobile device and POS device also communicate with financial institution 106 (*second device*).³

³ Jain uses the term “financial institution” to refer to devices, such as devices in an enterprise that authorize transactions through the network 108 by accepting data from clients and returning appropriate responses using, for example, the HTML or XML formats. Jain ¶¶[0038], [0039].

Jain interfaces the mobile device 110 (e.g., “a smartphone” (¶[0018])) with a transaction card 112 that “convert[s] the mobile device 110 to a contactless payment device loaded with a financial vehicle (FV) that may be, for example, a credit card, a debit card, a gift card and/or other retail payment product” (¶[0029]). In such embodiments, transaction card 112 is included as part of the mobile device 110 (i.e., the smartphone). Jain ¶[0019] (“The offline store 102 includes a mobile device [110a⁴] having a transaction card 112a and a Point of Sale (POS) device 114 that executes transactions with customers.”), Fig. 1 (showing transaction card 112a within mobile device 110a). *See also* EX1002 ¶¶90-91.

Moreover, a POSITA would also understand that Jain’s transaction card 112 can be considered part of mobile device 110, because Jain at least renders obvious implementing the processes discussed herein in connection with a transaction card 112 that is integrated into mobile device 110. EX1002 ¶176. A POSITA would make this change because separability of the transaction card is not always advantageous (e.g., a smartphone vendor might find it commercially advantageous to provide transaction card functionality with their smartphone but not allow users to leverage

⁴ The reference to “10a” in the specification is an obvious typographic error. No figures show a “10a” and Jain’s Figure 1 clearly shows element 110a that matches the description of “10a” in the specification.

that functionality with other devices). EX1002 ¶176. Also, integrating transaction card 112 with mobile device 110 allows the host device to achieve the benefits disclosed in Jain without incurring the cost of implementing an independent transaction card and while leveraging components of the mobile device 110. EX1002 ¶176. Finally, incorporating transaction card 112 into mobile device 110 protects against inadvertent loss of the transaction card 112 if it were to, *e.g.*, become detached from mobile device 110 without the user noticing. EX1002 ¶176.

Finally, Jain discloses that “[w]hile the user authentication is described with respect to entering a PIN through the mobile host device, the user may be authenticated using other information such as biometric information (*e.g.*, fingerprint).” Jain ¶[0075]. Based on this, a POSITA would understand that Jain’s mobile device has a fingerprint scanner (*sensor*) to implement this functionality. At a minimum, it would be obvious to implement Jain’s disclosure of using fingerprints in this manner, as addressed above in connection with limitations 1[a] and [b].

(f) Claim 7

(i) 7[pre]

Claim 5, *supra*.

(ii) 7[a]

Jain discloses the mobile device with the transaction card performing transactions with a nearby retail POS terminal 114 (*entity*) by sending requests and responses between one another over a “wireless connection (*e.g.*, NFC ...)” (*a short-*

range wireless link”). See Jain ¶¶[0018] (reciting “wireless connection (e.g., NFC...)”), [0019], [0023], [0027], [0029], [0051], [0054]. This is addressed in more detail in the ECMA 340 standard implemented by Jain (*see* limitation 1[g][i]), which describes an “Initiator” device and a “Target” device exchanging communications to select a particular “Target” and attributes/parameters for further communication (*establishing ... a short-range wireless link*). Indeed, Patent Owner’s infringement contentions allege the use of NFC as sufficient to show *establishing ... a short-range wireless link*. EX1016 at 212-213; see also EX1002 ¶179-80.

(iii) 7[b] & 7[c]

As addressed above in connection with limitations 1[h]-[i] and 3[a], the mobile device with a transaction card (*wireless device*) receives a transaction request and transaction receipt from and transmits a transaction response to the POS device (*entity*) using NFC or Bluetooth (*wirelessly* and *using unlicensed frequencies*). EX1002 ¶181.

(iv) 7[d]

As addressed above in connection with limitation 4[a], NFC and Bluetooth use *unlicensed frequencies in a time division duplex operation*. EX1002 ¶¶182-86.

(v) 7[e]

This limitation further requires that the *establishing the short range link* occur *responsive to the wireless device satisfying the proximity condition relative to the entity* (addressed above in connection with limitation 1[g][i]) and *responsive*

to the wireless device sensing the parameter and determining that the value associated therewith satisfies the threshold criterion (addressed above in connection with limitations 1[a]-[c] and 1[g][i]). Jain discloses both requirements.

Responsive to ... satisfying the proximity condition: As addressed in more detail above in connection with limitations 4[a] and 17[a], the NFC standard implemented by Jain teaches or at least renders obvious conducting a command/response exchange that concludes with the “Initiator” device selecting one or more “Target” devices and attributes/parameters for communication (*establishing ... a short-range wireless link*) after the “Initiator” and “Target” first detect RF signals from each other (*responsive to ... satisfying the proximity condition*). EX1002 ¶¶187-88.

Responsive to .. sensing ... and determining: As addressed above in connection with limitation 1[a]-[f], Jain’s mobile device with a transaction card (*wireless device*) is only able to process a transaction request from POS device 114 if the user previously completed process 700, including the PIN or biometric user authentication portion thereof, to enable the corresponding antenna, update the host signature, and thereafter complete activation process 900 (*responsive to ... sensing ... and determining*). EX1002 ¶188.

