

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. IPR2026-00507
U.S. Patent No. 11,347,949

**PETITION FOR INTER PARTES REVIEW OF
U.S. PATENT NO. 11,347,949**

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.	'949 PATENT.....	2
	A. SPECIFICATION	2
	B. FILE HISTORY	2
IV.	LEVEL OF ORDINARY SKILL IN THE ART.....	5
V.	CLAIM CONSTRUCTION	5
	A. TERMS CONSTRUED IN <i>MYNETTE</i>	5
	B. “MECHANICAL SWITCH”	6
VI.	SUMMARY OF PRIOR ART.....	8
	A. <i>DUA</i> (EX1023).....	8
	B. <i>WATERS</i> (EX1024).....	10
	C. <i>WOIKE</i> (EX1025) (SECONDARY REFERENCE).....	11
VII.	INVALIDITY	12
	A. GROUNDS 1-2: <i>DUA</i> ANTICIPATES AND/OR RENDERS OBVIOUS CLAIMS 1–23 AND 26–30	12
	i. Independent Claim 1	12
	ii. Dependent Claims 2–23 and 26–28	15
	iii. Independent Claim 29	32
	iv. Independent Claim 30	33
	B. GROUND 3: <i>DUA</i> IN VIEW OF <i>WOIKE</i> RENDERS OBVIOUS CLAIMS 24 AND 25	34
	i. Motivation to Combine	34
	ii. Claims 24 and 25.....	35
	C. GROUND 4: <i>WATERS</i> IN VIEW OF <i>DUA</i> RENDERS OBVIOUS CLAIMS 1-30.....	37

i.	Motivation to Combine	37
ii.	Independent Claim 1	38
iii.	Dependent Claims 2–28	41
iv.	Independent Claim 29	56
v.	Independent Claim 30	57
VIII.	CONCLUSION	57

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. 11,347,949 (“’949 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]	An electronic communication system comprising:
1[a]	a cellular telephone configured to communicate wirelessly using an inductive coupling,
1[b]	wherein the inductive coupling is part of a circuit including an electronic switch configured to change between states of the circuit and
1[c]	configured to communicate via the inductive coupling responsive to the states of the circuit.

Claim 2:

2	The system of claim 1, wherein the circuit includes a switchable RFID tag, input logic, processing logic, a return signal generator, switch logic, a switch state monitor, encryption logic, one or more antenna, memory or a power supply.
----------	---

Claim 3:

3	The system of claim 2, wherein the memory is configured to store a financial account balance.
----------	---

Claim 4:

4	The system of claim 2, wherein the cellular telephone further includes a user interface configured to enter a financial account number and the memory is configured to store the financial account number for use in the financial transaction.
----------	---

Claim 5:

5	The system of claim 1, wherein the circuit is configured to facilitate a financial transaction responsive to the states of the circuit via the inductive coupling.
----------	--

Claim 6:

6	The system of claim 5, wherein the electronic switch is configured for a user to select between a plurality of financial accounts for the financial transaction.
----------	--

Claim 7:

7	The system of claim 5, further including a user interface configured to approve the financial transaction via the electronic switch.
----------	--

Claim 8:

8	The system of claim 5, wherein the cellular telephone includes a biometric sensor and the circuit is configured to facilitate the financial transaction responsive to the biometric sensor.
----------	---

Claim 9:

9	The system of claim 5, wherein the circuit is configured to communicate an account number via the inductive coupling to facilitate the financial transaction.
----------	---

Claim 10:

10	The system of claim 5, further comprising an input configured for a user to enter a personal identification number, wherein the financial transaction is responsive to entry of the personal identification number and a signal communicated via the inductive coupling is responsive to the personal identification number.
-----------	--

Claim 11:

11	The system of claim 5, further comprising a key memory configured to store an encryption key used to facilitate the financial transaction.
-----------	--

Claim 12:

12	The system of claim 5, further comprising a key memory configured to store a key required to change the states of the circuit to facilitate the financial transaction via the inductive coupling.
----	---

