

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD. AND
SAMSUNG ELECTRONICS AMERICA, INC.

Petitioners

v.

SURECELL TRANSACTIONS LLC,
Patent Owner

Case No. IPR2026-00509
U.S. Patent No. 11,687,741

**PETITION FOR INTER PARTES REVIEW OF
U.S. PATENT NO. 11,687,741**

CONTENTS

I.	INTRODUCTION	1
II.	REQUIREMENTS UNDER 37 C.F.R. §42.104.....	1
	A. GROUNDS FOR STANDING	1
	B. IDENTIFICATION OF CHALLENGE AND STATEMENT OF PRECISE RELIEF REQUESTED	1
III.	'741 PATENT.....	2
	A. SPECIFICATION	2
	B. FILE HISTORY	2
IV.	LEVEL OF ORDINARY SKILL IN THE ART	4
V.	CLAIM CONSTRUCTION	4
	A. “RESPONSIVE”	4
	B. “SWITCH”	4
VI.	SUMMARY OF PRIOR ART.....	5
	A. <i>DUA</i> (EX1023).....	5
	B. <i>WATERS</i> (EX1024).....	7
	C. <i>WOIKE</i> (EX1025) (SECONDARY REFERENCE).....	8
VII.	INVALIDITY	9
	A. GROUNDS 1-2: <i>DUA</i>	9
	i. Independent Claim 1	9
	ii. Dependent Claims 2-13, 15-18	16
	iii. Independent Claim 19	30
	iv. Dependent Claims 20-28, 30.....	32
	B. GROUND 3: <i>DUA</i> IN VIEW OF <i>WOIKE</i> RENDERS OBVIOUS CLAIMS 9, 14, 29, AND 30	37
	i. Motivation to Combine	37
	ii. Claim Analysis.....	38
	C. GROUND 4: <i>WATERS</i> IN VIEW OF <i>DUA</i> RENDERS OBVIOUS CLAIMS 1-30.....	41
	i. Motivation to Combine	41

ii.	Independent Claim 1	43
iii.	Dependent Claims 2-18.....	50
iv.	Independent Claim 19	60
v.	Dependent Claims 20-30.....	62
VIII.	CONCLUSION	67

PETITIONERS' EXHIBIT LIST¹

Exhibit	Description of Documents
EX1001	[Reserved]
EX1002	U.S. Patent No. 11,347,949
EX1003	U.S. Patent No. 11,599,734
EX1004	U.S. Patent No. 11,687,741
EX1005	U.S. Patent No. 11,989,612
EX1006	U.S. Patent No. 12,039,396
EX1007	[Reserved]
EX1008	Prosecution History of U.S. Patent No. 11,347,949
EX1009	Prosecution History of U.S. Patent No. 11,599,734
EX1010	Prosecution History of U.S. Patent No. 11,687,741
EX1011	Prosecution History of U.S. Patent No. 11,989,612
EX1012	Prosecution History of U.S. Patent No. 12,039,396
EX1013	[Reserved]
EX1014	Declaration of Dr. Sayfe Kiaei in support of petition for <i>inter partes</i> review of U.S. Patent Nos. 11,347,949; 11,599,734; 11,687,741; 11,989,612; 12,039,396
EX1015	Sony, <i>Near Field Communication Technology jointly developed by Sony and Philips approved as ISO/IEC International Standard</i> , https://www.sony.com/en/SonyInfo/News/Press/200312/03-059E/ (Dec. 8, 2003)
EX1016	RFID Journal, <i>Nokia Unveils RFID Phone Reader</i> , https://www.rfidjournal.com/news/nokia-unveils-rfid-phone-reader/78579/ (Mar. 17, 2004)
EX1017	EuroTechnology, <i>ApplePay vs Osaifu-Keitai - CNBC Interview</i> , https://www.eurotechnology.com/2014/09/18/applepay-vs-osaifu-keitai-cnbc/ (Sept. 18, 2014)
EX1018	IEEE Spectrum, <i>Here Comes The Wallet Phone</i> , https://spectrum.ieee.org/here-comes-the-wallet-phone (Nov. 1, 2005)
EX1019	Declaration of Sylvia D. Hall-Ellis, Ph.D. in support of authenticity and public availability of documents for inter partes review of U.S.

¹ Unless otherwise indicated, U.S. patents are cited by column:line, U.S. patent application publications, complaints, and declarations by paragraph number, patent figures by figure number, and all other materials by Bates number. All emphasis has been added unless noted.

	Patent Nos. 11,347,949; 11,599,734; 11,687,741; 11,989,612; 12,039,396
EX1020	SureCell Transactions LLC v. Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc., No. 2:26-cv-00106, Dkt. 30 (E.D. Tex. Feb. 26, 2026) (“Second Amended Complaint”)
EX1021	SureCell's Infringement Contentions, <i>SureCell Transactions LLC v. Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.</i> , No. 2:26-cv-00106 (E.D. Tex. Feb. 26, 2026)
EX1022	Claim Construction Order, <i>Mynette Techs., Inc. and Steven M. Colby v. The United States and Unisys Corp.</i> , No. 16-1647 (COFC Aug. 17, 2018)
EX1023	U.S. Patent Publication No. 2006/0165060 (“Dua”), published July 27, 2006 (filed Jan. 21, 2005)
EX1024	U.S. Patent Publication No. 2009/0215385 (“Waters”), published August 27, 2009 (PCT filed Feb. 15, 2005)
EX1025	International Patent Publication No. WO 2001/054079 (“Woike”), published July 26, 2001
EX1026	Pont, <i>Embedded C</i> (2002)
EX1027	[Reserved]
EX1028	[Reserved]
EX1029	Finkenzeller, <i>RFID Handbook</i> , 2d ed. (2003)
EX1030	[Reserved]
EX1031	ISO/IEC 14443-1:2000 (“Identification cards - Contactless integrated circuit(s) cards - Proximity cards Part 1: Physical characteristics”)
EX1032	ISO/IEC 14443-2:2001 (“Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 2: Radio frequency power and signal interface”)
EX1033	Andrew Miceli, <i>Wireless Technician’s Handbook</i> , 2d ed. (2003)
EX1034	CV of Sayfe Kiaei
EX1035	Petitioners’ Stipulation

MANDATORY NOTICES UNDER 37 C.F.R. §42.8(A)(1)

Real Party in Interest: The real parties in interest are Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc., Petitioners.

Related Matters: U.S. Patent No. 11,687,741 (“’741 patent”) is currently asserted by Patent Owner (“PO”) against Petitioners in the case styled: *SureCell Transactions LLC v. Samsung Electronics Co., Ltd.*, No. 2:26-cv-00106 (E.D. Tex), which was originally filed on February 12, 2026.

Lead Counsel and Back-Up Counsel: Petitioners designate lead and back-up counsel as noted below. Powers of Attorney are filed concurrently herewith under 37 C.F.R. § 42.10(b).

LEAD COUNSEL	BACK-UP COUNSEL
Eliot D. Williams, Reg. No. 50,822 Baker Botts L.L.P. 700 K Street, N.W. Washington, D.C. 20001-5692 Phone: 202.639.1334 Fax: 202.639.7890 eliot.williams@bakerbotts.com	Neil Sirota, Reg. No. 38,306 Baker Botts L.L.P. 30 Rockefeller Plaza, Ste 4340 New York, NY 10112-4498 Phone: 212.408.2548 Fax: 212.259.2548 neil.sirota@bakerbotts.com Megan LaDriere White, Reg. No. 75,995 Baker Botts L.L.P. 2001 Ross Avenue Suite 900 Dallas, Texas 75201-2980 Phone: 214.953.6948 megan.white@bakerbotts.com Eric Faragi, Reg. No. 51,259 Baker Botts L.L.P.

LEAD COUNSEL	BACK-UP COUNSEL
	30 Rockefeller Plaza, Ste 4340 New York, NY 10112-4498 Phone: 212.408.2591 eric.faragi@bakerbotts.com Benjamin Rosen, Reg. No. 84,598 Baker Botts L.L.P. 30 Rockefeller Plaza, Ste 4340 New York, NY 10112-4498 Phone: 212.408.2691 benjamin.rosen@bakerbotts.com Coleman Strine, Reg. No. 79,981 Baker Botts L.L.P. 30 Rockefeller Plaza, Ste 4340 New York, NY 10112-4498 Phone: 212.408.2595 coleman.strine@bakerbotts.com

Service Information: Correspondence to lead and back-up counsel can be provided at the postal and electronic addresses above. Petitioners also consent to service by electronic mail at DLSamsungvSureCell_IPRs@bakerbotts.com.

CLAIMS LISTING

Claim 1:

1[pre]	A method of performing a financial transaction using a cellular telephone, the method comprising:
1[a]	placing the cellular telephone within reading range of a wireless communication device,
1[b]	the cellular telephone being configured to communicate wirelessly using an inductive coupling and an RF antenna,
1[c]	wherein communication by the cellular telephone is responsive to a circuit including an electronic switch configured to change a state of the circuit,
1[d]	the circuit being configured to communicate responsive to the state of the circuit;
1[e]	activating the electronic switch within the cellular telephone to change the state of the circuit, activation of the electronic switch being responsive to a biometric sensor included in the cellular telephone; and
1[f]	communicating financial account information from the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate the financial transaction, the communication of the financial account information using the inductive coupling or the RF antenna.

Claim 2:

2	The method of claim 1, wherein the circuit is configured to facilitate the financial transaction responsive to the biometric sensor.
----------	--

Claim 3:

3	The method of claim 1, wherein the circuit is configured to approve the financial transaction responsive to the biometric sensor.
----------	---

Claim 4:

4	The method of claim 1, wherein the circuit is configured to communicate the financial account information responsive to the biometric sensor.
----------	---

Claim 5:

5[pre]	The method of claim 1,
5[a]	wherein the circuit is changed from a first ON state to a second ON state, responsive to the electronic switch,
5[b]	and wherein the circuit includes a memory configured to store the first and second ON states.

Claim 6:

6[pre]	The method of claim 1,
6[a]	wherein the circuit is changed from a first ON state to a second ON state, responsive to the electronic switch,
6[b]	and wherein different amounts of personal information are communicated via the inductive coupling or RF antenna in the first ON state relative to the second ON state.

Claim 7:

7	The method of claim 1, wherein the circuit is configured to store transaction logs.
----------	---

Claim 8:

8	The method of claim 1, wherein the circuit is configured for a user to select between a plurality of financial accounts for the financial transaction.
----------	--

Claim 9:

9	The method of claim 1, wherein the cellular telephone is configured for a user to enter an amount of the financial transaction, and further comprising entering the amount to facilitate the financial transaction.
----------	---

Claim 10:

10	The method of claim 1, wherein the circuit is configured to communicate a financial account number via the inductive coupling or RF antenna to facilitate the financial transaction.
-----------	--

Claim 11:

11	The method of claim 1, wherein the cellular telephone includes a user interface configured to enter a financial account number and includes memory configured to store the financial account number for use in the financial transaction.
-----------	---

Claim 12:

12[pre]	The method of claim 1,
12[a]	wherein the cellular telephone is configured for a user to enter a personal identification number (PIN), communication of the financial account information via the inductive coupling or RF antenna being responsive to the personal identification number;
12[b]	and further comprising entering the personal identification number to facilitate the financial transaction.

Claim 13:

13	The method of claim 1, wherein the cellular telephone includes a memory configured to store a key required to change the state of the circuit to facilitate the financial transaction.
-----------	--

Claim 14:

14[pre]	The method of claim 1,
14[a]	wherein the cellular telephone is configured for mechanical insertion of an electronic key,
14[b]	the electronic key including a personal identification number,
14[c]	a signal communicated via the inductive coupling or RF antenna to facilitate the financial transaction being responsive to entry of the personal identification number by a user.

Claim 15:

15	The method of claim 1, wherein the cellular telephone is configured to store a financial account number and the communication via the inductive coupling or RF antenna including the financial account number.
-----------	--

Claim 16:

16	The method of claim 1, wherein activating the electronic switch is responsive to data stored in memory of the cellular telephone and the data stored in the memory includes biometric data.
-----------	---

Claim 17:

17	The method of claim 1, wherein the financial account information includes an account number corresponding to a financial account of a user of the cellular telephone.
-----------	---

Claim 18:

18[pre]	The method of claim 1,
18[a]	wherein the financial account information is stored in a memory on the cellular telephone,
18[b]	the financial account information corresponding to one of a plurality of financial accounts of a user of the cellular telephone, the method further comprising:
18[c]	presenting a user interface to the user, the user interface being configured to allow the user to select a specific member of the plurality of financial accounts of the user for the financial transaction;
18[d]	and wherein the step of communicating financial account information includes communicating financial account information corresponding to the selected specific member of the plurality of financial accounts.