At a minimum, it would be obvious to a POSITA that Jain’s smartphone would establish a NFC connection with the POS device (*establishing ... a short-*

range wireless link) after detecting *satisfying the proximity condition* and the claimed *sensing ... and determining*. To ensure communications would be successful and not wasted signaling, and further to avoid the security risk of indiscriminately transmitting sensitive financial information, Jain's smartphone needs to detect proximity and then establish a short-range communications link with the POS prior to proceeding with a payment transaction with the POS device. EX1002 ¶189. Use of a link after detecting proximity further improves reliability and security, because once a link is established, Jain's mobile device can receive confirmation of receipt of individual packets. Indeed, such implementations of devices communicating via NFC establishing a connection prior to transmitting information were well-known to a POSITA. EX1019 ¶¶[0011], [0124], [0182]. For example, in Lin, "to facilitate the establishment of an NFC connection (e.g., typically 2-4 cm)" (*satisfying the proximity condition*), an "RF field generated by the payee device [] may induce [] transition to an active mode of operation, thus establishing an NFC connection between the two devices." Lin ¶[0124]. "Accordingly, by way of this established NFC connection, the payment [information] may be transmitted to and received by the payor device." *Id.*

At a same time, it would be undesirable from the perspective of the POS device to establish a link before the user of the device has been authenticated (e.g., via the biometric processes discussed in connection with limitation 1[g][ii]), since

the established link can then be hijacked by other, unauthorized processes if the device is in the possession of an unauthorized user. Accordingly, a POSITA would be motivated to delay completion of the ECMA initiation process (described above in connection with limitation 1[g][i]) to *establish[] ... a short-range wireless link* until after the user has completed the biometric authorization process (described above in connection with limitation 1[g][ii]) (*responsive to the wireless device sensing ... and determining*). See EX1002 ¶190.

(g) Claim 8

(i) 8[pre]

Claim 5, *supra*.

(ii) 8[a]

Jain discloses that the mobile device 110 with transaction card 112 (*wireless device*) can communicate with a financial institution (*second device*) using cellular radio technology. Jain ¶[0021], [0041], [0081], Fig. 2. A POSITA would understand that communicating using cellular radio technology involves establishing a *link* to the recipients, including via, for example, packet switching. Jain ¶¶[0041]-[0043] (“establishing connections between packet-switched networks and communication devices” where a financial institution is part of a packet switched network), [0046], [0081]; *see also* Jain FIG. 2. Indeed, Patent Owner’s infringement contentions allege the use of mobile data as sufficient to show *establishing ... a link*. EX1016 at 231. See EX1002 ¶193.

Plus, to improve reliability, a POSITA would further implement this communication using TCP, a very well-known connection-based protocol that is even referenced in Jain itself. Jain ¶[0052]. Moreover, part of this *link*, from mobile device 110 to base station 210, is a *wireless link*. Jain Fig. 2. *See* EX1002 ¶194.

As an alternative to cellular radio technology, Jain also discloses “the mobile device 110 [can] transmit packet data using its own connection to the external world (e.g., SMS, cellular, **Wi-Fi**).” Jain ¶[0053] (emphasis added); *see also* Jain at claim 13, 14. This includes using “WiFi technology” to “wirelessly interface” with financial institutions. Jain ¶[0068], Fig. 5. As with cellular radio technology, this use of Wi-Fi involves establishing a *link*, part of which (from mobile device 110f to client 104e) is a wireless. Jain ¶[0068], Fig. 5. *See* EX1002 ¶195.

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

As addressed above in connection with limitations 1[d] and 1[e], Jain discloses that mobile device 110 “wirelessly transmits a request for the activation code using the cellular radio technology” to the financial institution (*wirelessly transmitting information to the second device over said wireless link*) and receives an activation code back from the financial institution (*wirelessly receiving information from the second device over said wireless link*). Jain ¶[0081]. Moreover, a POSITA would understand that transmissions over “cellular radio technology” use *licensed frequencies*. EX1002 ¶196. If they do not, then they use

unlicensed frequencies, which is also claimed. EX1002 ¶197. Either way, this limitation is met.

Finally, as addressed above in connection with limitation 8[a], Jain discloses using Wi-Fi instead of cellular radio technology for requesting and receiving the activation code (*wirelessly transmitting information* and *wirelessly receiving information*). A POSITA would understand that transmissions over Wi-Fi use *unlicensed frequencies*. EX1002 ¶196. If they do not, then they use *licensed frequencies*, which is also claimed. EX1002 ¶197.

(iv) 8[d]

Limitation 8[e] lists specific protocols that need to be used for the *transmitting* and *receiving* of limitations 8[c] and 8[d]. In Jain, these steps involve communications with a financial institution using cellular radio technology. Jain ¶[0081]; *see also* EX1002 ¶198. The cellular radio technology in Jain includes GSM, CDMA, UMTS, and other modes. Jain ¶[0041]. A POSITA would be motivated to use the most advanced and performant cellular radio technologies such as LTE and WiMAX (a competitor to LTE) (also known as 4G cellular technologies), well-known next generation technologies for cellular communications, in addition to the cellular radio technology explicitly mentioned in Jain to keep up with ever-evolving technologies that allow for higher data rates and that even as of the priority date of the '743 patent were known to a POSITA to be in line to displace older technologies

in the near future. EX1002 ¶198; *see also* EX1045, EX1046. Wi-Max and LTE both use both ***Orthogonal Frequency Division Multiplexing air interface protocol*** and ***an Orthogonal Frequency Division Multiple Access air interface protocol***. EX1002 ¶198; *see also* EX1045, EX1046.

Finally, as addressed above in connection with limitation 8[a], Jain discloses using Wi-Fi instead of cellular radio technology for requesting and receiving the activation code (***wirelessly transmitting information*** and ***wirelessly receiving information***). Jain's Wi-Fi is ***a WiFi air interface protocol***. EX1002 ¶198; *see also* EX1043, EX1044.

(v) 8[e]

As addressed above in connection with limitation 1[a]-[f], Jain's mobile device with a transaction card (***wireless device***) only proceeds to activation process 900 and the associated communicating with the financial institution (***establishing by the wireless device a link with the second device***) after completing authentication process 700, including user authentication via PIN or biometrics (***responsive to ... sensing ... and determining***). EX1002 ¶199-200.