Claim 13:

13	The system of claim 5, further comprising a mechanical switch configured to approve the financial transaction.
----	--

Claim 14:

14	The system of claim 5, further comprising a reader configured to read a signal generated by the inductive coupling of the cellular telephone to perform the financial transaction.
----	--

Claim 15:

15	The system of claim 14, further comprising a point of sale device including the reader.
----	---

Claim 16:

16	The system of claim 1, wherein the circuit is configured to operate in at least a first ON state and a second ON state of the states, responsive to the electronic switch.
----	--

Claim 17:

17	The system of claim 16, wherein the circuit is configured to facilitate a financial transaction in the first ON state but not in the second ON state.
----	---

Claim 18:

18	The system of claim 1, wherein the circuit includes a state memory configured to store the states of the circuit.
----	---

Claim 19:

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

Claim 20:

20	The system of claim 1, wherein the electronic switch is responsive to a biometric sensor.
-----------	---

Claim 21:

21	The system of claim 1, further comprising an input configured for a user to enter a personal identification number (PIN), communication via the inductive coupling being responsive to the personal identification number.
-----------	--

Claim 22:

22	The system of claim 1, wherein the cellular telephone further includes an antenna configured to communicate using WiFi, the antenna being configured to operate at a different frequency than the inductive coupling.
-----------	---

Claim 23:

23	The system of claim 1, wherein the inductive coupling is part of a radio frequency identification device.
-----------	---

Claim 24:

24	The system of claim 1, further comprising an electronic key configured to be inserted into the cellular telephone, the electronic key including an account identifier and a signal communicated via the inductive coupling being responsive to the account identifier.
-----------	--

Claim 25:

25	The system of claim 24, wherein the electronic key is configured to store a password.
-----------	---

Claim 26:

26	The system of claim 1, wherein the circuit includes both the electronic switch and a mechanical switch configured to approve a financial transaction.
-----------	---

Claim 27:

27	The system of claim 1, wherein the cellular phone is configured to purchase goods by placing the circuit within the reading range of a wireless point of sale device and communicating a financial account number to the wireless point of sale device using the induction coupling responsive to the states of the circuit.
-----------	--

Claim 28:

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

Claim 29:

29[pre]	A cellular telephone configured to communicate wirelessly using an inductive coupling and also configured to communicate using WiFi,
29[a]	wherein the inductive coupling is part of a circuit configured to facilitate a financial transaction communicated via the inductive coupling,
29[b]	the circuit being configured to facilitate the financial transaction responsive to a biometric sensor.

Claim 30:

30[pre]	A cellular telephone configured to communicate wirelessly using an inductive coupling and also configured to communicate using WiFi,
30[a]	wherein the inductive coupling is part of a circuit configured to facilitate a financial transaction communicated via the inductive coupling,
30[b]	the circuit being configured to facilitate the financial transaction being responsive to a personal identification number entered by a user.

I. INTRODUCTION

The Office materially erred in granting U.S. Patent No. 11,347,949 (“the ’949 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 ’949 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 ’949 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 1–23, 26–30
Ground 2	<i>Dua</i> renders obvious claims 1–23, 26–30
Ground 3	<i>Dua</i> with <i>Woike</i> renders obvious claims 24–25
Ground 4	<i>Waters</i> with <i>Dua</i> renders obvious claims 1–30

III. '949 PATENT

A. SPECIFICATION

The '949 Patent relates to an electronic communication system capable of communicating via an inductive coupling. EX1002, 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.*, 9:54–55. 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.*, 10:3–8.

B. FILE HISTORY

The '949 Patent was filed as App. No. 17/522,697 (the “'697 Application”) on November 9, 2021, and on its face, purports to claim priority to a provisional application filed on May 6, 2005. EX1002, Cover. In a Preliminary Amendment dated December 3, 2021, Applicant added certain claims and made amendments throughout. EX1008, 305–08. Independent claims 1, 29, and 30 recited:

1. (Currently Amended) An electronic communication system comprising:

a cellular telephone configured to communicate wirelessly using an inductive ~~antenna coupling~~
~~and also configured to communicate wirelessly using a cellular transmitter~~, wherein the
inductive ~~antenna coupling~~ is part of a circuit including an electronic switch configured
to change between states ~~of the circuit and configured to communicate via the~~
~~inductive coupling responsive to the states of the circuit.~~

Id., 305.