Claim 19:

19[pre]	A method of performing a financial transaction using a cellular telephone,
19[a]	the method comprising: placing the cellular telephone within reading range of a wireless communication device,
19[b]	the cellular telephone being configured to communicate wirelessly using an RF antenna,
19[c]	wherein the RF antenna is responsive to a circuit including an electronic switch configured to change a state of the circuit,
19[d]	the circuit being configured to communicate via the RF antenna responsive to the state of the circuit;

19[e]	activating the electronic switch within the cellular telephone to change the state of the circuit, activation of the electronic switch being responsive to entry of a personal identification number;
19[f]	and communicating financial account information from the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate the financial transaction, the communication of the financial account information using the RF antenna.

Claim 20:

20	The method of claim 19, wherein the communication of the financial account information is responsive to a biometric sensor and a mechanical switch included in the cellular telephone.
-----------	--

Claim 21:

21	The method of claim 19, further comprising approving the financial transaction using a biometric sensor.
-----------	--

Claim 22:

22	The method of claim 19, wherein the cellular telephone includes a user interface configured for a user to enter a financial account number for use in the financial transaction.
-----------	--

Claim 23:

23[pre]	The method of claim 22,
23[a]	wherein the cellular telephone includes memory configured to store the financial account number, wherein the circuit is configured for the user to select between a plurality of financial accounts for the financial transaction;
23[b]	and further comprising selecting a specific member of the plurality of financial accounts for the financial transaction.

Claim 24:

24	The method of claim 19, wherein the circuit is configured for a user to select between a plurality of financial accounts for the financial transaction.
-----------	---

Claim 25:

25[pre]	The method of claim 19,
25[a]	wherein the circuit is changed from a first ON state to a second ON state, responsive to the electronic switch,
25[b]	and wherein different amounts of personal information are communicated via the RF antenna in the first ON state relative to the second ON state.

Claim 26:

26	The method of claim 19, wherein the circuit is configured to store transaction logs.
-----------	--

Claim 27:

27	The method of claim 19, wherein the circuit is configured to communicate a financial account number via the RF antenna to facilitate the financial transaction.
-----------	---

Claim 28:

28	The method of claim 19, wherein the cellular telephone is configured for storing a password in memory of the cellular phone, the password being entered by a user of the cellular phone to engage in the transaction.
-----------	---

Claim 29:

29[pre]	The method of claim 19,
29[a]	wherein the cellular telephone is configured for insertion of an electronic key,
29[b]	the electronic key being configured to store the personal identification number, the communication via the RF antenna being responsive to the personal identification number.

Claim 30:

30	The method of claim 19, wherein the cellular telephone is configured for a user to enter an amount of the financial transaction.
-----------	--

I. INTRODUCTION

The Office materially erred in granting U.S. Patent No. 11,687,741 (“the ’741 Patent”). As Petitioners will address in detail in their brief regarding the discretionary institution factors, the Examiner overlooked the obviousness of the claimed limitations, and the search was insufficient to locate highly relevant references. Grounds 1–4 disclose or render obvious every claimed element of the ’741 Patent.

II. REQUIREMENTS UNDER 37 C.F.R. §42.104

A. GROUNDS FOR STANDING

Petitioners certify under 37 C.F.R. § 42.104(a) that the ’741 Patent is eligible for IPR and that Petitioners are not barred or estopped from requesting IPR on Grounds 1-4.

B. IDENTIFICATION OF CHALLENGE AND STATEMENT OF PRECISE RELIEF REQUESTED

This IPR, supported by the declaration of Dr. Sayfe Kiaei (EX1014), asserts the following grounds of unpatentability:

Petitioners’ or PO’s Claim Interpretations	
Ground 1	<i>Dua</i> anticipates claims 1-13, 15-28, 30
Ground 2	<i>Dua</i> renders obvious claims 1-13, 15-28, 30
Ground 3	<i>Dua</i> with <i>Woike</i> renders obvious claims 9, 14, 29, 30
Ground 4	<i>Waters</i> with <i>Dua</i> renders obvious claims 1-30

III. '741 PATENT

A. SPECIFICATION

The '741 Patent relates to methods for performing a financial transaction using a switchable circuit to control communication of financial information using inductive coupling or an RF antenna. EX1004, Cl. 1. While the specification describes a switchable RFID tag, “[v]arious embodiments of the invention include a portable communication device such as a cellular telephone.” *Id.*, 9:63-64. The communication device includes a user interface used “to turn on or off operation of the RFID tag, to enter security data into the RFID tag, to enter financial information (e.g., a credit or debit card number[]) into the RFID tag, to enter an identifying number (e.g., telephone number) into the RFID Tag, or to enter account number into the RFID tag.” *Id.*, 10:11-17. The communication device is further “configured to use voice recognition to approve an RFID based financial transaction. For example, in some embodiments voice recognition authentication may be required before an RFID tag is activated.” *Id.*, 11:25-29.

B. FILE HISTORY

The '741 Patent was filed as App. No. 17/952,176 (the “'176 Application”) on September 23, 2022, and on its face, purports to claim priority to a provisional application filed on May 6, 2005. EX1004, Cover. In a Preliminary Amendment dated December 23, 2022, Applicant canceled certain claims, added certain claims, and made short amendments throughout. *Id.*, 265-69. Independent claim 1 recited:

1. (Currently Amended) A method of performing a financial transaction using a cellular telephone, the method comprising:
placing the cellular telephone within reading range of a wireless communication device, the cellular telephone being configured to communicate wirelessly using an inductive coupling and an RF antenna, wherein ~~the~~ communication (verb) by the cellular telephone is responsive to a circuit including an electronic switch configured to change a state of the circuit, the circuit being configured to communicate responsive to the state of the circuit;
activating the electronic switch within the cellular telephone to change the state of the circuit, activation of the electronic switch being responsive to a biometric sensor included in the cellular telephone; and
communicating financial account information from the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate the financial transaction, the communication of the financial account information using the inductive coupling or the RF antenna.

Id., 265.

In a first Non-Final Office Action dated December 28, 2022, the Examiner provisionally rejected all claims for nonstatutory double patenting over claims 1-24 of copending U.S. Application No. 17/697,923 (the “’923 Application”) which was granted as U.S. Pat. No. 11,599,734 (the “’734 Patent”). *Id.*, 98-103. In response, Applicant filed a terminal disclaimer to the ’923 Application. *Id.*, 92-93. On April 13, 2023, the Office issued a Notice of Allowance for all claims. *Id.*, 30.

IV. LEVEL OF ORDINARY SKILL IN THE ART

A Person of Ordinary Skill in the Art (“POSITA”) at the time of the ’741 Patent would have had either (i) a Master of Science in Electrical Engineering or an equivalent field, or (ii) a Bachelor of Science in Electrical Engineering or an equivalent field and two years of experience in the field of RFID communications. EX1014, ¶¶59-60.

V. CLAIM CONSTRUCTION

Petitioners propose that all terms be given their ordinary and customary meaning and identify the following terms for construction, in view of potential differing interpretations.

A. “RESPONSIVE”

A POSITA would have understood “responsive” to have its plain and ordinary meaning. *See* EX1022, 15 (the parties, including the inventor, Steven Colby, agreed that “the term ‘responsive’ is properly construed according to its ‘plain and ordinary meaning’”).

B. “SWITCH”

A POSITA would have understood “switch” to mean a control device that makes or breaks an electrical connection in a circuit. *See* EX1022, 15 (the parties, including the inventor, Steven Colby, agreed that “the term ‘switch’ is properly construed to mean ‘[a] control device that makes or breaks an electrical connection in a circuit’”).

VI. SUMMARY OF PRIOR ART

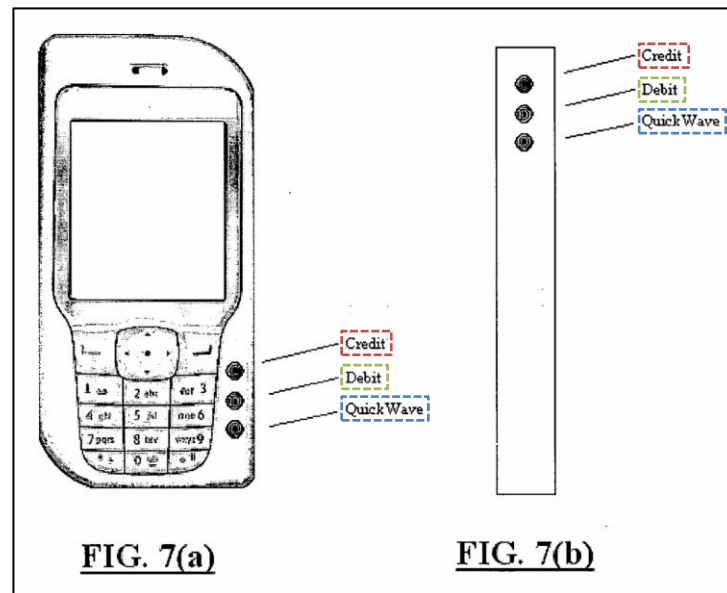
Petitioners assume, without conceding, that claims 1-30 of the '741 Patent ("Challenged Claims") are entitled to a May 6, 2005 priority date and are subject to pre-AIA provisions.

A. *DUA* (EX1023)

Dua was filed on January 21, 2005 and published on July 27, 2006. Thus, *Dua* is prior art under pre-AIA 35 U.S.C. § 102(e).

Dua is titled "Method and Apparatus for Managing Credentials Through a Wireless Network." *Dua* relates generally to systems and methods for conducting financial transactions using a cell phone. EX1023, [0026], [0041], [0296], FIG. 7. *Dua*'s cell phone is loaded with a wallet application, which manages a user interface, data storage, processing, and communication associated with the financial transaction functionality. *Id.*, [0288], [0309]–[0311]. *Dua* describes that "PIN-entry is required before the wallet application can be 'opened' and any credentials transmitted to an external device," and that devices "with embedded biometric technologies could use a fingerprint in lieu of a PIN code to authenticate a user to the wallet application." *Id.*, [0366]. *Dua* further explains that a user may "designate specific credentials in their wallet as requiring advance PIN-entry and others to function without the prior input of the wallet PIN," so that certain credentials having an associated "reader key" can be transmitted without authentication while others

cannot. *Id.*, [0367]–[0370]. *Dua* also discloses a “wallet button” and three “hot buttons” (“Credit,” “Debit/ATM,” and “QuickWave”), which can be configured to launch the wallet application and to act as shortcuts for transmitting frequently used credentials. *Id.*, [0383]–[0395], FIG. 7. In the QuickWave mode, the device can transmit pre-selected PIN-less credentials to a reader which has previously registered a “reader key” with the device, without requiring the user to enter a PIN. *Id.*, [0392]. In the Credit and Debit modes, the device can transmit credit card and debit card information, respectively, upon successful authentication by the user. *Id.*, [0393], [0395].



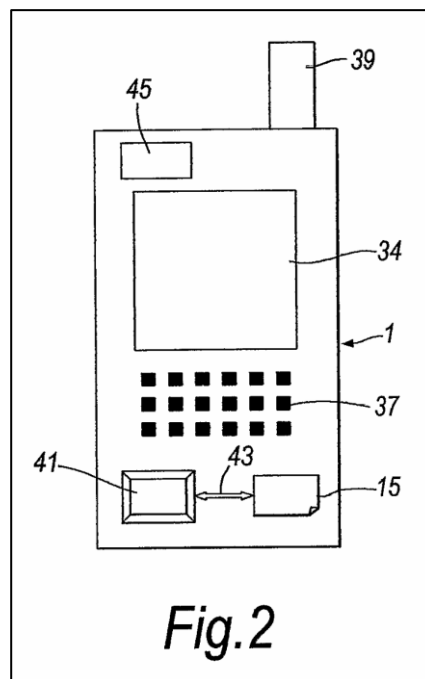
EX1023, FIG. 7.

B. *WATERS* (EX1024)

Waters (U.S. Pat. Pub. No. 2009/0215385) published on August 27, 2009 and claims priority to WO 2006/087503, which was filed on February 15, 2005. WO 2006/087503 was filed as a PCT application in Great Britain, was published in English, and designated the United States. Thus, *Waters* is prior art under pre-AIA 35 U.S.C. § 102(e).

Waters is titled “Security for Wireless Communication” and relates generally to “a mobile terminal ... which includes a near field or RFID tag (41)” for facilitating financial transactions. EX1024, Abstract. *Waters* explains that its mobile terminal “is operable to obtain security data from the user thereof, such as a PIN or biometric data,” and that “[t]he input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment.” *Id.* “The keypad **37** of the mobile terminal **1** is used to enter a PIN (or other secret password) to enable the near field tag **41**,” or “the mobile terminal **1** may incorporate a fingerprint reader **45**,” which “scans the fingerprint of the user when the user’s finger is placed on the reader **45** and compares it to the user’s fingerprint stored in the memory of the mobile terminal **1** or the SIM **15**.” *Id.*, [0051]. If the PINs or fingerprints match, “the SIM transmits a message, via link **43**, to the near field tag **41** to activate the near field tag.” *Id.*

Waters's mobile terminal **1** includes “a near field or RFID tag **41**” that “includes an inbuilt inductive antenna that allows the card to exchange information with a tag reader when the two are brought into close proximity,” and that “may transmit selected information.” *Id.*, [0034]–[0035]. The tag “is selectively enabled or disabled for communication with the reader under control of the SIM **15**, by means of communication link **43**.” *Id.*, [0037].