(h) Claim 9

Claim 9 is a broader version of claim 4 (only applying to ***transmitting*** or ***sending*** as opposed to both ***wirelessly transmitting*** and ***wirelessly receiving***) and only further adds that the steps of claim 4 are implemented by the ***wireless device*** of

claim 5. EX1002 ¶201. The use of the word *selectively* also does not add a meaningful limitation, since at least the authorization response 120 containing a transaction receipt (*information*) in limitations 3[a], which in turn is referenced in limitation 4[b], is received only if a transaction is successfully executed (*selectively*). For the reasons set forth above in connection with claims 4 and 5, Jain also discloses claim 9. EX1002 ¶202.

(i) Claims 6, 10-11

Claims 6, 10-11 are substantively identical to claims 2-4 and only further add that the steps of claims 2-4.

B. Ground 2: Dua (EX1018)

1. Background

Dua is prior art under at least pre-AIA 35 U.S.C. § 102(b), having been published on July 27, 2006, and thus more than a year before the earliest effective filing date of the '793 patent. Dua discloses all limitations of the '793 patent claims, but Petitioner presents Dua as an obviousness reference in the event Patent Owner identifies any differences between Dua's disclosure and the '793 patent claims.

Dua was cited during prosecution of the '793 patent, but was only relied upon for rejections in the prosecution of related patents (the '015 and '432 patents) that contain substantially different limitations. EX1008 at 212-213; EX1009 at 171. Also, during prosecution of the '432 patent, applicant argued, and the examiner agreed, that paragraphs [0026], [0089], and [0495] from the application publication

version of Dua 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.

While each limitation is addressed in the “Analysis” section below in detail, given the repetitive and nonsequential nature of the ’793 patent’s claim language, below is a short, non-limiting overview of Ground 2:

’793 patent claim 1 can be divided into two parts: first establishing a function to conduct a financial transaction, and then conducting such a financial transaction. Those steps are broken down in Section VIII.A.1 above.

For the claimed *first step*, Dua discloses (1) performing PIN or biometric authentication to open a wallet application; (2) once the wallet is opened, establishing a SIP communication session with a credit card issuer’s wireless credential manager; and (3) using the SIP communication session to receive credentials from the wireless credential manager. After receiving/retrieving credentials under either theory, Dua then discloses the claimed *second step* by (1) requiring the user to authenticate via PIN or biometrics or requiring receipt of a reader key; (2) requiring that the user device is sufficiently close to a point-of-sale terminal to engage in a transaction; and (3) if both conditions are met, transmitting

the received/retrieved credentials to the point-of-sale terminal to perform the transaction.

2. Analysis

(a) Claim 1

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

Dua discloses a method for obtaining a credit card from an issuer's Wireless Credential Manager (WCM) (Dua ¶[0128]) and then using that credit card for a subsequent "authorized transaction... via... a short range wireless link with a point-of-sale... terminal" (Dua Abstract). EX1002 ¶212.

(ii) 1[a]: *sensing a physiological parameter; then*

(iii) 1[b]: *determining whether or not the physiological parameter sensed satisfies a criterion; then*

(iv) 1[c]: *responsive to the physiological parameter sensed satisfying the criterion, enabling at least one first function; then*

The claim begins with a prerequisite to establishing the function to conduct a financial transaction: (1) *determining* if a *criterion* is satisfied; and (2) *enabling at least one first function*.

In Dua, the wallet application must be opened for the wallet application to be issued a credit card. Dua ¶¶[0128]-[0129], [0178], [0180], [0250]. Thus, the "default security setting in the wallet application is that PIN-entry is required before the wallet application can be 'opened'" or otherwise "allow[s] the user access to the

application,” which receive an issued a credit card. Dua ¶¶[0366], [0429]. This understanding is confirmed by additional disclosure in Dua. **First**, using the wallet application requires authentication because “[d]ata in the wallet application is encrypted and protected with a special wallet PIN code.” Dua ¶¶[0366], [0429]. **Second**, Dua requires user authentication for making significant changes in the wallet application, such as “access[ing] stored credentials and chang[ing] any application settings or preferences.” Dua ¶[0366]. Adding a new credit card is such a change. **Third**, a wallet application can hold many pieces credit card and other confidential information. Dua ¶¶[0041], [0055], [0287]-[0288], [0334]. Regardless of how the wallet is opened, the wallet application allows the user to navigate and view the stored credentials and thus needs to be protected. Dua ¶¶[0324]-[0332], [0334], [0366], [0378]. *See also* EX1002 ¶¶213-215.

Further, a feature within a wallet/payment application to add an account or credit cards is well known to a POSITA. EX1002 ¶216; EX1019 ¶¶[0136]-[0140], Figs. 5A-B; EX1021 ¶[0047]; EX1039 ¶[0117]. A POSITA would be motivated to incorporate that feature in the wallet application because it improves the wallet application’s utility regarding credit card management. EX1002 ¶¶216-218.

At a minimum, requiring PIN entry under these circumstances would be obvious. To ensure security of the other credentials, alongside allowing use of an encrypted wallet application and changes to the wallet application by an

authenticated user, a POSITA would retain Dua's "default" user authentication—PIN-entry—for credit card issuance. Dua ¶[0366]. Indeed, it was well known to require such verification before permitting access to such sensitive functionality. EX1019 ¶[0107], Fig. 10A, 10B; EX1002 ¶¶217-18.

For Dua's PIN-entry, the wireless device receives a PIN code (*parameter*) through a PIN entry or text field after the PIN code is typed in with a keyboard or touchscreen keyboard (*sensing a ... parameter*), which a POSITA would also understand as a sensor for sensing touch (*e.g.*, capacitive touch screen). Dua ¶¶[0366], [0384], [0395], FIGS. 1, 3, 6(a), 8, FIG. 9; EX1042. The entered PIN code is then used to decrypt data or otherwise matched against a validation PIN code stored on the wallet application, thereby validating the user's identity (*determining whether or not the ... parameter sensed satisfies a criterion*). Dua ¶¶[0050], [0366], [0399], [0429]; *see also* EX1002 ¶215.