29. (New) A cellular telephone configured to communicate wirelessly using an inductive coupling and also configured to communicate using WiFi, wherein the inductive coupling is part of a circuit configured to facilitate a financial transaction communicated via the inductive coupling, the circuit being configured to facilitate the financial transaction responsive to a biometric sensor.

30. (New) A cellular telephone configured to communicate wirelessly using an inductive coupling and also configured to communicate using WiFi, wherein the inductive coupling is part of a circuit configured to facilitate a financial transaction communicated via the inductive coupling, the circuit being configured to facilitate the financial transaction being responsive to a personal identification number entered by a user.

Id., 308.

In a first Non-Final Office Action dated March 3, 2022, the Examiner rejected all pending claims 1–30 under pre-AIA 35 U.S.C. §102(b) as being anticipated by U.S. Patent Publication No. 2007/0257767 (“Beeson”). *Id.*, 76–82.

Later that same day, Applicant filed a Response to Non-Final Office Action, alleging that Beeson is not valid prior art, because the disclosures relied upon by the Examiner were not entitled to a priority date earlier than the priority date of the ’697

Application. *Id.*, 73. Together therewith, Applicant submitted an Amendment to correct a typographical error in claim 2. *Id.*, 70–72.

In a second Non-Final Office Action dated April 5, 2022, the Examiner rejected pending claim 8 under 35 U.S.C. §112(b) or pre-AIA 35 U.S.C. §112 as being indefinite, based on the limitation reciting “wherein the circuit is configured to store transaction logs.” *Id.*, 47. Specifically, the Examiner noted that the claim did “not set forth a clear understanding of how a circuit in itself is configured to store transaction logs. Is a component of the circuit configured to store transaction logs?” *Id.*, 47. Additionally, pending claims 1–3, 6–18, 20, and 23–30 were rejected under pre-AIA 35 U.S.C. §102(b) as being anticipated by U.S. Patent Publication No. 2017/0357961 (“Bidari”). *Id.*, 48–51. Further, the Examiner indicated that pending claims 4, 19, 21, and 22 would be allowable if rewritten in independent form. *Id.*, 51.

Later that same day, Applicant filed a Response to Non-Final Office Action, alleging that claim 8 is not indefinite, because “storage of digital data is well known in the art, for example in the memory circuits taught in the specification of the current application. The storage of particular data may include memory sizes, data structures, file structures, etc.....[I]mplementation of a circuit to store transaction logs would be well understood by one [of] ordinary skill in the art.” *Id.*, 65. Additionally, Applicant alleged that Bidari is not valid prior art, because the

disclosures relied upon by the Examiner were not entitled to a priority date earlier than the priority date of the '697 Application. *Id.*

On April 14, 2022, the Office issued a Notice of Allowance for all pending claims 1–30. *Id.*, 30–32.

IV. LEVEL OF ORDINARY SKILL IN THE ART

A Person of Ordinary Skill in the Art (“POSITA”) at the time of the '949 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. TERMS CONSTRUED IN *MYNETTE*

The following terms, which Petitioners identify for construction, were construed in prior litigation involving U.S. Patent No. 7,924,156, which is related to the '949 Patent and is also asserted in *SureCell Transactions LLC v. Samsung Electronics Co., Ltd.*, No. 2:26-cv-00106 (E.D. Tex.):