Id., FIG. 2.

C. *WOIKE* (EX1025) (SECONDARY REFERENCE)

Woike (International Patent Publication No. WO 2001/054079) was published July 26, 2001, and is prior art under pre-AIA 35 U.S.C. § 102(a)(1).

VII. INVALIDITY

A. **GROUND 1-2: *DUA***

Dua anticipates and/or renders obvious claims 1-13, 15-28, and 30.

i. **Independent Claim 1**

1[Pre]: A method of performing a financial transaction using a cellular telephone, the method comprising:

To the extent the preamble is limiting, *Dua* discloses it. *Dua* describes a “mobile device” (*i.e.*, cellular telephone) “with a wallet application” that can “transmit payment, identification, or other confidential information to a reader using the short-range transmission capability of the wireless device (e.g. RF).” *Id.*, [0315]. Thus, *Dua* discloses 1[Pre].

1[a]: placing the cellular telephone within reading range of a wireless communication device,

Dua discloses that “[d]uring a proximity transaction, the wireless device can transmit payment, identification, or other confidential information to a reader using the short-range transmission capability of the wireless device (e.g. RF).” EX1023, [0315]. For example, “a wireless device loaded with a wallet application, that also has an integrated RFID chip can simply be waved slowly in close proximity to a reader device to facilitate a transaction.” *Id.* The reader device is connected to “point of sale terminal 860.” *Id.*, [0405], FIG. 8. Thus, *Dua* discloses Limitation 1[a].

1[b]: the cellular telephone being configured to communicate wirelessly using an inductive coupling and an RF antenna,

Dua states that its device has “an integrated short-range communication capability for transmitting confidential information and exchanging other data between the wallet application and an external reader that is in proximity to the wireless device.” EX1023, [0041]. Specifically, *Dua* explains that “[w]ireless devices with integrated RFID proximity chips or Near Field Communication (NFC) technology may also provide users the ability to transfer information to a reader device.” *Id.*, [0016].

Dua’s wireless device includes an RFID interface configured to carry out transactions using RFID communication. *Id.*, [0378]. *Dua* also explains that ISO/IEC 14443, which describes the use of inductive coupling antennas to facilitate contactless payments, was known in the art. *Id.*, [0013]; EX1014, ¶¶393-95.

While *Dua* does not expressly disclose “using an inductive coupling and an RF antenna,” implementation of an RFID antenna (a type of RF antenna), which uses inductive coupling, naturally flows from *Dua*’s disclosure of such RFID communication, in particular because of *Dua*’s disclosure of NFC technology. EX1014, ¶¶393-95.

To the extent that “RF antenna” means an antenna for RF communications separate from the RFID antenna, *Dua* also discloses or renders obvious this limitation. For example, *Dua* describes “peer-to-peer” transactions with connectivity

“made via 802.11a/b/g, Bluetooth, or other RF protocols.” EX1023, [0318]. *Dua* also describes that “[i]n a remote—or online—environment, transactions are conducted with a remote server over a wireless network. For example, a remote transaction using a wireless device can be conducted over the Internet with a browser on the wireless device.” *Id.*, [0323]; *see also id.*, [0423] (describing web-based transactions). *Dua* further explains that “wireless device 200 is preferably a device that is capable of wirelessly connecting to the Internet using network protocols such as GSM/GPRS, CDMA2000, W-CDMA, EDGE, HDR, 1xRTT, UMTS, IMT-2000, 802.11a, 802.11b, 802.11g, or BLUETOOTH or other relevant protocols developed hereinafter.” *Id.*, [0041]. These include RF protocols that can operate over a cellular network. EX1014, ¶¶393-95.

Thus, *Dua* discloses, or at least renders obvious, Limitation 1[b].

1[c]: wherein communication by the cellular telephone is responsive to a circuit including an electronic switch configured to change a state of the circuit,

Dua explains that “[t]he wallet application handles processing of incoming credentials and extensions, the execution of extensions within the wallet framework, controlling access to secure storage, *enabling communication with an embedded RF interface* or smart card, and facilitating the use of operating system and hardware features such as display and sound.” EX1023, [0309]. A POSITA would understand that the wireless device running the wallet application that enables communication

with the embedded RF interface necessarily includes processing and control circuitry (*i.e.*, a circuit) that executes the wallet application and controls the embedded RF interface or smart card. EX1014, ¶¶396-98.

Dua further discloses the use of PIN or biometric authentication to implement RFID communication logic responsive to a PIN or biometric sensor. *Id.*, [0395] (“a user may be required to input a PIN...to enable RF communication”), [0414] (“biometrics could also be used in lieu of PINs”).

A POSITA would understand that the PIN and biometric authentication mechanisms necessarily include an electronic switch that, in response to PIN or biometric entry, makes or breaks an electrical connection in the processing or control circuitry that executes the wallet application and controls the embedded RF interface (*i.e.*, the circuit). EX1014, ¶¶396-98. A POSITA would understand that the electronic switch, in response to PIN or biometric entry, makes or breaks an electrical connection in the circuit, causing an electronic signal to change the operative state of the circuit (*e.g.*, from disabled to enabled; from PIN-less to authenticated). EX1014, ¶¶396-98; EX1023, [0367] (describing PIN-less state), [0395] (describing disabled/enabled states), [0397] (describing authenticated state), [0414] (biometrics can be used in lieu of PINs). Thus, *Dua* discloses Limitation 1[c].

1[d]: the circuit being configured to communicate responsive to the state of the circuit;

As noted above, *Dua*'s processing and control circuitry executes the wallet application and controls RF interface communication responsive to the state of the circuit (*e.g.*, enabled, disabled; PIN-less, authenticated). *See supra* § VII.A.i.1[c]; EX1023, [0309].

Dua teaches that a user may “designate specific credentials in their wallet as requiring advance PIN-entry and others to function without the prior input of the wallet PIN.” EX1023, [0368]; *see also id.*, [0367], [0369]-[0370].

Dua explains that “[t]he PIN-less option for certain credentials that have a ‘reader key’ associated with them allows users to complete time-sensitive transactions by simply passing their wireless device in front of a reader without any further key entry.” EX1023, [0370]. *Dua* further explains that after the wallet application is launched, it can prompt the user to enter a PIN or biometric to access authentication-protected credentials. *See, e.g., id.* [0366].

Thus, because the circuit can transmit a PIN-less credential (*e.g.*, communicate less sensitive financial account information) in a PIN-less state and a PIN/biometric protected credential (*e.g.*, communicate more sensitive financial account information) in an authenticated state, *Dua* discloses communication responsive to the state of the circuit. EX1014, ¶399.

1[e]: activating the electronic switch within the cellular telephone to change the state of the circuit, activation of the electronic switch being responsive to a biometric sensor included in the cellular telephone; and

Dua discloses Limitation 1[e] for the reasons discussed above in § VII.A.i.1[c]. Specifically, a POSITA would understand that the biometric authentication mechanism taught by *Dua* necessarily discloses an electronic switch that, in response to a correct biometric entry, is activated to make or break an electrical connection in the processing or control circuitry that executes the wallet application and controls the embedded RF interface (*i.e.*, a circuit). EX1014, ¶400. A POSITA would further understand that the electronic switch, in response to PIN or biometric entry, makes or breaks an electrical connection in the circuit, causing an electronic signal to change the operative state of the circuit (*e.g.*, from disabled to enabled; from PIN-less to authenticated). Thus, *Dua* discloses Limitation 1[e]. EX1014, ¶400.

1[f]: communicating financial account information from the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate the financial transaction, the communication of the financial account information using the inductive coupling or the RF antenna.

Dua discloses communication by the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate a financial transaction using inductive coupling or an RF antenna. *See* §§ VII.A.i.1[Pre], 1[b]-1[d].

Dua explains that the wallet application “is specifically designed to store several types of electronic credentials,” including “Payment Methods” such as “[c]redit, debit/ATM, stored value, electronic check, and RFID payment methods.” EX1023, [0334], [0336]. The “credential record” contains “Account number” among other account-specific information. *Id.*, [0297], [0302]-[0304]. *Dua* further states that “[e]lectronic credentials issued to a user and stored in the wallet application can be used” in a proximity transaction, where “the wireless device can transmit payment, identification, or other confidential information to a reader using the short-range transmission capability of the wireless device (e.g. RF).” *Id.*, [0313]-[0315]. *Dua* also describes “peer-to-peer” transactions with connectivity “made via 802.11a/b/g, Bluetooth, or other RF protocols” and that “remote transaction[s] using a wireless device can be conducted over the Internet with a browser on the wireless device.” *Id.*, [0318], [0323]; *see also id.*, [0423] (describing web-based transactions). In these cases, communication of financial account information is responsive to the state of the circuit as explained above. §§ VII.A.i.1[c], 1[e]. Thus, *Dua* discloses Limitation 1[f]. EX1014, ¶¶401-03.

Accordingly, *Dua* discloses or renders obvious each element of independent Claim 1. EX1014, ¶¶391-403.

ii. **Dependent Claims 2-13, 15-18**

Claim 2: The method of claim 1, wherein the circuit is configured to facilitate the financial transaction responsive to the biometric sensor; and

Claim 4: The method of claim 1, wherein the circuit is configured to communicate the financial account information responsive to the biometric sensor.

Dua discloses every element of Claim 1. *See* § VII.A.i. *Dua*'s wallet is "the core" of the platform and "handles...enabling communication with an embedded RF interface," including performance of financial transactions. EX1023 [0309], [0315]. The "default security setting in the wallet application is that PIN-entry is required before the wallet application can be 'opened' and any credentials transmitted to an external device." EX1023 [0366]. *Dua* further discloses that the PIN-entry can be replaced with "a fingerprint in lieu of a PIN code to authenticate a user to the wallet application" in phones with "embedded biometric technologies." EX1023, [0366].

As identified in § VII.A.i, *Dua*'s "circuit" is the processing and control circuitry that executes the wallet application and controls the embedded RF interface or smart card. EX1014, ¶¶404-05. That circuitry is configured to facilitate the financial transaction and to communicate financial account information based on the functionality of the wallet application it executes. EX1014, ¶¶404-05. Thus, by making the wallet application functionality and transmission of financial credentials responsive to a fingerprint sensor, *Dua* discloses Claims 2 and 4. EX1014, ¶¶404-05.

Claim 3: The method of claim 1, wherein the circuit is configured to approve the financial transaction responsive to the biometric sensor.

Dua discloses every element of Claim 1. *See* § VII.A.i. As noted above, *Dua* discloses that a biometric sensor can be used to enable financial transactions. *See* claim 2 and § VII.A.i.1[e]. *Dua* also explains that “[t]he wallet application displays the PIN Approval Request received from Sample Bank, and prompts the user to enter his PIN in order to approve the transaction.” EX1023, [0419], Fig. 9. *Dua* further explains that “biometrics could also be used in lieu of PINs” in such verification methods. *Id.*, [0414] (“For example, a user may be prompted to scan his fingerprint using an integrated scanner in the wireless device **800** instead of inputting a PIN as described earlier.”).

As identified in § VII.A.i, *Dua*’s “circuit” is the processing and control circuitry that executes the wallet application and controls the embedded RF interface or smart card. EX1014, ¶¶406-07. That circuitry is configured to approve the financial transaction based on the functionality of the wallet application it executes. EX1014, ¶¶406-07. Thus, by making the wallet application’s user authentication and financial transaction approval responsive to a fingerprint sensor, *Dua* discloses Claim 3. EX1014, ¶¶406-07.

5[Pre]: The method of claim 1,

Dua discloses every element of Claim 1. *See* § VII.A.i.

5[a]: wherein the circuit is changed from a first ON state to a second ON state, responsive to the electronic switch,

Dua explains that its circuit—the processing and control circuitry executing the wallet application and controlling the embedded RF interface—can operate in multiple ON states that differ in whether authentication is required and in which credentials can be transmitted. EX1014, ¶409. *Dua* teaches that a user may “designate specific credentials in their wallet as requiring advance PIN-entry and others to function without the prior input of the wallet PIN.” EX1023, [0368]; *see also id.*, [0367], [0369]-[0370].

Dua explains that “[t]he PIN-less option for certain credentials that have a ‘reader key’ associated with them allows users to complete time-sensitive transactions by simply passing their wireless device in front of a reader without any further key entry.” EX1023, [0370]. A POSITA would understand that this functionality necessarily discloses that the underlying processing and control circuitry executing the wallet application is in a first ON state. EX1014, ¶409.