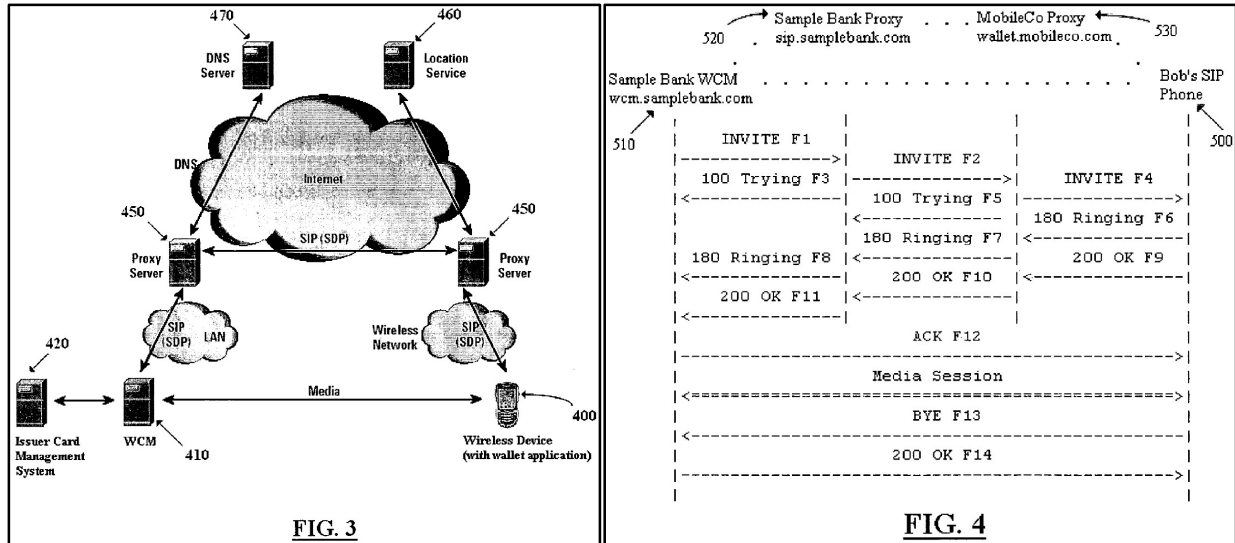
Due further teaches that PIN codes can be replaced with fingerprints (*physiological parameter*) scanned by the "wireless device's embedded biometric technologies," which involves biometric sensors (*sensing a physiological parameter*). Dua ¶¶[0366], [0414]. Dua also contemplates other biometric data, including "iris, voiceprints, facial recognition, and hand geometry." Dua ¶[0534]. A POSITA would understand that using biometric data, like a "fingerprint[,] in lieu of a PIN code to authenticate a user to the wallet application," involves determining if

the scanned biometric data matches the biometric data stored on the wireless device or, as also disclosed by Dua, determining if the scanned biometric data can decrypt the wallet application's data. Both entail “***determining whether or not the physiological parameter sensed satisfies a criterion.***” Dua ¶¶[0050], [0366], [0399], [0429]; EX1002 ¶218.

Further confirming this limitation is met, Patent Owner alleges in its infringement contentions in the district court litigation that the use of biometric verification is itself sufficient to show claimed ***sensing*** and ***determining***. EX1016 at 46-49; *see also* EX1002 ¶¶219-20.

At a minimum, it would be obvious to implement Dua's teaching of “authentication using... biometric information” in this manner for the reasons explained above in connection with Jain's disclosure of limitation 1[a]-[c].

After matching PIN code or fingerprint is sensed, the wallet application is opened in order to be issued a credit card. The wallet application then establishes Session Initiation Protocol (“SIP”) communication session between the wireless device and the issuer's wireless credential manager (***enabling at least one first function***). Dua ¶¶[0046], [0104], [0128], [0178]; *see also* EX1002 ¶221-22. “The... SIP architecture... establish[es] direct communication between... WCM and wallet application... for... transferring... credentials.” Dua ¶¶[0128], [0178], Figs. 3 and 4:

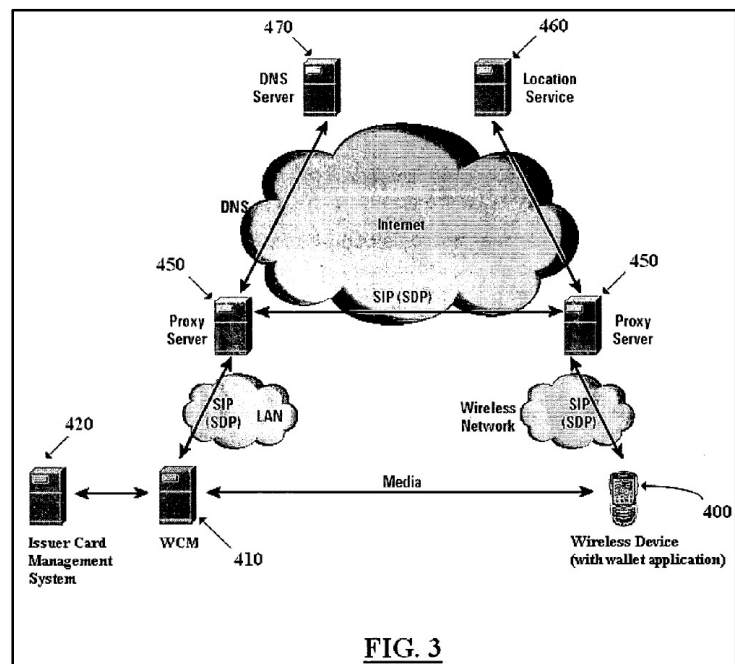


- (v) 1[d]: while said at least one first function is enabled, responsive to having sensed the physiological parameter and responsive to having determined that the physiological parameter sensed satisfies the criterion, requesting an authorization to establish a function to conduct a financial transaction; then
- (vi) 1[e]: responsive to the requesting, receiving the authorization to establish the function to conduct the financial transaction; then
- (vii) 1[f]: responsive to receiving the authorization, establishing the function to conduct the financial transaction; and then

Finally, with the claimed *determining* and *enabling* complete, claim 1 recites the specific steps for *establishing the function to conduct the financial transaction*: *requesting* and *receiving* authorization. Dua discloses these steps.