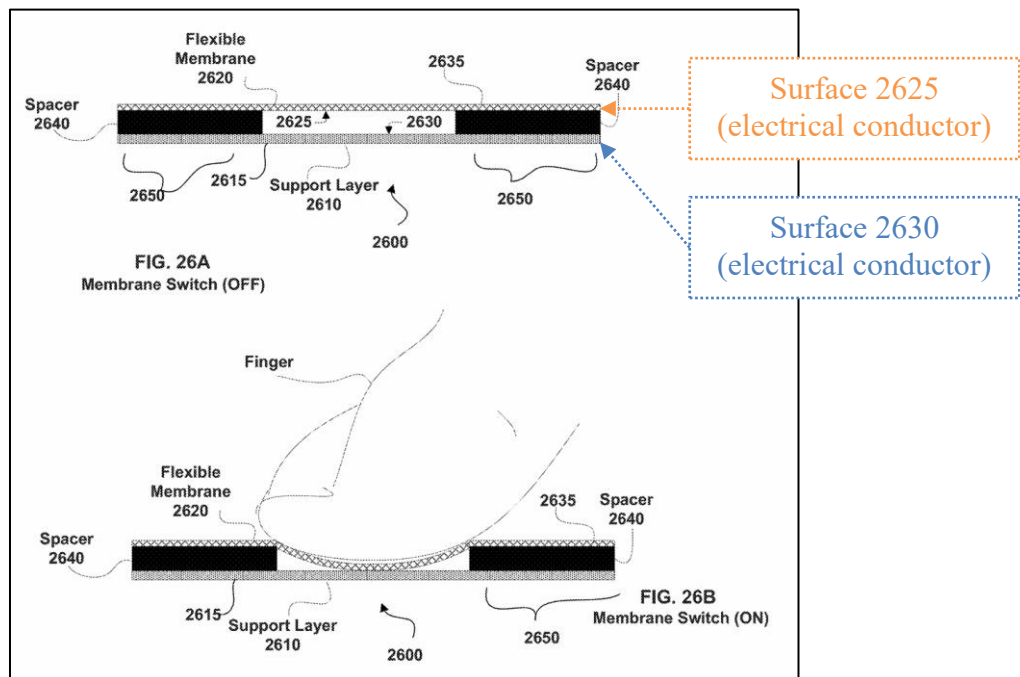
Term	Proposed Construction
RFID tag	Radio Frequency Identification Tag
State memory	Volatile memory, non-volatile memory, FLASH, SDRAM, ROM, or DRAM which stores/holds the status of an RFID Tag
Key memory	Volatile memory, non-volatile memory, FLASH, SDRAM, ROM, or DRAM which stores/holds a key of an RFID Tag
Responsive	Plain and ordinary meaning
Switch	A control device that makes or breaks an electrical connection in a circuit
Switch logic	Circuitry and set or sets of logic instructions directing the operation of a RFID tag

EX1022, 15, 41.

B. “MECHANICAL SWITCH”

Petitioners further identify the term “mechanical switch” for construction. A POSITA would have understood “mechanical switch” to mean “a control device that makes or breaks an electrical connection in a circuit responsive to movement of one or more components of the control device.” EX1014, ¶¶61-64. The specification describes that a mechanical switch “is optionally a sliding switch, a flip switch, a rotating switch, membrane switch, pushbutton switch, or other mechanical switch.” EX1002, 25:20–23. The specification further describes that in some embodiments,

the switch “is a mechanical contact switch activated by applying pressure to an outside surface of Switchable RFID Device 2200.” *Id.*, 25:28–31. Further, the switch can be “configured to be moved between the on position and the off position, for example using a finger.” *Id.*, 26:38–40. As illustrated in Figures 26A–B (showing a membrane switch, which is a type of mechanical switch), the switch makes or breaks an electrical connection responsive to movement of the switch components. *Id.*, 25:20–23 (listing “membrane switch” among types of mechanical switches), 26:59–61 (when the membrane switch is pressed by a user, “electrical conductors on a Surface 2630 and a Surface 2625 [are brought] together” and “a switchable RFID tag is controlled, activated or deactivated”); EX1014, ¶¶61-64.



EX1002, FIGs. 26A–B.