Dua explains that after the wallet application is launched, it can prompt the user to enter a PIN or biometric to access authentication-protected credentials. *See, e.g., id.* [0366]. In one embodiment using a “wallet button,” the wallet application is first launched without authentication and then prompts the user to enter a PIN. *Id.*, [0384]. And “if the user wants to open the wallet application to select credentials or make changes to settings, the user can simply enter his wallet PIN when prompted.”

Id. *Dua* further explains that the PIN-entry can be replaced with “a fingerprint in lieu of a PIN code to authenticate a user to the wallet application” in phones with “embedded biometric technologies.” *Id.* As discussed above in § VII.A.i.1, this authentication mechanism is used to change the operative state of the circuit (*i.e.*, from a PIN-less state to an authenticated state enabling RF communication of secured credentials). EX1014, ¶409. A POSITA would understand this state of the circuit to be a second ON state. *Id.*

A POSITA would have understood these two states to be a first ON state and a second ON state as recited in Claim 5, because different credentials are transmitted in each state (*e.g.*, less sensitive PIN-less credentials, more sensitive credentials requiring PIN/biometric entry). EX1014, ¶409; EX1023, [0383], [0384], [0394]. A POSITA would further have understood that successful PIN or biometric authentication activates the electronic switch, which makes or breaks an electrical connection in the circuit, causing an electronic signal to change the operative state of the circuit from the first ON state (*i.e.*, wallet application is launched and communication of PIN-less credentials is enabled) to the second ON state (*i.e.*, authenticated and communication of PIN/biometric-protected credentials is enabled). EX1014, ¶409; EX1023, [0366], [0368], [0384].

Thus, *Dua* discloses Limitation 5[a]. EX1014, ¶409.

5[b]: and wherein the circuit includes a memory configured to store the first and second ON states.

Dua's wireless device includes the circuit identified in § VII.A.i (the processing and control circuitry that executes the wallet application and controls the embedded RF interface or smart card) and memory. EX1014, ¶410; EX1023, [0309]. *Dua* discloses that its circuit can be changed from a first ON state (*i.e.*, the PIN-less state in which only credentials designated for PIN-less use can be transmitted) to a second ON state (*i.e.*, the authenticated state in which PIN-protected credentials can also be transmitted). *See* §§ VII.A.i.1[c]-1[d], VII.A.ii (Limitation 5[a]). A POSITA would have understood that, to enable implementation of the software-based logic described above (transitioning from a first ON state to a second ON state), it would have been necessary for the circuit to store the alternative ON states in memory. EX1014, ¶410; *see* EX1029, 273, 278–280. Alternatively, it would have been obvious to store the state in memory, as software/firmware execution was known to store data in memory, including state memory or registers, in order to take different execution action based on the content of that data. *Id.* Thus, *Dua* discloses Limitation 5[b]. EX1014, ¶410.

Accordingly, *Dua* discloses or renders obvious each element of Claim 5. EX1014, ¶¶408-10.

6[Pre]: The method of claim 1,

Dua discloses every element of Claim 1. *See* § VII.A.i.

6[a]: wherein the circuit is changed from a first ON state to a second ON state, responsive to the electronic switch,

Dua discloses Limitation 6[a] for the reasons discussed above in § VII.A.ii (Limitation 5[a]).

6[b]: and wherein different amounts of personal information are communicated via the inductive coupling or RF antenna in the first ON state relative to the second ON state.

Dua describes various categories of information that can be contained in its wallet application, including “Personal Information—Name, billing address, shipping address, home phone number, business phone number, fax number, social security number, and date of birth. Electronic business cards could also be stored.” EX1023, [0343]. *Dua* discloses that the circuit identified in § VII.A.i has a first ON state (*i.e.*, the PIN-less state) and a second ON state (*i.e.*, the authenticated state), as discussed in § VII.A.ii (Limitation 5[a]). A user can “designate specific credentials in their wallet as requiring advance PIN-entry and others to function without the prior input of the wallet PIN.” *Id.*, [0368]. In the first ON state, the circuit transmits only “a credential that has a ‘reader key’ and is approved for PIN-less transactions” (*e.g.*, less-sensitive personal information). *Id.*, [0383]; *see also id.*, [0369]-[0370]. Once the electronic switch is activated by correct biometric entry and the circuit enters the second ON state, the circuit can transmit the PIN-less credentials, plus PIN-protected credentials (*e.g.*, payment and other sensitive personal information) to carry out a credit card or debit card transaction. *Id.*, [0393]

(“Pressing buttons **1** or **2** could in addition to transmitting a payment method, also transfer a PIN-less credential that has a ‘reader key’ associated with it—provided that the reader sent the key in its initial communication with the wireless device.”). Thus, *Dua* discloses Limitation 6[b]. EX1014, ¶413.

Accordingly, *Dua* discloses or renders obvious each element of Claim 6. EX1014, ¶¶411-13.

Claim 7: The method of claim 1, wherein the circuit is configured to store transaction logs.

Dua discloses every element of Claim 1. *See* § VII.A.i. *Dua* states that “the wallet application will log all transactions made in proximity, personal, or remote mode.” EX1023, [0489]. The wallet application maintains transaction history including details such as date, time, merchant, and amount. *Id.*, [0362]. As identified in § VII.A.i, *Dua*’s circuit is the processing and control circuitry that executes the wallet application and controls the embedded RF interface or smart card. EX1014, ¶414. That circuitry is configured to store transaction logs based on the functionality of the wallet application it executes. EX1014, ¶414. Thus, *Dua* discloses Claim 7. EX1014, ¶414.

Claim 8: The method of claim 1, wherein the circuit is configured for a user to select between a plurality of financial accounts for the financial transaction.

Dua discloses every element of Claim 1. *See* § VII.A.i. *Dua*’s wallet application can store multiple payment credentials, including “[c]redit, debit/ATM,

stored value, electronic check, and RFID payment methods.” EX1023, [0336]. *Dua* further explains that “[o]nce the user completes making his selection(s) in the ‘Credential Selector’, the wallet application is ready to transmit the credential(s) via its RFID interface.” *Id.*, [0378]. As identified in § VII.A.i, *Dua*’s circuit is the processing and control circuitry that executes the wallet application and controls the embedded RF interface or smart card. EX1014, ¶415. The circuit is configured for a user to select between a plurality of financial accounts for the financial transaction based on the functionality of the wallet application it executes. EX1014, ¶415. Thus, *Dua* discloses Claim 8. EX1014, ¶415.

Claim 9: The method of claim 1, wherein the cellular telephone is configured for a user to enter an amount of the financial transaction, and further comprising entering the amount to facilitate the financial transaction.

Dua discloses every element of Claim 1. *See* § VII.A.i. *Dua* discloses that its device can facilitate “person-to-person, person-to-company, or company-to-company electronic payments or fund transfers.” *Id.*, [0048], [0311]. Such functionality includes a “mechanism by which a user could transfer funds to another user.” *Id.*, [0311]. *Dua* further explains that an “an over-the-air reload tool” associated with a stored value credential can be programmed into the wallet application. EX1023, [0293]. It would have been obvious to a POSITA that these mechanisms would include a user interface (for example, *Dua*’s display screen showing a transaction amount field, in combination with *Dua*’s key pad, with which

the user can enter an amount into the field) for a user to enter an amount of money to transfer to another user, company, or reload card as the device would require such information, in order to facilitate a transaction. EX1023, [0041]; EX1014, ¶416. Thus, *Dua* discloses, or at least renders obvious, Claim 9. EX1014, ¶416.

Claim 10: The method of claim 1, wherein the circuit is configured to communicate a financial account number via the inductive coupling or RF antenna to facilitate the financial transaction.

Dua discloses every element of Claim 1. *See* § VII.A.i. *Dua* discloses that the circuit is configured to communicate financial account information via the inductive coupling or RF antenna to facilitate the financial transaction. *See* § VII.A.i.1[f]. *Dua* further provides that the credential record contains an “Account number” that is transmitted via the RFID interface. EX1023, [0297], [0302]-[0304], [0383]. Thus, *Dua* discloses Claim 10. EX1014, ¶417.

Claim 11: The method of claim 1, wherein the cellular telephone includes a user interface configured to enter a financial account number and includes memory configured to store the financial account number for use in the financial transaction.

Dua discloses every element of Claim 1. *See* § VII.A.i. *Dua* states that the wallet application may request the user to enter “such information as the user’s account number with the issuer.” EX1023, [0444]. *Dua* further provides that “[t]he wallet application is specifically designed to store several types of electronic credentials.” *Id.*, [0334]. These credentials are stored in memory. *Id.*, [0381]. *Dua*

further provides that the credential record contains an “Account number” that is transmitted via the RFID interface. EX1023, [0297], [0302]-[0304], [0383]. Thus, *Dua* discloses Claim 11. EX1014, ¶418.

12[Pre]: The method of claim 1,

Dua discloses every element of Claim 1. *See* § VII.A.i.

12[a]: wherein the cellular telephone is configured for a user to enter a personal identification number (PIN), communication of the financial account information via the inductive coupling or RF antenna being responsive to the personal identification number;

12[b]: and further comprising entering the personal identification number to facilitate the financial transaction.

As discussed above in § VII.A.i, *Dua* discloses the use of a biometric authentication mechanism to facilitate a financial transaction. *Dua* also describes that, separate from wallet application authentication, “[c]ertain credential issuers such as financial institutions may require that users validate their identity during a transaction by providing a PIN that was established with or set by the financial institution.” EX1023, [0397]. *Dua* further describes: “credential issuers may issue a credential to a wireless device, require the wallet PIN with every transaction, but also prompt the user for an issuer PIN (or PIN set with the issuer) on the POS terminal during each transaction. The POS terminal may know to prompt for a PIN based on a card BIN number for example.” *Id.*, [0402]. Since *Dua*’s mobile device is configured for PIN-entry (*see* EX1023, [0366]), it would have been obvious to a

POSITA that this dual-authentication scheme (*i.e.*, biometric entry to open the wallet application followed by issuer PIN entry to facilitate the transaction) could be executed by utilizing the fingerprint sensor and the PIN-entry functionalities of the mobile device itself. EX1014, ¶420.

Accordingly, *Dua* discloses or renders obvious each element of Claim 12. EX1014, ¶¶419-21.

Claim 13: The method of claim 1, wherein the cellular telephone includes a memory configured to store a key required to change the state of the circuit to facilitate the financial transaction.

Dua discloses every element of Claim 1. *See* § VII.A.i. *Dua* explains that a reader key “is sent with an electronic credential record to a wireless device during the issuance process.” EX1023, [0353]. The reader key is then stored in the wireless device’s memory “with the electronic credential to which it is linked.” *Id.*, [0354]; EX1014, ¶422. All RFID readers associated with the issuer also store a corresponding key. *Id.*, [0353]. At the start of a transaction, an RFID reader associated with the issuer transmits its key to the wireless device. *Id.* The circuit identified in § VII.A.i then passes the key to the wallet application it executes, which uses the key to look up a credential associated with the corresponding reader key, which was received and stored during the issuance process. *Id.*, [0353], [0354]. The circuit then completes a transaction using the relevant credential. *Id.* Such functionality “allows a reader device to automatically capture specific credential

information from a wireless device without the end-user having to scroll through different screens within the wallet application and pressing multiple buttons on his device.” *Id.*, [0355]. Thus, the reader key, which is stored in memory, is used to transition the circuit to an ON state that enables RF communication with the issuer-associated reader. EX1014, ¶422. Thus, *Dua* discloses Claim 13. EX1014, ¶422.

Claim 15: The method of claim 1, wherein the cellular telephone is configured to store a financial account number and the communication via the inductive coupling or RF antenna including the financial account number.

Dua discloses every element of Claim 1. *See* § VII.A.i. *Dua* discloses that the circuit is configured to communicate financial account information including the account number via the inductive coupling or RF antenna to facilitate the financial transaction. *See* §§ VII.A.i.1[f]; VII.A.ii (Claim 11). Thus, *Dua* discloses Claim 15. EX1014, ¶423.

Claim 16: The method of claim 1, wherein activating the electronic switch is responsive to data stored in memory of the cellular telephone and the data stored in the memory includes biometric data.

Dua discloses every element of Claim 1. *See* § VII.A.i. *Dua* discloses “activating the electronic switch within the cellular telephone to change the state of the circuit, activation of the electronic switch being responsive to a biometric sensor included in the cellular telephone.” *See* § VII.A.i.1[e]. A POSITA would have understood that, to enable implementation of the software-based logic described

above (authentication using biometric verification via a fingerprint scanner), it would have been necessary, or at least obvious, for the circuit to store the user's biometric data in memory for comparison to the biometric data entered, and that activation of the electronic switch is therefore responsive to that stored biometric data. EX1023, [0366]; EX1014, ¶424. Thus, *Dua* discloses Claim 16. EX1014, ¶424.

Claim 17: The method of claim 1, wherein the financial account information includes an account number corresponding to a financial account of a user of the cellular telephone.