As discussed with limitations 1[a][i] and 1[a][ii], the *first function* is SIP communications. Dua ¶¶[0046], [0104], [0128], [0178]. *While that function is enabled*, the “issuer’s system will authenticate the... user’s identity... to ensure that

the [user]... is... the person that requested the digital credential.” Dua ¶[0180]. The “authentication process [is]... accomplished by... the issuer system prompting the user for some cardholder... information,” where the “user would see such a request for information within the wallet application.” Dua ¶[0180]. The credential-issuance request asks for a “special code or PIN that was mailed to the user in advance of the issuance.” Dua ¶[0180]; *see also* EX1002 ¶223-225. The wireless device’s wallet application then sends the “special code or PIN” (*requesting an authorization to establish a function to conduct a financial transaction*) to the wireless credential manager to allow “the issuer’s system [to] validat[e] the user's identity in real-time.” Dua ¶[0180], FIG.3 (depicting WCM 410 as a server communicating with the wireless device 400):



“Subsequent to... validating the user’s identity[,]... the WCM 510 will transmit the credential to the wallet application” (*receiving the authorization*). Dua ¶[0180]. Because the exchange results in the issuance of a credit card, the transmission of the PIN code requests *authorization*, the credentials are an *authorization to establish the function to conduct the financial transaction*, and completing this exchange enables the wireless device to execute those transactions (thereby *establishing the function*). EX1002 ¶¶226-28.

This mirrors Patent Owner’s infringement contentions, where Patent Owner asserts that “adding a credit card” is sufficient to show *requesting* and *receiving* an *authorization to establish a function* and then *establishing* that function. EX1016 at 26. *See also* EX1002 ¶229.

(viii) 1[g][i]: *responsive to satisfying a proximity condition relative to an entity and*

After the claimed *establishing the function*, claim 1 requires *using* the same. Before getting to the actual *using*, claim 1 defines two prerequisites that have to be met. The first of those is *satisfying a proximity condition relative to an entity*.

After receiving/retrieving credentials, Dua discloses that the wireless device makes proximity transactions with point-of-sale readers. “Credentials... may [be] use[d] [by] the handheld device to conduct... [a] transaction... via... a short range wireless link with a point-of-sale terminal” (*entity*). Dua Abstract; *see also* EX1002 ¶¶230-231.

Because the short range wireless link between the wireless device and point-of-sale reader includes NFC, the transaction occurs only if (*responsive to*) the wireless device is in “close proximity” to the point-of-sale reader and can thus detect its NFC communications, including the “reader key” (*satisfying a proximity condition*). Dua Abstract, ¶¶[0016], [0318]. NFC and other short range wireless communication protocols are only effective if there is an underlying signal of sufficient strength such that the device and the terminal can communicate using that protocol. EX1002 ¶232, 236. Signal strength attenuates with increasing distance. EX1002 ¶232. Thus, when Dua is able to communicate with the POS terminal using NFC, the wireless device has *satisfied a proximity condition*(*e.g.*, Dua at Abstract, ¶¶[0041], [0314]-[0315], [0382], [0395]) by receiving and decoding a short-range NFC signal from the POS device.

In addition, the claimed *satisfying a proximity condition* also occurs earlier in Dua’s NFC exchange, prior to sending payment information. Dua teaches that its short-range communication is based on NFC. Dua ¶[0016]. As explained above in connection with Jain with reference to the ECMA 340 standard for NFC communication, regardless of what NFC mode is being used and which device in Dua is the Initiator and which device is the Target, both devices detect whether *a proximity condition* has been satisfy, establish a link, and then use that link to exchange data. This includes transmission of Dua’s credentials and payment

transaction. At a minimum, it would have been obvious to implement Dua's NFC communications in this manner. Dua already tells a POSITA to look to the "ISO/IEC 14443" RF proximity standard (Dua ¶[0013]), which would motivate a POSITA to also look to the standard for NFC, in addition to the benefits for implementing a standard discussed above in connection with Jain. EX1002 ¶233.

Further confirming this limitation is met, Patent Owner alleges in its infringement contentions in district court litigation that the use of NFC is itself sufficient to show the claimed *satisfying*. EX1016 at 46; EX1002 ¶234.

In addition, it would be obvious to a POSITA that Dua's wireless device would detect proximity to the POS terminal based on a signal from the POS terminal. Dua's wireless device has to establish a peer-to-peer communication session with the POS terminal over NFC. *E.g.*, Dua ¶[0016], Claims 33, 36, 50. Dua contemplates NFC communication sessions transferring a significant amount of data, such as encryption keys and several credentials, "requir[ing] the user to hold the wireless device in front of the reader for a longer period of time while the processing... takes place." Dua ¶[0359]. As explained by Dua, the smartphone and POS communicate using short range signals. Dua Abstract, ¶¶[0016], [0041], [0314]-[0315], [0382], [0395]. To ensure communications will be successful and not just wasted signals and wasted user time, Dua's wireless device first needs to detect it is near the POS prior to proceeding with a payment transaction with the POS device. In addition,

transmitting sensitive financial information when there is no bona fide POS in proximity poses a security risk. As such, it would have been obvious for a POSITA to configure the smartphone to first detect that it is proximate to Dua's POS device prior to attempting short-range signal communication to prevent the error conditions or fraud. EX1002 ¶235-38. Indeed, such implementations were well-known to a POSITA. For example, EX1020 discloses and leverages NFC to limit the range at which communication may take place. EX1020 ¶¶[0041], [0063]. Indeed, in the context of Wi-Fi, EX1020 even more explicitly discloses using the ability to receive such signals as an indication of proximity. Dua ¶[0073].