VI. SUMMARY OF PRIOR ART

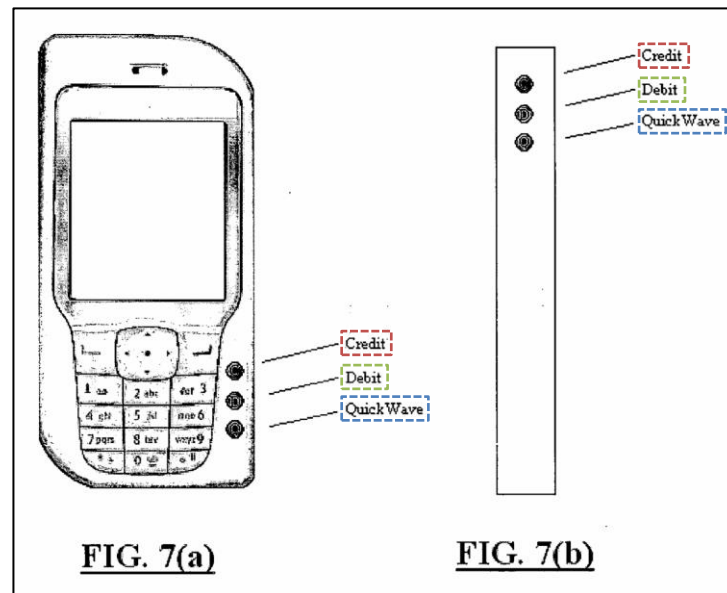
Petitioners assume, without conceding, that claims 1-30 of the '949 Patent ("Challenged Claims") are entitled to a May 6, 2005 priority date and are subject to pre-AIA provisions.

A. *DUA* (EX1023)

U.S. Patent Publication No. 2006/0165060 ("*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 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].



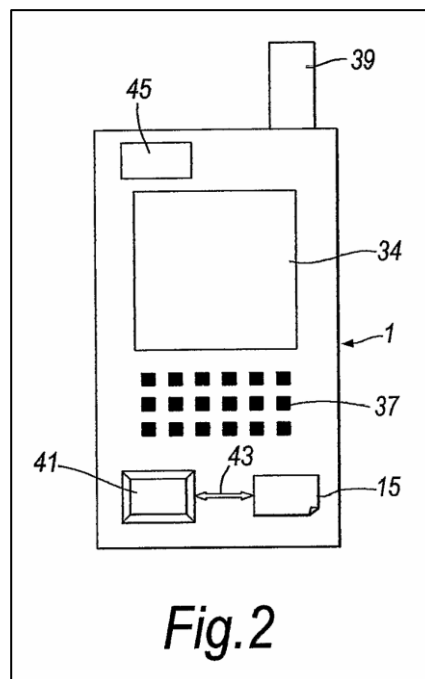
EX1023, FIG. 7.

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(b).

VII. INVALIDITY

A. **GROUND 1-2: *DUA* ANTICIPATES AND/OR RENDERS OBVIOUS CLAIMS 1–23 AND 26–30**

i. **Independent Claim 1**

1[pre]: An electronic communication system

Dua describes a “mobile device” (an electronic communication system) “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).” EX1023, [0315].

Thus, *Dua* discloses 1[pre].

1[a]: a cellular telephone configured to communicate wirelessly using an inductive coupling

A POSITA would understand that *Dua*’s “mobile telephone” is a cellular telephone. EX1014, ¶¶75-77. Indeed, *Dua*’s mobile telephone is “capable of wirelessly connecting to the Internet using network protocols such as GSM/GPRS, CDMA2000, W-CDMA, EDGE, HDR, 1xRTT, UMTS, [and] IMT-2000.” EX1023, [0026], [0041]. Each of these protocols are cellular communication protocols. EX1014, ¶¶75-77. Thus, *Dua*’s device is a cellular telephone. *Id.*

Dua discloses that its device is a “wireless device,” which includes an RFID interface configured to carry out transactions using wireless RFID communication. EX1023, Abstract, [0041], [0378]. *Dua* also explains that ISO/IEC 14443, which describes the use of inductive coupling antennas to facilitate wireless RFID

communication, was known in the art. *Id.*, [0013]; EX1014, ¶¶75-77. While *Dua* does not expressly use the term “inductive coupling,” *Dua*’s disclosure of RFID technology renders inherent or obvious an inductive coupling for wireless communication, because RFID technology uses an RFID antenna (using inductive coupling) to enable the RFID communication *Dua* describes. EX1014, ¶¶75-77; *see* EX1031, 7-10.