Dua discloses Claim 17 for the reasons discussed above in § VII.A.ii (Claim 10).

18[Pre]: The method of claim 1,

Dua discloses every element of Claim 1. *See* § VII.A.i.

18[a]: wherein the financial account information is stored in a memory on the cellular telephone,

18[b]: the financial account information corresponding to one of a plurality of financial accounts of a user of the cellular telephone, the method further comprising:

Dua discloses limitations 18[a]-[b] for the same reasons as discussed above in § VII.A.ii (Claims 11 and 8, respectively).

18[c]: presenting a user interface to the user, the user interface being configured to allow the user to select a specific

member of the plurality of financial accounts of the user for the financial transaction;

Dua states that “[a] ‘Credential Selector’ in the wallet application allows for one credential or multiple credentials to be selected from the credential tree (described earlier) for transmission to a reader device.” EX1023, [0371], [0378]. Thus, *Dua* discloses Limitation 18[c]. EX1014, ¶429.

18[d]: and wherein the step of communicating financial account information includes communicating financial account information corresponding to the selected specific member of the plurality of financial accounts.

As discussed immediately above, *Dua* states that “[a] ‘Credential Selector’ in the wallet application allows for one credential or multiple credentials to be selected from the credential tree (described earlier) *for transmission to a reader device.*” EX1023, [0371], [0378]. Thus, *Dua* discloses Limitation 18[d]. EX1014, ¶430.

Accordingly, *Dua* discloses or renders obvious each element of Claim 18. EX1014, ¶¶426-31.

iii. **Independent Claim 19**

19[Pre]: A method of performing a financial transaction using a cellular telephone, the method comprising:

19[a]: placing the cellular telephone within reading range of a wireless communication device,

19[b]: the cellular telephone being configured to communicate wirelessly using an RF antenna,

Dua discloses limitations 19[Pre]-[d] for the reasons discussed above in § VII.A.i.1[Pre]-1[b].

19[c]: wherein the RF antenna is responsive to a circuit including an electronic switch configured to change a state of the circuit,

19[d]: the circuit being configured to communicate via the RF antenna responsive to the state of the circuit;

Limitations 19[c]-[d] are substantively identical to Limitations 1[c]-[d] except that Limitations 19[c]-[d] require that “the RF antenna” (rather than “communication by the cellular telephone” as recited in Limitations 1[c]-[d]) is “responsive to the state of the circuit.” As discussed above in § VII.A.i.1[b], “communication by the cellular telephone” in *Dua* occurs using an RF antenna. Thus, *Dua* discloses limitations 19[c]-[d] for the reasons discussed above in § VII.A.i.1[c]-1[d].

19[e]: activating the electronic switch within the cellular telephone to change the state of the circuit, activation of the electronic switch being responsive to entry of a personal identification number;

Dua describes that “[t]he default security setting in the wallet application is that PIN-entry is required before the wallet application can be ‘opened’ and any

credentials transmitted to an external device.” EX1023, [0366]. *Dua* further discloses that a user “may be required to input a PIN and click ‘OK’ to enable RF communication for a 30 second window” or to “input his PIN, click ‘OK’ to initiate PIN verification, and upon positive confirmation be prompted to hold down either button 1 or 2 while placing the device in close proximity to a reader.” *Id.*, [0395].

A POSITA would understand that this PIN-based authentication mechanism necessarily discloses the same electronic switch identified in § VII.A.i.1[c], which, in response to correct PIN entry, makes or breaks an electrical connection in the processing and control circuitry that executes the wallet application and controls the embedded RF interface (*i.e.*, the circuit). EX1014, ¶¶438-39. A POSITA would further understand that the electronic switch, in response to PIN or biometric entry, makes or breaks an electrical connection in the circuit, causing an electronic signal to change the operative state of the circuit (*e.g.*, from disabled to enabled, from PIN-less to authenticated). EX1014, ¶¶438-39; *see also* § VII.A.i.1[c]. Thus, *Dua* discloses Limitation 19[e]. EX1014, ¶¶438-39.

19[f]: and communicating financial account information from the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate the financial transaction, the communication of the financial account information using the RF antenna.

Dua discloses Limitation 19[f] for the reasons discussed above in § VII.A.i.1[f].

Accordingly, *Dua* discloses or renders obvious each element of independent Claim 19. EX1014, ¶¶432-41.

iv. **Dependent Claims 20-28, 30**

Claim 20: The method of claim 19, wherein the communication of the financial account information is responsive to a biometric sensor and a mechanical switch included in the cellular telephone.

Dua discloses every element of Claim 19. *See* § VII.A.iii. As discussed above in § VII.A.ii (Limitation 12[b]), *Dua* renders obvious a dual-authentication scheme using both PIN-entry (*e.g.*, as recited in Claim 19) and a biometric sensor (*e.g.*, as recited in Claim 20). *Dua* provides that its “wallet button” can “be used as a short-cut for the user to launch the wallet application without using the wireless device’s operating system functions used to launch resident applications.” EX1023, [0384]. *Dua*’s wallet button corresponds to a mechanical switch. EX1014, ¶442. Additionally, *Dua* explains that once the application is launched using the wallet button, “the application is ready to communicate with a reader, and simultaneously prompts the user for his Wallet PIN. . . . Separately, if the user wants to open the wallet application to select credentials or make changes to settings, the user can simply enter his wallet PIN when prompted.” EX1023, [0384]. As discussed throughout *Dua* and this petition, “wireless devices with embedded biometric technologies could use a fingerprint in lieu of a PIN code to authenticate a user to the wallet application.” *Id.*, [0366]. Thus, by describing a wallet button (*i.e.*,

a mechanical switch) that opens the wallet application, the wallet application prompting the user for authentication (*e.g.*, utilizing the biometric sensor), and subsequent entry of an issuer PIN (*see* § VII.A.ii (Limitation 12[b])), *Dua* discloses Claim 20. EX1014, ¶442.

Claim 21: The method of claim 19, further comprising approving the financial transaction using a biometric sensor.

Dua discloses every element of Claim 19. *See* § VII.A.iii. “[A]pproving the financial transaction using a biometric sensor” is disclosed by *Dua*. *See* § VII.A.i.1[e]. Thus, *Dua* discloses Claim 21. EX1014, ¶443.

Claim 22: The method of claim 19, wherein the cellular telephone includes a user interface configured for a user to enter a financial account number for use in the financial transaction.

Dua discloses every element of Claim 19. *See* § VII.A.iii. *Dua* also discloses a user interface for entering financial account numbers. *See* § VII.A.ii (Claim 11). Thus, *Dua* discloses Claim 22. EX1014, ¶444.

23[Pre]: The method of claim 22,

Dua discloses every element of Claim 22. *See* § VII.A.iv (Claim 22).

23[a]: wherein the cellular telephone includes memory configured to store the financial account number, wherein

the circuit is configured for the user to select between a plurality of financial accounts for the financial transaction;

23[b]: and further comprising selecting a specific member of the plurality of financial accounts for the financial transaction.

Dua discloses Limitations 23[a]-[b] for the reasons discussed above in § VII.A.ii (Claims 8 and 11).

Accordingly, *Dua* discloses or renders obvious each element of Claim 23. EX1014, ¶¶444-47.

Claim 24: The method of claim 19, wherein the circuit is configured for a user to select between a plurality of financial accounts for the financial transaction.

Dua discloses Claim 24 for the reasons discussed above in § VII.A.ii (Claim 8).

25[Pre]: The method of claim 19,

Dua discloses every element of Claim 19. *See* § VII.A.iii.

25[a]: wherein the circuit is changed from a first ON state to a second ON state, responsive to the electronic switch,

Dua discloses Limitation 25[a] for the reasons discussed above in § VII.A.ii (Limitation 5[a]).

To the extent that “RF antenna” here refers to an antenna for RF communications via a cellular network, *Dua* discloses this limitation. EX1014, ¶¶450-51. In this context of RF communications via a cellular network, a POSITA would have understood that the circuit is in a first ON state when the mobile

telephone is powered on (*i.e.*, the mobile telephone has service and can communicate with the cellular network). EX1014, ¶¶450-51. A POSITA would further understand that circuit is in a second ON state when the RF interface is enabled to communicate with a reader. EX1014, ¶¶450-51. Thus, *Dua* discloses Limitation 25[a].

25[b]: and wherein different amounts of personal information are communicated via the RF antenna in the first ON state relative to the second ON state.

Dua discloses Limitation 25[b] for the reasons discussed above in § VII.A.ii (Limitation 6[b]). To the extent that “RF antenna” refers to an antenna for RF communications via a cellular network, *Dua* discloses this limitation. EX1014, ¶¶452-54. A POSITA would understand that in the first ON state (*i.e.*, mobile telephone is powered on), the circuit of the mobile terminal can communicate personal information using the cellular network. EX1014, ¶¶452-54. A POSITA would further understand that in the second ON state (*i.e.*, RF interface is enabled), the circuit of the mobile terminal can communicate different amounts of personal information (*i.e.*, authentication-protected sensitive payment and personal information). *Id.*, ¶¶452-54. Thus, *Dua* renders obvious Limitation 25[b].

Accordingly, *Dua* discloses or renders obvious each element of Claim 25. EX1014, ¶¶449-54.

Claim 26: The method of claim 19, wherein the circuit is configured to store transaction logs.

Dua discloses Claim 26 for the reasons discussed above in § VII.A.ii (Claim 7).

Claim 27: The method of claim 19, wherein the circuit is configured to communicate a financial account number via the RF antenna to facilitate the financial transaction.

Dua discloses Claim 27 for the reasons discussed above. *See* § VII.A.ii (Claim 10).

Claim 28: The method of claim 19, wherein the cellular telephone is configured for storing a password in memory of the cellular phone, the password being entered by a user of the cellular phone to engage in the transaction.

Dua discloses every element of Claim 19. *See* § VII.A.iii. *Dua* discloses PIN-based authentication with the password stored in memory. *See* § VII.A.ii (Claim 12). *Dua* describes that “[t]he default security setting in the wallet application is that PIN-entry is required before the wallet application can be ‘opened’ and any credentials transmitted to an external device.” EX1023, [0366]. *Dua* further describes that “PINs can be any length, and be comprised of any combination of upper or lower case letters, numbers, and special characters as provided for by the wireless device itself.” *Id.* A POSITA would have understood such a PIN used to open and enable the wallet application can correspond to a password. EX1014, ¶457. A POSITA would have further understood that, to enable implementation of the software-based logic described above (authentication using PIN-based verification), it would have

been necessary, or at least obvious, to store the entered PIN (*i.e.*, a password) in memory, such that the device can verify whether it matches the correct PIN. EX1014, ¶457. Thus, *Dua* discloses Claim 28. EX1014, ¶457.

Claim 30: The method of claim 19, wherein the cellular telephone is configured for a user to enter an amount of the financial transaction.

Dua discloses every element of Claim 19. *See* § VII.A.iii. “[T]he cellular telephone is configured for a user to enter an amount of the financial transaction” is also disclosed, or at least rendered obvious, by *Dua*. *See* § VII.A.ii (Claim 9). Thus, *Dua* discloses, or at least renders obvious, Claim 30. EX1014, ¶458.

B. GROUND 3: *DUA* IN VIEW OF *WOIKE* RENDERS OBVIOUS CLAIMS 9, 14, 29, AND 30

i. Motivation to Combine

Dua and *Woike* are both directed to electronic systems for conducting financial transactions using portable electronic devices. EX1014, ¶459. *Dua* discloses a mobile device wallet application that uses RFID technology for contactless payments. EX1023, [0011], [0336], [0383]. *Woike* discloses a method for contactless payments using a mobile telephone and a computer. EX1025, Abstract, p. 2, ll. 14-16.

A POSITA would have been motivated to combine the wireless device of *Dua* and the methods of *Woike* because the methods of *Woike* allow the wireless device of *Dua* to be used without requiring a merchant “to set up an expensive and complex

payment system with a card reader.” *Id.*, p. 2, 28-29. “Another advantage is that the previously required printout and signing of receipts, filling out checks, or entering a PIN code is no longer necessary, thus preventing long lines at checkout. A connection to the authorization computer and entering of the ID number of the payment receiver can be completed by the purchaser shortly before paying, such that the purchaser only has to enter and verify the amount in the cell phone.” *Id.*, p.3, ll. 7-12. Implementing these methods with the mobile device and wallet application of *Dua* would allow *Dua*’s mobile device to facilitate contactless transactions with a broader group of vendors and in a broader range of environments. EX1014, ¶459.

A POSITA would have had a reasonable expectation of success in combining these references because both describe mobile device-based payment systems using similar underlying technologies. EX1014, ¶459. The combination would involve implementing *Woike*’s contactless payments with *Dua*’s mobile device and wallet application, which is a straightforward software implementation. *Id.*

ii. Claim Analysis

Claim 9.