(ix) 1[g][ii]: *responsive to sensing the physiological parameter and determining that the physiological parameter sensed satisfies the criterion,*

The second prerequisite in claim 1 to *using* the claimed *function to conduct the financial transaction* is *sensing the physiological parameter and determining that the physiological parameter sensed satisfies the criterion*.

According to Patent Owner, limitation 1[g][ii] does not impose any new requirement relative to limitations 1[a] and 1[b]: the same sensing of *the* at least parameter and determining it meets *the* criterion prior to establishing the function to conduct the financial transaction is also a prerequisite to then *using* that function. Compare EX1016 at 46-49 with EX1016 at 56-59 (pointing to the same “fingerprint unlock” and similar security functionality for both limitations).

Even if the claims require an additional transaction-specific *sensing* and *determining*, Dua discloses that individual transactions, same as receiving or retrieving credentials, require opening the wallet application, which in turn is subject to the “default security setting in the wallet application is that PIN-entry is required before” (*responsive to*) “any credentials [are] transmitted to an external device,” such as for a transaction with a point-of-sale reader. Dua Abstract, ¶[0366]; *see also* EX1002 ¶239-41. Dua’s “default security setting” discloses or renders obvious the claimed *sensing* and *determining* via PIN entry or fingerprint scanning for the reasons discussed above in connection with limitation 1[a][i]. *See also* EX1002 ¶¶241-42.

- (x) 1[g][iii]: *using the function that has been established to conduct the financial transaction and conducting the financial transaction by paying for a product;*

Dua further discloses, after satisfaction of all the requirements discussed above, that the wireless device execute the financial transaction (*conducting the financial transaction*) to pay for a product, such as groceries or train ticket (*paying for a product*). Dua Abstract, ¶¶[0352]-[0353]; *see also* EX1002 ¶¶243-245.

- (xi) 1[h]: *... sensing that the proximity condition is satisfied relative to an access point maintained by a vendor at a point of purchase counter, by detecting a short-range signal that is transmitted by the access point, ... and then ... paying for the product by selectively sending information to at least one device;*

Limitation 1[h] for the most part just repeats the *detecting* of limitation 1[d] and only further specifies that this is done “*relative to an access point maintained by a vendor at a point of purchase counter*” and by detecting “*a short-range signal that is transmitted by the access point.*” Even those requirements, however, are addressed above in connection with limitation 1[d][ii], since Dua’s “RFID reader[]” (*access point*)⁵ is “installed at POS terminals in [the grocery chain’s] stores” (*maintained by a vendor at a point of purchase counter*). Dua Abstract, ¶¶[0016], [0041], [0314]-[0315]; *see also* EX1002 ¶¶246-47.

(xii) 1[i]: ... *selectively and wirelessly transmitting information to the at least one device using unlicensed frequencies; and*

The only additional requirement of limitation 1[i] is that the “information” of limitation 1[h] be sent *using unlicensed frequencies*. Dua meets this requirement by transmitting credentials using NFC and Bluetooth (*using unlicensed frequencies*). Dua Abstract, ¶¶[0016], [0318]; EX1002 ¶¶248-50. As addressed above in connection with limitation 1[i] for Jain, NFC and Bluetooth use unlicensed frequencies. EX1002 ¶250-252.

⁵ According to Patent Owner’s infringement contentions, the claimed *access point* and claimed *at least one device* can be one and the same device. EX1016 at 56, 70 (pointing to “the point-of-sale device” or “terminal” for both limitations).

- (xiii) 1[j]: *wherein said paying for a product further comprises deducting/withdrawing an amount of money from an account.*

Dua discloses paying for a product, such as groceries and train tickets (*paying for a product*), as discussed with limitation 1[g][iii]. Dua Abstract, ¶[0352]. The money to pay for the product could come out of any number of accounts, such as an account linked to a debit card (*deducting/withdrawing an amount of money from an account*). Dua ¶¶[0290], [0336], Claim 44; EX1002 ¶¶253-54.

(b) Claim 2

(i) 2[pre][i]

Claim 1, *supra*.

(ii) 2[pre][ii]

Limitation 2[pre][ii] requires that, when the *first function* of limitation 1[c] is enabled, a *second function* is *disabl[ed]*. Dua discloses this limitation.

Patent Owner contends that the “*enabling a first function*” and “*disabling a second function*” limitations are met by “unlocking the Samsung smartphone or application” and “locking the Samsung smartphone or application.” EX1016 at 73-76. The same disclosure is also found in Dua. The “default security setting in the wallet application is that PIN-entry is required before the wallet application can be ‘opened.’” Dua ¶¶[0366], [0429]. And the “wireless device... could use a fingerprint in lieu of a PIN code... .” Dua ¶[0366]. Once the PIN or fingerprint is received and

the wallet is opened, the PIN-entry or fingerprint-scanning function for opening the wallet is disabled. EX1002 ¶¶256-57.

(iii) 2[a]-[c]

Limitation 2[a] requires performing limitation 1[a] and 1[b] *repeatedly* and based on the result of the claimed *sensing* and *determining* whether to maintain the *first function* and keep the *second function disabled*. Dua discloses this limitation.

As discussed with limitation 2[pre][ii], Dua discloses “*enabling a first function*” and “*disabling a second function*” by PIN/fingerprint entry to enable the unlocked wallet application and disable the locked function on the wallet application, similar to Patent Owner’s infringement read. EX1016 at 73-76; *see also* EX1002 ¶¶258-260. Further, “*repeatedly sensing*” a PIN/fingerprint entry and “*repeatedly deciding... whether... to maintain enabled*” the unlocked wallet application “*while maintaining disabled*” the lock function on the wallet application is rendered obvious to a POSITA by Dua. Dua discloses security risks regarding the wireless device being lost, stolen, or otherwise ending up in possession of someone other than the rightful owner. Dua ¶[0451]. If the device were lost or taken while sensitive functionality, including transaction related functionality, was enabled, then the device could be misused. For example, enabled functionality might remain enabled so long as someone (anyone) continued to use the device before it could enter sleep mode. If, however, the device repeatedly prompted the user to re-

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

EX1002 ¶261. This locking and unlocking of the wallet application, and thereby enabling the first function and disabling the second function, or vice versa, meets the requirements of both limitations 2[b] and [c].