Thus, *Dua* inherently discloses, or otherwise renders obvious, 1[a].

1[b]: wherein the inductive coupling is part of a circuit including an electronic switch configured to change between states of the circuit

Dua explains that its “wallet application handles...enabling communication with an embedded RF interface.” 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 that executes the wallet application and controls the embedded RF interface. EX1014, ¶¶78-80.

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, ¶¶78-80. 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, ¶¶78-80; 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 1[b].

1[c]: configured to communicate via the inductive coupling responsive to the states of the circuit

As discussed above, *Dua* discloses, or otherwise renders obvious, that its processing and control circuitry executes the wallet application and controls RFID communication (i.e., is configured to communicate) via the inductive coupling. *See supra* §§ VII.A.i.1[a]–[b]; EX1023, [0309]. As further discussed above, such communication is responsive to the states of the circuit, because the circuit can transmit a credential (communicate) in an enabled state, but not in a disabled state. *See supra* § VII.A.i.1[b]; EX1014, ¶¶81-83.

Thus, *Dua* discloses 1[c].

Accordingly, *Dua* discloses or renders obvious each element of independent Claim 1.

ii. **Dependent Claims 2–23 and 26–28**

Claim 2: wherein the circuit includes a switchable RFID tag, input logic, processing logic, a return signal generator, switch logic, a switch state monitor, encryption logic, one or more antenna, memory or a power supply

This limitation is recited in the disjunctive, and *Dua*’s wireless device includes at least memory. *See Brown v. 3M*, 265 F.3d 1349, 1352 (Fed. Cir. 2001) (construing “or” as meaning that the apparatus was capable of meeting only one of the preceding elements or any combination of the preceding elements). For example, *Dua* discloses that the device circuitry enabling the wallet application includes “secure storage capabilities,” which allow it to “host and operate a wallet application capable of receiving, storing, managing and transmitting multiple payment, identification, and other confidential information electronically.” EX1023, [0041].

Further, to the extent that *Dua* does not expressly disclose a switchable RFID tag, input logic, processing logic, a return signal generator, switch logic, a switch state monitor, encryption logic, one or more antenna, or a power supply, it would have been obvious to a POSITA to implement each of these components in the device of *Dua*, because these are necessary to enable the RFID payment functionality described above. EX1014, ¶¶84-86; *see supra* §VII.A.i.

Thus, *Dua* discloses, or otherwise renders obvious, Claim 2.

Claim 3: wherein the memory is configured to store a financial account balance

As discussed above, *Dua*'s memory is configured to "host and operate a wallet application capable of...storing...payment...information electronically." EX1023, [0041]. Specifically, *Dua*'s wallet application stores several types of electronic credentials in the device's memory, including stored value credentials, such as a "Starbucks S-Value" card. EX1023, [0295], [0334], [0345], [0429]. *Dua* explains that when such a stored value credential "is waved in front of a reader at the turnstile, the electronic balance is automatically debited from the onboard chip," and that "an over-the-air reload tool" can be programmed into the wallet application. *Id.*, [0290], [0293]. It would have been obvious to a POSITA to store the value of such credentials in memory, to enable the account debiting and reloading functionality described by *Dua*. EX1014, ¶¶87-88.

Thus, *Dua* renders obvious Claim 3.