Dua discloses every element of Claim 1. *See* § VII.A.i. *Dua* discloses, or at least renders obvious, that the user can enter transaction amounts. *See* § VII.A.ii (Claim 9). Additionally, *Woike* explains that a payment can be made by “quickly entering the identification number for the receiver of the payment, *and the payment*

amount, in the cell phone, and sending this data to the authorization computer.” EX1025, p. 2, ll. 17-19. Thus, *Dua* in view of *Woike* renders obvious Claim 9. EX1014, ¶460.

14[Pre]: The method of claim 1,

Dua discloses every element of Claim 1. *See* § VII.A.i.

14[a]: wherein the cellular telephone is configured for mechanical insertion of an electronic key,

Woike explains that “[b]ecause current cell phones can only be used with a SIM card (Subscriber Identity Module card), which usually has a PIN code, prevention of misuse of this payment method requires no additional precautions.” EX1025, p. 2, ll. 24-26. A SIM card including a PIN code (*i.e.*, an electronic key) is a separate component that is mechanically inserted into a device such as a cellular telephone. EX1014, ¶462. Thus, *Dua* in view of *Woike* renders obvious Limitation 14[a]. EX1014, ¶462.

14[b]: the electronic key including a personal identification number,

As discussed immediately above, *Woike* explains that “[b]ecause current cell phones can only be used with a SIM card (Subscriber Identity Module card), which usually has a PIN code, prevention of misuse of this payment method requires no additional precautions.” EX1025, p. 2, ll. 24-26. Thus, *Dua* in view of *Woike* renders obvious Limitation 14[b]. EX1014, ¶463.

14[c]: a signal communicated via the inductive coupling or RF antenna to facilitate the financial transaction being responsive to entry of the personal identification number by a user.

Dua discloses this limitation for the reasons discussed in § VII.A.iii.19[e].

Woike explains that the SIM card requires a PIN code, which prevents misuse of its payment methods. EX1025, p. 2, ll. 24-26. It would have been obvious to a POSITA that the PIN code included in the SIM described by *Woike* is used to authenticate a user prior to facilitating the described financial transactions. EX1014, ¶464. When implementing the methods of *Woike* using the mobile device of *Dua*, the PIN code included in the SIM described by *Woike* can be used to authenticate a user for accessing the wallet application. *Id.* Thus, *Dua* in view of *Woike* renders obvious Limitation 14[c]. EX1014, ¶464.

Accordingly, *Dua* in view of *Woike* renders obvious each element of Claim 14. EX1014, ¶¶461-65.

29[Pre]: The method of claim 19,

Dua discloses every element of Claim 19. *See* § VII.A.iii.

29[a]: wherein the cellular telephone is configured for insertion of an electronic key,

29[b]: the electronic key being configured to store the personal identification number,

29[c]: the communication via the RF antenna being responsive to the personal identification number.

Dua in view of *Woike* renders obvious Limitations 29[a]-[c] for the reasons discussed above in § VII.B.ii (Limitations 14[a]-[c]).

Accordingly, *Dua* in view of *Woike* renders obvious each element of Claim 29. EX1014, ¶467.

Claim 30.

Dua discloses every element of Claim 19. *See* § VII.A.iii. “[T]he cellular telephone is configured for a user to enter an amount of the financial transaction” is also rendered obvious, by *Dua* in view of *Woike*. *See* § VII.B.ii (Claim 9). Thus, *Dua* in view of *Woike* renders obvious Claim 30. EX1014, ¶468.

C. GROUND 4: *WATERS* IN VIEW OF *DUA* RENDERS OBVIOUS CLAIMS 1-30

i. Motivation to Combine

Waters and *Dua* are both directed to mobile payment systems using wireless communication technology. EX1014, ¶469. *Waters* discloses a mobile terminal including a near field or RFID tag, wherein the mobile terminal is operable to obtain security data from the user to confirm the identity of the user before enabling the near field tag to make a payment. EX1024, Abstract. *Dua* discloses a comprehensive

mobile wallet application with RFID capabilities. *See* § VI.A; EX1023, [0011], [0336], [0383]. Both references address the goal of improving data security in RFID applications. EX1023, [0382]–[0383]; EX1024, [0049]–[0050], [0053]. Each of these references teaches that PIN or biometric authentication can be implemented to enable or disable RFID communication, to prevent skimming. EX1014, ¶469.

Both *Waters* and *Dua* address the problem of enabling secure financial transactions using mobile devices. EX1014, ¶469. *Waters* teaches using a mobile terminal with wireless capabilities to perform financial transactions using a near field tag read by a reader. EX1024, [0041]–[0045], [0052]. *Dua* provides detailed implementation of a wallet application with credential management and RFID communication. EX1023, [0295]–[0305], [0334]–[0347].

A POSITA would have been motivated to combine *Waters* with *Dua* because *Dua* provides detailed implementation guidance for the wallet application functionality that *Waters* describes at a higher level. EX1014, ¶469. Specifically, *Dua*’s detailed disclosures regarding credential storage, user authentication, and RFID communication would have provided a POSITA with implementation details for *Waters*’s mobile payment system to make it commercially useful. *Id.* Thus, a POSITA would have been motivated to incorporate *Dua*’s wallet application, including the processing and control circuitry that executes it (*see* § VII.A.i.1[c]) into the mobile terminal of *Waters*. *Id.* This combination would enable *Dua*’s wallet

application and associated circuitry to provide additional functionality and control using the RFID enabling mechanisms and near field tag **41** of *Waters*'s mobile terminal. *Id.*

A POSITA would have had a reasonable expectation of success in combining these references because both describe compatible mobile payment technologies using RFID/NFC for contactless transactions. EX1014, ¶469. The combination would involve using *Dua*'s wallet application implementation within *Waters*'s mobile transaction framework. *Id.*

ii. **Independent Claim 1**

1[Pre].

To the extent the preamble is limiting, *Waters* in view of *Dua* renders it obvious. *Waters* teaches a mobile terminal including a near field or RFID tag, wherein the mobile terminal is operable to facilitate financial transactions. EX1024, Abstract (“use the near field tag (41) to make a payment”), [0045] (“use their RF tag to make payments”). *Waters* further states that “[t]he mobile terminal **1** may be a *handheld mobile telephone*, a personal digital assistant (PDA) or a laptop computer equipped with a datacard.” *Id.*, [0020] (emphasis added). Thus, *Waters* in view of *Dua* renders obvious 1[Pre].²

² *Dua* also discloses each limitation of Claims 1-13, 15-28, and 30 for the reasons discussed above in Grounds 1-2. *See supra* § VII.A.

1[a].

Waters explains that its RFID tag **41** can “exchange information with a tag reader when the two are brought into close proximity.” EX1024, [0035]. *Waters* further teaches that the mobile terminal can be used to “make a payment” at a reader (e.g., a point-of-sale terminal). *Id.*, Abstract; *see also id.*, [0041]–[0043], [0045]. A POSITA would understand that the tag reader disclosed in *Waters* corresponds to “a wireless communication device” as recited in Claim 1. EX1014, ¶471. Thus, *Waters* in view of *Dua* renders obvious Limitation 1[a].

1[b].

Waters teaches that its device includes an “inbuilt inductive antenna” configured to “exchange information with a tag reader when the two are brought in close proximity.” EX1024, [0035]. *Waters* further explains its “near field tag 41 may operate in accordance with ISO-IEC 14443 and ISO-IEC 15693 standards.” *Id.* A POSITA would understand that the use of inductive coupling and an RF antenna naturally flows from *Waters*'s “near field tag” including an “inbuilt inductive antenna” operating “in accordance with ISO-IEC 14443 and ISO-IEC 15693 standards.” EX1014, ¶¶472-73.

To the extent that “RF antenna” means an antenna for RF communications separate from the RFID antenna, *Waters* in view of *Dua* also discloses or renders obvious this limitation. For example, *Waters* provides “an antenna **39** for

communicating wirelessly with the mobile communications network 3.” EX1024, [0034]. *Dua* describes “peer-to-peer” transactions with connectivity “made via 802.11a/b/g, Bluetooth, or other RF protocols.” EX1023, [0318]. *Dua* further explains that “wireless device 200 is preferably a device that is capable of wirelessly connecting to the Internet using network protocols such as GSM/GPRS, CDMA2000, W-CDMA, EDGE, HDR, 1xRTT, UMTS, IMT-2000, 802.11a, 802.11b, 802.11g, or BLUETOOTH or other relevant protocols developed hereinafter.” *Id.*, [0041]. These include RF protocols that can operate over a cellular network. EX1014, ¶¶472-73. *See* § VII.A.i.1[b]. Thus, *Waters* in view of *Dua* renders obvious Limitation 1[b].

1[c].

Dua explains that “[t]he wallet application handles processing of incoming credentials and extensions, the execution of extensions within the wallet framework, controlling access to secure storage, ***enabling communication with an embedded RF interface*** or smart card, and facilitating the use of operating system and hardware features such as display and sound.” EX1023, [0309]; *see also* § VII.A.i.1[c]. A POSITA would understand that the mobile terminal of *Waters* incorporating the wallet application of *Dua* that enables communication with the embedded RF interface necessarily includes processing and control circuitry (*i.e.*, a circuit) that executes the wallet application and controls the embedded RF interface or smart card. EX1014, ¶¶474-76; *see also* § VII.A.i.1[c].

Waters explains that “the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal **1** into proximity to the reader.” EX1024, [0052]. *Waters* further states that these authentication mechanisms “may advantageously be combined with an RF tag **41** that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal **1** into proximity to the reader. After successful reading of the RF tag **41**, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal **1** is lost or stolen, an unauthorised person cannot use the RF tag **41**.” *Id.*, [0052]. It would have been obvious to a POSITA incorporating the wallet application of *Dua* into the mobile terminal of *Waters* to include the multiple ON states (*e.g.*, PIN-less state, authenticated state) discussed above (*see* §§ VII.A.i.1[c]-[d], VII.A.ii (Limitation 5[a]) controlled by these PIN and/or biometric authentication mechanism. EX1014, ¶¶474-76.

A POSITA would understand that these PIN and biometric authentication mechanisms necessarily include an electronic switch that, in response to PIN or biometric entry, makes or breaks an electrical connection in the processing or control circuitry that executes the wallet application of *Dua* (*i.e.*, the circuit) and controls the embedded RF interface (*i.e.*, automatic deauthorizing after use). EX1014, ¶¶474-76. A POSITA would further understand that the electronic switch, in response to

PIN or biometric entry, makes or breaks an electrical connection in the circuit, causing an electronic signal to change the operative state of the circuit (*e.g.*, from disabled to enabled; from PIN-less to authenticated). EX1014, ¶¶474-76; EX1023, [0367] (describing PIN-less state), [0395] (describing disabled/enabled states), [0397] (describing authenticated state), [0414] (biometrics can be used in lieu of PINs). Thus, *Waters* in view of *Dua* renders obvious Limitation 1[c].

1[d].

Waters teaches that “the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal **1** into proximity to the reader.” EX1024, [0052].

A POSITA would understand that the circuit identified in § VII.C.ii.1[c]—the processing or control circuitry that executes the wallet application of *Dua* and controls the embedded RF interface—is configured to communicate responsive to its own state, because that circuit has an enabled state in which the tag “is then able to communicate with readers” and a disabled state in which “a reader is not able to obtain any information from the near field tag **41**, even when brought into close proximity thereto.” EX1024, [0037], [0042]. The circuit communicates only in the enabled state, and it enters that state when the electronic switch identified in § VII.C.ii.1[c] is activated by correct PIN or biometric entry. *Id.*, [0051]-[0052]; EX1014, ¶477. A POSITA would further understand that, by incorporating the two

ON states discussed above in § VII.C.ii.1[c], the circuit can transmit a PIN-less credential in a PIN-less state and a PIN/biometric protected credential in an authenticated state. EX1014, ¶477; *see also supra* § VII.A.i.1[d]. Thus, *Waters* in view of *Dua* renders obvious Limitation 1[d].

1[e].

Waters discloses Limitation 1[e] for the reasons discussed above in § VII.C.ii.1[c]. Specifically, a POSITA would understand that the biometric authentication mechanism taught by *Waters* necessarily discloses an electronic switch that, in response to a correct biometric entry, is activated to make or break an electrical connection in the processing or control circuitry that executes the wallet application of *Dua* (*i.e.*, a circuit) and controls the embedded RF interface. EX1014, ¶478. A POSITA would further understand that the making or breaking of an electrical connection in the processing and control circuitry by the electronic switch changes the state of the circuit (*e.g.*, from disabled to enabled; from PIN-less to authenticated). EX1014, ¶478. Thus, *Waters* in view of *Dua* renders obvious Limitation 1[e].

1[f].

Waters in view of *Dua* renders obvious communication by the cellular telephone to the wireless communication device responsive to the state of the circuit

to facilitate a financial transaction using inductive coupling or an RF antenna. *See* §§ VII.C.ii.1[Pre], 1[b]-1[d].