(c) Claim 3

(i) 3[pre]

Claim 1, *supra*.

(ii) 3[a]

Dua discloses that the wireless device transmits messages to close out the communication channel between it and the POS reader. A wireless device sets up a “peer-to-peer communication session... through Near Field Communication.” Dua Abstract, ¶[0016], Claim 38. This peer-to-peer communication is based on the “Transmission Control Protocol (TCP).” Dua ¶¶[0101], [0205], [0279], [0311], [0488]; EX1002 ¶263; *see also* EX1040 at 1. After a transaction is complete, the wireless device sends a “BYE” message and the reader responds with an “OK” message (*information*) to close the communication channel. Dua ¶[0182], FIG. 4; EX1002 ¶263; *see also* EX1040 at 5, 12.

The point-of-sale reader can also transmit to a wireless device an indication of a “successful transmission of credentials to [the] reader” (*information*) after a transaction is complete. Dua ¶¶[0015], [0041], [0293], [0364]-[0365]; *see also* EX1002 ¶264.

(d) Claim 4

(i) 4[pre]

Claim 3, *supra*.

(ii) 4[a]

Limitation 4[a] requires that the wireless transmitting and receiving of limitations 1[i] and 3[a] be done using *unlicensed frequencies over a short-range link in a Time Division Duplex operation*.

Dua teaches sending of limitation 1[i] and 3[a] is done via NFC or Bluetooth. Dua Abstract, ¶¶[0016], [0318]. As addressed above in connection with limitation 4[a] for Jain, NFC and Bluetooth use *unlicensed frequencies over a short-range link in a Time Division Duplex operation*. EX1002 ¶266-69.

(iii) 4[b]

Limitation 4[a] mostly repeats the requirements of limitations 1[h]-[i] and 3[a] but further adds that the information of limitations 1[h]-[i] and 3[a] is transmitted to and received from *the access point maintained by the vendor* and adds the further requirement of transmitting information to and receiving information from *at least one other device that is predetermined*. Dua discloses both limitations.

Dua discloses the wireless device sending credentials to a point-of-sale reader (*access point*), which is then forwarded to the issuer system (*at least one other device that is predetermined*). Dua Abstract, ¶¶[0009], [0015], [0041], [0293], [0365], Fig. 8; EX1002 ¶¶270-71.

Dua discloses the wireless device receiving an “OK” message and a “successful transmission” indication from the reader (*access point*). See limitation 3[a]; see also EX1002 ¶272.

Dua also discloses the wireless device receiving digital receipts of the transaction from a merchant’s wireless credential manager (*selectively receiving information... from at least one other device that is predetermined*). Specifically, the wallet application can “receiv[e] digital receipts from merchants,” which are a “record of payment transaction... during a... transaction using the wallet application.” Dua ¶[0430]; EX1002 ¶¶272-73.

(e) Claim 5

Claim 5 is substantively identical to claim 1 and only further adds that the steps of claim 1 be implemented by *a wireless device that comprises a smartphone and a sensor*. See EX1002 ¶274.

Dua discloses a wireless device, which includes a *smartphone*. Dua Abstract, FIGS. 3, 5, 6(a)-8. The wireless device includes a “handheld device, such as a mobile telephone,” “capable of wirelessly connecting to the internet” and with applications like a “wallet application.” Dua Abstract, ¶¶[0041], [0049], [0050], [0051], [0287]-[0288], FIGS. 3, 5, 6(a)-8. The wallet application can “conduct[] financial... transactions” (*perform[] at least one financial transaction*). Dua Abstract, ¶¶[0041], [0312]-[0313], [0333]. See also EX1002 ¶275.

Moreover, Dua’s wireless device includes embedded biometric technologies (*sensor*). Dua discloses that “[w]hile this document references the use of PIN codes throughout, wireless device's with embedded biometric technologies could use a fingerprint in lieu of a PIN code to authenticate a user to the wallet application.” Dua ¶[0366]. Based on this, a POSITA would understand that Dua’s wireless device has a fingerprint scanner or similar embedded biometric technologies (*sensor*) to implement this functionality. EX1002 ¶276. At a minimum, it would be obvious to implement Dua’s disclosure of using fingerprints in this manner, as addressed above in connection with limitations 1[a] and [b].

(f) **Claim 7**

(i) **7[pre]**

Claim 5, *supra*.

(ii) **7[a]**

Dua discloses the wireless device *establishing a short range wireless link with* a point-of-sale terminal (*entity*) using NFC to transmit its credentials to the terminal. Dua Abstract, ¶¶[0016], [0318]; EX1002 ¶279. *Establishing a short-range wireless link* using NFC is addressed in more detail in the ECMA 340 standard implemented by Dua (*see* limitation 1[g][i]), which describes an “Initiator” device and a “Target” device exchanging communications to select a particular “Target” and attributes/parameters for further communication (*establishing ... a short-range wireless link*). Indeed, Patent Owner’s infringement contentions allege

the use of NFC as sufficient to show *establishing ... a short-range wireless link*.

EX1016 at 212-213.

(iii) 7[b]-[d]

Dua discloses a wireless device *wirelessly transmitting* credential *information* to a point-of-sale terminal (*entity*). Dua Abstract, ¶[0352], [0353]. In response, the point-of-sale terminal transmits to the wireless device an indication of a “successful transmission of credentials to [the] reader” after a transaction is complete (*wirelessly receiving information from the entity*). Dua ¶¶[0364]-[0365]; *see also* Dua ¶¶[0015], [0041], [0293]. The transmission between the wireless device and point-of-sale terminal is done with short range wireless communication, including NFC and Bluetooth. Dua Abstract, ¶¶[0016], [0318]; *see also* EX1002 ¶280. As addressed above in connection with limitations 7[b]-[d] for Jain, NFC and Bluetooth use *unlicensed frequencies in a time division duplex operation*. *See* EX1002 ¶281-85.

(iv) 7[e]

This limitation further requires that the *establishing the short range link* occur *responsive to the wireless device satisfying the proximity condition relative to the entity* (addressed above in connection with limitation 1[g][i]) and *responsive to the wireless device sensing the parameter and determining that the value*

associated therewith satisfies the threshold criterion (addressed above in connection with limitations 1[a]-[c] and 1[g][i]). Dua discloses both requirements.

Responsive to ... satisfying the proximity condition: As addressed in more detail above in connection with limitations 4[a] and 17[a], the NFC standard implemented by Dua teaches or at least renders obvious conducting a command/response exchange that concludes with the “Initiator” device selecting one or more “Target” devices and attributes/parameters for communication (***establishing ... a short-range wireless link***) after the “Initiator” and “Target” first detect RF signals from each other (***responsive to ... satisfying the proximity condition***). See EX1002 ¶286

Responsive to ... sensing ... and determining: As addressed above in connection with limitation 1[a]-[f] and [g][ii], Dua’s ***wireless device*** is only able to conduct financial transactions after the wallet application is first opened, both to be issued a credit card in the first instance and to later use that credit card, which in turn requires biometric authentication (***responsive ... sensing ... and determining***). See EX1002 ¶287.

At a minimum, and as discussed in more detail in connection with limitation 7[e] for Jain, it would be obvious to a POSITA a wireless device (such as Dua’s) would establish a NFC connection with the point-of-sale terminal (***establishing ... a short-range wireless link***) after ***satisfying the proximity condition*** and ***sensing ...***

and determining that the physiological parameter sensed satisfies the criterion.

See EX1002 ¶288.

(g) Claim 8

(i) 8[pre]

Claim 5, *supra*.

(ii) 8[a]

Dua discloses how the wireless device establishes connections with the WCM through SIP. “The... SIP architecture... establish[es] direct communication between... WCM and wallet application... for... transferring... credentials.” Dua ¶¶[0128], [0178]; *see also* Dua FIGS. 3-4. A “real-time connection is initiated between the wallet application and the storage service” by “utiliz[ing] SIP.”. Dua ¶¶[0494]-[0495]. A connection established through SIP can entail several servers and various electronic communication protocols such as cellular wireless technology (*e.g.*, “2.5G” and “3G”) and “Wi-Fi.” *E.g.*, Dua ¶[0104], FIG 3; *see also* EX1002 ¶291.

(iii) 8[b]-[c]

As discussed with limitation 8[a], Dua discloses the wireless device communicating with the WCM using cellular wireless technology (*e.g.*, “2.5G” and “3G”) and “Wi-Fi” (*wirelessly transmitting [and receiving] information to the second device over said wireless link*). *See* Dua ¶[0104]. Cellular wireless

technology/protocols 2.5G and 3G *us[e] ... licensed frequencies*. EX1002 ¶292.

Wi-Fi uses *unlicensed frequencies*. EX1002 ¶292.

(iv) 8[d]

As discussed with limitations 8[a] and 8[c], Dua discloses the wireless device using a cellular wireless technology or Wi-Fi to communicate with the WCM. 2.5G and 3G cellular wireless technology and Wi-Fi *us[e] ... orthogonal frequency division multiplexing*. EX1002 ¶¶293-94.

(v) 8[e]

As discussed with limitations 1[a]-[c] and 8[a], Dua discloses *establishing the link with the second device responsive to ... the parameter ... satisf[ying] the threshold criterion*. Scanning a valid fingerprint causes the wireless device to open the wallet application and establish a connection with WCM. EX1002 ¶295.

(h) Claim 9

Claim 9 is substantively identical to claim 4 and only further adds that the steps of claim 4 be implemented by the *wireless device* of claim 5. EX1002 ¶296. The use of the word *selectively* also does not add a meaningful limitation, since at least the “OK” message (*information*) in limitations 3[a], which in turn is referenced in limitation 4[b], is received only if the wireless device is sufficiently close to the POS terminal to commence a financial transaction (*selectively*). EX1002 ¶297. For the reasons set forth above in connection with claims 4 and 5, Dua also discloses claim 9.

(i) Claim 6, 10-11

Claims 6, 10-11 are substantively identical to claims 2-4 and only further add that the steps of claims 2-4. EX1002 ¶¶277, 298.

C. Secondary Considerations

Any secondary considerations further weigh in favor of obviousness, and certainly do not overcome the strong showing of obviousness. EX1002 ¶299. First, Patent Owner has not practiced the claimed invention—at any point in time—evidencing a lack of commercial success for any product practicing the '793 patent. EX1002 ¶300. Additionally, there was no long felt, unresolved need met by the '793 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 ¶301. Further, the vast number of contactless payment systems and trials of those systems before the '793 patent's priority date indicates that many within the market observed the desirability of such systems and were concurrently working towards implementing them. Section IV.A-B.

IX. 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.

X. CONCLUSION

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

Date: May 23, 2025

Respectfully submitted,

By: /s/ James Glass
James M. Glass

Counsel for Petitioner

CERTIFICATION UNDER 37 C.F.R. § 42.24

Under the provisions of 37 C.F.R. § 42.24, the undersigned hereby certifies that the word count for the foregoing Petition for *inter partes* review (excluding the table of contents, table of authorities, mandatory notices, certificate of service or word count, and appendix of exhibits or claim listing) totals 13,961 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 '793 patent as shown in USPTO PAIR via FedEx:

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

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

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

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

apederson@carlsoncaspers.com

Date: May 23, 2025

/s/ *James Glass*

James Glass (Reg. No. 46729)