A POSITA would have understood that to facilitate a financial transaction, financial account information would have to be exchanged between the cellular telephone and the wireless communication device, otherwise a vendor would not be able to charge the user's account. EX1014, ¶¶479-80. *Dua* separately discloses this limitation. *See* § VII.A.ii.1[f]. *Dua* explains that the wallet application "is specifically designed to store several types of electronic credentials," including "Payment Methods" such as "[c]redit, debit/ATM, stored value, electronic check, and RFID payment methods." EX1023, [0334], [0336]. The "credential record" contains "Account number" among other account-specific information. *Id.*, [0297], [0302]-[0304]. *Dua* further states that "[e]lectronic credentials issued to a user and stored in the wallet application can be used" in a proximity transaction, where "the wireless device can transmit payment, identification, or other confidential information to a reader using the short-range transmission capability of the wireless device (e.g. RF)." *Id.*, [0313]-[0315]. Thus, *Waters* in view of *Dua* renders obvious Limitation 1[f].

Accordingly, *Waters* in view of *Dua* renders obvious each element of independent Claim 1. EX1014, ¶¶470-81.

iii. **Dependent Claims 2-18**

Claims 2, 4.

Waters in view of *Dua* renders obvious every element of Claim 1. *See* § VII.C.ii. *Waters* teaches a mobile terminal including a near field or RFID tag, wherein the mobile terminal is operable to facilitate financial transactions. EX1024, Abstract (“use the near field tag (41) to make a payment”), [0045] (“use their RF tag to make payments”). *Waters* states that “the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader.” EX1024, [0052]. *Waters* further explains that when the RF tag is enabled, it “may transmit selected information” to the reader. *Id.*, [0035]. Conversely, in the disabled state, “a reader is not able to obtain any information from the near field tag 41, even when brought into close proximity thereto.” *Id.*, [0037]. A POSITA would have understood that to facilitate a financial transaction, financial account information would have to be exchanged between the cellular telephone and the wireless communication device, otherwise a vendor would not be able to charge the user’s account. EX1014, ¶¶482-83. *Dua* also discloses making its wallet application functionality and transmission of financial credentials responsive to a fingerprint sensor. *See* § VII.A.ii (Claims 2 and 4). *Dua* explains that the wallet application “is specifically designed to store several types of electronic credentials,” including “Payment Methods” such as “[c]redit, debit/ATM, stored value, electronic check,

and RFID payment methods.” EX1023, [0334], [0336]. The “credential record” contains “Account number” among other account-specific information. *Id.*, [0297], [0302]-[0304]. *Dua* further states that “[e]lectronic credentials issued to a user and stored in the wallet application can be used” in a proximity transaction, where “the wireless device can transmit payment, identification, or other confidential information to a reader using the short-range transmission capability of the wireless device (e.g. RF).” *Id.*, [0313]-[0315].

As identified in § VII.C.ii, the “circuit” is the processing and control circuitry that executes the wallet application of *Dua* and controls the embedded RF interface. EX1014, ¶¶482-83. That circuitry is configured to facilitate the financial transaction and to communicate financial account information based on the functionality of the wallet application it executes. EX1014, ¶¶482-83. Thus, by making the wallet application functionality and transmission of financial credentials responsive to a fingerprint sensor, *Waters* in view of *Dua* renders obvious Claims 2 and 4.

Claim 3.

Waters in view of *Dua* renders obvious every element of Claim 1. *See* § VII.C.ii. As noted above, *Waters* in view of *Dua* discloses or renders obvious that a biometric sensor can be used to enable financial transactions. §§ VII.C.ii.1[e], VII.C.iii (Claim 2). *Waters* states that “the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to

the reader. After successful reading of the RF tag **41**, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered.” EX1024, [0052]. *Waters* explains that in the disabled state, “a reader is not able to obtain any information from the near field tag 41” but when enabled, the tag “is then able to communicate with readers to allow use of” financial services. *Id.*, [0037], [0042]. This biometric authentication scheme is also disclosed by *Dua*, where the fingerprint sensor is used to “authenticate a user to the wallet application,” and the processing and control circuitry executing that wallet application approves the transaction. *See* § VII.A.ii (Claim 3).

As identified in § VII.C.ii, the “circuit” is the processing and control circuitry that executes the wallet application of *Dua* and controls the embedded RF interface. EX1014, ¶¶484-85. That circuitry is configured to approve the financial transaction responsive to the biometric sensor based on the functionality of the wallet application it executes. EX1014, ¶¶484-85. Thus, by making the wallet application’s user authentication and financial transaction approval responsive to a fingerprint sensor, the combination of *Waters* in view of *Dua* renders obvious Claim 3.

5[Pre].

Waters in view of *Dua* renders obvious every element of Claim 1. *See* § VII.C.ii.

5[a].

Dua discloses Limitation 5[a] for the reasons discussed above in § VII.A.ii (Limitation 5[a]). Specifically, *Dua* explains that its circuit—the processing and control circuitry executing the wallet application and controlling the embedded RF interface—can operate in multiple ON states (*e.g.*, PIN-less, authenticated) that differ in whether authentication is required and in which credentials can be transmitted. EX1014, ¶487; § VII.A.ii (Claim 5). A POSITA would have understood that the circuit is changed from the first ON state to the second ON state responsive to an electronic switch (*see* § VII.A.i.1[c]) because correct entry of the user’s fingerprint activates the electronic switch, which makes or breaks an electrical connection in the processing and control circuitry and thereby transitions the circuit from the PIN-less state to the authenticated state in which PIN-protected credentials can be transmitted. EX1014, ¶487; EX1023, [0366], [0368], [0384].

Waters states that “the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader.” EX1024, [0052]. It would have been obvious to a POSITA incorporating the wallet application of *Dua* into the mobile terminal of *Waters* to include multiple ON states (*e.g.*, PIN-less state, authenticated state) responsive to an electronic switch that makes or breaks an electrical connection in the circuit in response to correct PIN or

biometric entry. EX1014, ¶487. Thus, *Waters* in view of *Dua* renders obvious Limitation 5[a]. EX1014, ¶487.

5[b].

As discussed above in Grounds 1-2, a POSITA would have understood that, to enable implementation of the software-based logic described above (transitioning from a first ON state to a second ON state), it would have been necessary for the circuit to store the alternative ON states in memory. § VII.A.ii (Limitation 5[b]). Alternatively, it would have been obvious to store the state in memory, as software/firmware execution was known to store data in memory, including state memory or registers, in order to take different execution action based on the content of that data. *Id.* Thus, *Waters* in view of *Dua* renders obvious Limitation 5[b]. EX1014, ¶488.

Accordingly, *Waters* in view of *Dua* renders obvious each element of Claim 5. EX1014, ¶¶486-88.

6[Pre].

Waters in view of *Dua* renders obvious every element of Claim 1. See § VII.C.ii.

6[a].

Waters in view of *Dua* renders obvious Limitation 6[a] for the reasons discussed above in § VII.C.iii (Limitation 5[a]).

6[b].

Waters in view of *Dua* renders obvious Limitation 6[b] for the reasons discussed above. *See* § VII.A.ii (Limitation 6[b]).

Accordingly, *Waters* in view of *Dua* renders obvious each element of Claim 6. EX1014, ¶¶489-91.

Claim 7.

Waters in view of *Dua* renders obvious Claim 7 for the same reasons discussed above in Grounds 1-2. *See* § VII.A.ii (Claim 7).

Claim 8: The method of claim 1, wherein the circuit is configured for a user to select between a plurality of financial accounts for the financial transaction.

The mobile terminal of *Waters* incorporating the wallet application of *Dua* renders obvious Claim 8 for the same reasons discussed above in Grounds 1-2. *See* § VII.A.ii (Claim 8). Specifically, the processing and control circuitry that executes the wallet application (*i.e.*, the circuit) provides a “Credential Selector” for the user to select from multiple payment credentials once the user is authenticated by the biometric sensor of *Waters*. EX1023, [0371], [0378]. That circuitry is configured for a user to select between a plurality of financial accounts for the financial transaction based on the functionality of the wallet application it executes. EX1014, ¶493. Thus, *Waters* in view of *Dua* renders obvious claim 8.

Claim 9.

Waters in view of *Dua* renders obvious Claim 9 for the same reasons discussed above in Grounds 1-2. *See* § VII.A.ii (Claim 9).

Claim 10.

Waters in view of *Dua* renders obvious Claim 10 for the same reasons discussed above in Grounds 1-2. *See* § VII.A.ii (Claim 10).

Claim 11.

Waters in view of *Dua* renders obvious Claim 11 for the same reasons discussed above in Grounds 1-2. *See* § VII.A.ii (Claim 11).

12[Pre]-[b].

As discussed above in § VII.C.ii.1[e], *Waters* in view of *Dua* renders obvious the use of a biometric authentication mechanism to facilitate a financial transaction. *Waters* describes that “the keypad **37** of the mobile terminal **1** is used to enter a PIN (or other secret password) to enable the near field tag **41**. . . . If the PINs match, the SIM transmits a message, via link **43**, to the near field tag **41** to activate the near field tag.” EX1024, [0051]. *Dua* also describes that, separate from wallet application authentication, “[c]ertain credential issuers such as financial institutions may require that users validate their identity during a transaction by providing a PIN that was established with or set by the financial institution.” EX1023, [0397].

Along with strict biometric authentication, both references also teach dual-authentication schemes. EX1014, ¶¶497-501. *Waters* explains that its activation

arrangements can be used in any combination and “may work in series,” such that the tag is enabled only after more than one arrangement has been satisfied. EX1024, [0056]. *Dua* likewise describes a dual-authentication scheme using biometric entry and an issuer PIN, which it would have been obvious to a POSITA to implement fully on its mobile device running its wallet application. EX1014, ¶¶497-501; *see* VII.A.ii (Limitations 12[a]-[b]).

Waters describes dual-authentication using both a biometric sensor and PIN-entry in series, which is consistent with *Dua*’s biometric/issuer PIN scheme. EX1024, [0056]. It would also have been obvious to a POSITA to implement the same dual-authentication scheme discussed in § VII.A.ii (Limitations 12[a]-[b]) in the device of *Waters* incorporating the wallet application of *Dua*. Thus, *Waters* in view of *Dua* renders obvious Limitations 12[a]-[b].

Accordingly, *Waters* in view of *Dua* renders obvious each element of Claim 12. EX1014, ¶¶497-501.

Claim 13.

Waters in view of *Dua* renders obvious Claim 13 for the same reasons discussed above in Grounds 1-2. *See* § VII.A.ii (Claim 13).

14[Pre].

Waters in view of *Dua* renders obvious every element of Claim 1. *See* § VII.C.ii.

14[a].

Waters's "mobile terminals **1**, **11** and **13** is provided with a respective smart card or subscriber identity module (SIM) **15**." EX1024, [0023]. A SIM card is a separate component that is mechanically inserted into a device such as a cellular telephone and includes an electronic key (*i.e.*, a PIN). EX1014, ¶504; *see infra* § VII.C.iii (Limitation 14[b]). Thus, *Waters* in view of *Dua* renders obvious Limitation 14[a].

14[b].

Waters explains that "[t]he user's PIN may be stored in a secure location in the mobile terminal **1** or in the SIM **15**." EX1024, [0051]. Thus, *Waters* in view of *Dua* renders obvious Limitation 14[b].

14[c].

Waters describes that "the keypad **37** of the mobile terminal **1** is used to enter a PIN (or other secret password) to enable the near field tag **41**. . . . If the PINs match, the SIM transmits a message, via link **43**, to the near field tag **41** to activate the near field tag." EX1024, [0051]. *Waters* further explains that its activation arrangements can be used in any combination (*e.g.*, PIN entry and biometric entry). *Id.*, [0056]. *Waters* describes that "the arrangements may work in series—for example, the near field tag **41** would be enabled if the light sensor was activated and the correct PIN was subsequently entered." *Id.* *Dua* also discloses Limitation 14[c] for the reasons discussed above in § VII.A.iii.19[e].

Accordingly, *Waters* in view of *Dua* renders obvious each element of Claim 14. EX1014, ¶¶503-06.

Claim 15.

Waters in view of *Dua* renders obvious Claim 15 for the same reasons discussed above in Grounds 1-2. *See* § VII.A.ii (Claim 15).

Claim 16.

Waters in view of *Dua* renders obvious every element of Claim 1. *See* § VII.C.ii. *Waters* in view of *Dua* also renders obvious that the electronic switch is responsive to a biometric sensor. *See* § VII.C.ii.1[e]. *Waters* further states that “[t]he pressure sensor may be combined with the fingerprint scanner **45**. The combined sensor detects, not only that pressure is applied, but also that an authorised person is pressing the sensor.” EX1024, [0053]. *Waters* also explains that the fingerprint reader “scans the fingerprint of the user when the user’s finger is placed on the reader **45** and compares it to the user’s fingerprint stored in the memory of the mobile terminal **1** or the SIM **15**.” *Id.*, [0051]; *see also id.*, [0068], FIG. 5 (“[t]he print is ideally compared to a previously taken print stored in the memory **130** of the smart card **100**”). Thus, *Waters* in view of *Dua* renders obvious Claim 16.

Claim 17.

Waters in view of *Dua* renders obvious Claim 17 for the same reasons discussed above in § VII.C.iii (Claim 10).

18[Pre].

Waters in view of *Dua* renders obvious every element of Claim 1. *See* § VII.C.ii.

18[a]-[b].

Waters in view of *Dua* renders obvious Limitations 18[a]-[b] for the same reasons discussed above. *See* § VII.C.iii (Claims 11 and 8, respectively).

18[c].

Waters in view of *Dua* renders obvious Limitation 18[c] for the same reasons discussed above in Grounds 1-2. *See* § VII.A.ii (Limitation 18[c]).

18[d]: and wherein the step of communicating financial account information includes communicating financial account information corresponding to the selected specific member of the plurality of financial accounts.

Waters in view of *Dua* renders obvious Limitation 18[d] for the same reasons discussed above in Grounds 1-2. *See* § VII.A.ii (Limitation 18[d]).

Accordingly, *Waters* in view of *Dua* renders obvious each element of Claim 18. EX1014, ¶¶510-15.

iv. Independent Claim 19

19[Pre]-[b].

Waters in view of *Dua* renders obvious limitations 19[Pre]-[b] for the reasons discussed above in § VII.C.ii.1[Pre]-[b].

19[c]-[d].

Limitations 19[c]-[d] are substantively identical to Limitations 1[c]-[d] except that Limitations 19[c]-[d] require that “the RF antenna” (rather than “communication by the cellular telephone” as recited in Limitations 1[c]-[d]) is “responsive to the state of the circuit.” As discussed above in § VII.A.i.1[b], “communication by the cellular telephone” in the *Waters-Dua* combination occurs using an RF antenna. Thus, *Waters* in view of *Dua* renders obvious limitations 19[c]-[d] for the reasons discussed above in § VII.C.ii.1[c]-[d].

19[e].

Waters describes that “the keypad **37** of the mobile terminal **1** is used to enter a PIN (or other secret password) to enable the near field tag **41**. . . . If the PINs match, the SIM transmits a message, via link **43**, to the near field tag **41** to activate the near field tag.” EX1024, [0051]. *Dua* also explains that “[p]ressing buttons 1 or 2, may prompt the user to input a PIN before RF communication can be enabled. As such, a user may be required to input a PIN and click ‘OK’ to enable RF communication for a 30 second window.” EX1023, [0395].

A POSITA would have understood that this PIN-based authentication mechanism necessarily discloses the same electronic switch identified in § VII.C.ii.1[c], which, in response to a correct PIN entry, makes or breaks an electrical connection in the processing and control circuitry that executes the wallet

application and controls the embedded RF interface (*i.e.*, the circuit). EX1014, ¶¶521-22. A POSITA would further understand that the making or breaking of that electrical connection changes the state of the circuit from the PIN-less state, in which only PIN-less credentials can be transmitted, to the authenticated state, in which PIN protected credentials can be transmitted. EX1014, ¶¶521-22; § VII.C.ii.1[e]. Thus, *Waters* in view of *Dua* renders obvious Limitation 19[e].

19[f].

Waters in view of *Dua* renders Limitation 19[f] obvious for the reasons discussed above in § VII.C.ii.1[f].

Accordingly, *Waters* in view of *Dua* renders obvious each element of independent Claim 19. EX1014, ¶¶516-524.

v. Dependent Claims 20-30

Claim 20.

Waters in view of *Dua* renders obvious every element of Claim 19. *See* § VII.C.iv. As discussed above in § VII.C.iii (Limitation 12[b]), *Waters* in view of *Dua* renders obvious a dual-authentication scheme using both PIN-entry (*e.g.*, as recited in Claim 19) and a biometric sensor (*e.g.*, as recited in Claim 20). *Waters* further describes that its “pressure sensor may be combined with the fingerprint scanner 45. The combined sensor detects, not only that pressure is applied, but also that an authorised person is pressing the sensor.” EX1024, [0053]. *Waters* further explains that its activation arrangements can be used in any combination (*e.g.*, PIN

entry and biometric entry). *Id.*, [0056]. *Waters* describes that “the arrangements may work in series—for example, the near field tag **41** would be enabled if the light sensor was activated and the correct PIN was subsequently entered.” *Id.* Thus, because *Waters* describes an activation scheme responsive to both a pressure sensor (*i.e.*, a mechanical switch) and a fingerprint scanner (*i.e.*, a biometric sensor), and *Dua* describes subsequent entry of an issuer PIN (*see* § VII.C.iii (Limitation 12[b])), *Waters* in view of *Dua* renders obvious Claim 20. EX1014, ¶525.

Claim 21.

Waters in view of *Dua* renders obvious every element of Claim 19. *See* § VII.C.iv. *Dua* also discloses Claim 21. *See* § VII.A.iv (Claim 21). *Waters* further explains that biometric data entered at the fingerprint scanner **45** is used to enable the near field tag **41**, such that no transaction is approved unless the biometric sensor confirms an authorized user. EX1024, [0050]–[0051]. Thus, *Waters* in view of *Dua* renders obvious Claim 21.

Claim 22.

Waters in view of *Dua* renders obvious every element of Claim 19. *See* § VII.C.iv. *Dua* also discloses Claim 22. *See* § VII.A.iv (Claim 22). Thus, *Waters* in view of *Dua* renders obvious Claim 22.

23[Pre].

Waters in view of *Dua* renders obvious every element of Claim 22. *See* § VII.C.v (Claim 22).

23[a].

Dua discloses Limitation 23[a] for the reasons discussed above in § VII.A.iv (Limitation 23[a]). Thus, *Waters* in view of *Dua* renders obvious Limitation 23[a].

23[b].

Waters in view of *Dua* renders obvious Limitation 23[b] for the same reasons discussed above in § VII.C.iii (Claim 8).

Accordingly, *Waters* in view of *Dua* renders obvious each element of Claim 23. EX1014, ¶¶528-31.

Claim 24.

Waters in view of *Dua* renders obvious every element of Claim 19. *See* § VII.C.iv. *Dua* also discloses Claim 24. *See* § VII.A.iv (Claim 24). Thus, *Waters* in view of *Dua* renders obvious Claim 24.

25[Pre].

Waters in view of *Dua* renders obvious every element of Claim 19. *See* § VII.C.iv.

25[a].

Waters in view of *Dua* renders obvious Limitation 25[a] for the reasons discussed above in § VII.C.iii (Limitation 5[a]).

To the extent that “RF antenna” refers to an antenna for RF communications via a cellular network, *Waters* in view of *Dua* renders obvious this limitation. EX1014, ¶¶534-35. In this context of RF communications via a cellular network, a

POSITA would have understood that the circuit of the mobile terminal of *Waters* incorporating the wallet application of *Dua* (*i.e.*, the processing and control circuitry executing the wallet application and controlling the embedded RF interface) is in a first ON state when the mobile terminal is powered on (*i.e.*, the mobile terminal has service and can communicate with the cellular network). EX1014, ¶¶534-35. A POSITA would further understand that circuit is in a second ON state when the near field tag **41** is enabled to communicate with a reader. EX1014, ¶¶534-35. Thus, *Waters* in view of *Dua* renders obvious Limitation 25[a].

25[b].

Waters in view of *Dua* renders obvious Limitation 25[b] for the reasons discussed above in § VII.C.iii (Limitation 6[b]). To the extent that “RF antenna” refers to an antenna for RF communications via a cellular network, *Waters* in view of *Dua* renders obvious this limitation. EX1014, ¶¶536-37. A POSITA would understand that in the first ON state (*i.e.*, mobile terminal is powered on), the circuit of the mobile terminal can communicate personal information using the cellular network. EX1014, ¶¶536-37. A POSITA would further understand that in the second ON state (*i.e.*, the near field tag **41** is enabled), the circuit of the mobile terminal can communicate different amounts of personal information (*i.e.*, authentication-protected sensitive payment and personal information). *Id.* Thus, *Waters* in view of *Dua* renders obvious Limitation 25[b].

Accordingly, *Waters* in view of *Dua* renders obvious each element of Claim 25. EX1014, ¶¶533-38.

Claim 26.

Waters in view of *Dua* renders obvious Claim 26 for the reasons discussed above in § VII.C.iii (Claim 7).

Claim 27.

Waters in view of *Dua* renders obvious Claim 27 for the reasons discussed above in § VII.C.iii (Claim 10).

Claim 28.

Waters in view of *Dua* renders obvious every element of Claim 19. *See* § VII.C.iv. *Dua* also discloses Claim 28. *See* § VII.A.iv (Claim 28). *Waters* also states that “[t]he user's PIN may be stored in a secure location in the mobile terminal **1** or in the SIM **15**.” EX1024, [0051]. Thus, *Waters* in view of *Dua* renders obvious Claim 28.

29[Pre].

Waters in view of *Dua* renders obvious every element of Claim 19. *See* § VII.C.iv.

29[a]: wherein the cellular telephone is configured for insertion of an electronic key,

29[b]: the electronic key being configured to store the personal identification number,

29[c]: the communication via the RF antenna being responsive to the personal identification number.

Waters in view of *Dua* renders obvious Limitations 29[a]-[c] for the reasons discussed above in § VII.C.iii (Limitations 14[a]-[c]).

Accordingly, *Waters* in view of *Dua* renders obvious each element of Claim 29. EX1014, ¶¶542-44.

Claim 30.

Waters in view of *Dua* renders obvious every element of Claim 19. *See* § VII.C.iv. *Dua* also discloses, or at least renders obvious, Claim 30. *See* § VII.A.iv (Claim 30). Thus, *Waters* in view of *Dua* renders obvious Claim 30.

VIII. CONCLUSION

For the foregoing reasons, Petitioners respectfully request that the Board institute *inter partes* review and cancel Claims 1-30 of the '741 Patent as unpatentable.

Dated: September 22, 2026

Respectfully submitted,

/ Eliot D. Williams /

Eliot D. Williams, Reg. No. 50,822

eliot.williams@bakerbotts.com

Baker Botts L.L.P.

700 K Street, N.W.

Washington, D.C. 20001-5692

Phone: 202.639.1334

Fax: 202.639.7890

Neil Sirota, Reg. No. 38,306

Baker Botts L.L.P.

30 Rockefeller Plaza, Ste 4340

New York, NY 10112-4498

Phone: 212.408.2548

Fax: 212.259.2548

neil.sirota@bakerbotts.com

Megan LaDriere White, Reg. No. 75,995

Baker Botts L.L.P.

2001 Ross Avenue

Suite 900

Dallas, Texas 75201-2980

Phone: 214.953.6948

megan.white@bakerbotts.com

Eric Faragi, Reg. No. 51,259

Baker Botts L.L.P.

30 Rockefeller Plaza, Ste 4340

New York, NY 10112-4498

Phone: 212.408.2591

eric.faragi@bakerbotts.com

Benjamin Rosen, Reg. No. 84,598

Baker Botts L.L.P.

30 Rockefeller Plaza, Ste 4340

New York, NY 10112-4498

Phone: 212.408.2691

benjamin.rosen@bakerbotts.com

Coleman Strine, Reg. No. 79,981
Baker Botts L.L.P.
30 Rockefeller Plaza, Ste 4340
New York, NY 10112-4498
Phone: 212.408.2595
coleman.strine@bakerbotts.com

CERTIFICATION UNDER 37 C.F.R. §42.24(d)

Pursuant to 37 C.F.R. §42.24(d), the undersigned hereby certifies that the word count under §42.24(a)(1) for the foregoing Petition for *Inter Partes* Review totals 13,867 words, within the 14,000 word limit allowed under §42.24(a)(1)(i).

Dated: September 22, 2026

/ Eliot D. Williams /
Eliot D. Williams

CERTIFICATE OF SERVICE

In accordance with 37 C.F.R. §§42.6(e) and 42.105, the undersigned certifies that, on this date, the foregoing was served via FedEx Overnight Delivery on the Patent Owner at the correspondence addresses of record (as listed in Patent Center and on the Patent Assignment Cover Sheet) for the subject patent at:

Patent Center	Patent Assignment Cover Sheet
Steven Colby Rimon Law, P.C. 1655 W. Fairview Ave., Suite 102 Boise, Idaho 83702	SureCell Transactions, LLC P.O. Box 837 Verdi, Nevada 89439

A complete copy was also served via electronic mail to counsel of record for Patent Owner in the litigation pending before the U.S. District Court for the Eastern District of Texas entitled *SureCell Transactions LLC v. Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.*, No. 2:26-cv-00106 at:

sdavis@stafforddavisfirm.com
cbartles@stafforddavisfirm.com

Dated: September 22, 2026

/ Eliot D. Williams /
Eliot D. Williams