Claim 4: wherein the cellular telephone further includes a user interface configured to enter a financial account number and the memory is configured to store the financial account number for use in the financial transaction

Dua's device is equipped with a key pad (a type of user interface) "for alphanumeric and special character input." EX1023, [0041]. *Dua* discloses that the wallet application may request the user to enter "such information as the user's account number with the issuer." *Id.*, [0444]. Additionally, *Dua* discloses that its

device can store and use credit card and debit card numbers, and that the wallet application can request that a user enter a “card account number.” *Id.*, [0180]; *see also id.*, [0019], [0336], [0345], [0392]. Accordingly, a POSITA would have understood that *Dua*’s key pad (user interface) is used to enter a financial account number. EX1014, ¶¶89-91.

Further, as discussed above, *Dua*’s memory is configured to store such “payment...information,” to enable the wallet application and associated circuitry to carry out a financial transaction. EX1023, [0041].

Thus, *Dua* discloses Claim 4.

Claim 5: wherein the circuit is configured to facilitate a financial transaction responsive to the states of the circuit via the inductive coupling

Dua is configured to facilitate financial transactions, because *Dua* explains that the circuitry of its device is configured such 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...information to a reader.” *Id.*, [0313]-[0315]. Such financial transactions are communicated via the inductive coupling when the RFID circuitry is enabled (i.e., responsive to the states of the circuit), for the reasons discussed above with reference to Claim 1. *See* §§ VII.A.i.1[b]-1[c].

Thus, *Dua* discloses Claim 5.

Claim 6: wherein the electronic switch is configured for a user to select between a plurality of financial accounts for the financial transaction

Dua discloses that its wallet application can store multiple payment credentials (financial accounts), including “[c]redit, debit/ATM, stored value, electronic check, and RFID payment methods.” EX1023, [0336]. *Dua* further discloses that a user can designate certain of these credentials as “requiring advance PIN-entry and others to function without the prior input of the wallet PIN.” *Id.*, [0366] (fingerprint can be used in lieu of a PIN), [0368].

As discussed above, *Dua*’s device also includes an electronic switch that controls the RFID communication responsive to the PIN or biometric authentication mechanism. *See supra* § VII.A.i.1[b]. For example, when the user is authenticated, the electronic switch can cause a transition from a PIN-less state (in which only credentials “designated by the user as not requiring entry of a wallet PIN” can be transmitted) to an authenticated state (in which other credentials “requiring advance PIN-entry” can be transmitted). *See supra* §VII.A.i.1[b]; EX1023, [0367]-[0368]. Accordingly, by authenticating themselves, the user can select between credentials (financial accounts) “designated by the user as not requiring entry of a wallet PIN” and credentials (financial accounts) “requiring advance PIN-entry,” via the electronic switch. EX1023, [0367]-[0368]. The selected credentials are then used for a subsequent financial transaction. *Id.*; EX1014, ¶¶94-96.

Thus, *Dua* discloses Claim 6.

Claim 7: a user interface configured to approve the financial transaction via the electronic switch

Dua discloses that its PIN and biometric authentication mechanisms include a key pad (used to capture a user's PIN) and a fingerprint scanner (used to capture a user's fingerprint), respectively. EX1023, [0041] (describing a "key pad for alphanumeric and special character data input"), [0414] ("PINs can be entered directly into the user's wireless device....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."). Accordingly, *Dua*'s key pad and fingerprint scanner are user interfaces for the PIN and biometric authentication mechanisms, respectively, because they interface with the user to capture data (PIN or fingerprint) to enable these mechanisms. EX1014, ¶¶97-99.

Additionally, as explained above, *Dua*'s device includes an electronic switch that enables transmission of certain credentials, responsive to the PIN or biometric authentication mechanisms. *See* §§VII.A.i.1[b], VII.A.ii (Claim 6). As discussed above, when the user is successfully authenticated using PIN or biometric authentication (via the key pad and fingerprint scanner user interfaces), RFID communication of payment credentials is enabled (a financial transaction is approved) via the electronic switch. *See supra* §§VII.A.i.1[b], VII.A.ii (Claim 6).

Thus, *Dua* discloses Claim 7.

Claim 8: the cellular telephone includes a biometric sensor and the circuit is configured to facilitate the financial transaction responsive to the biometric sensor

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 discussed above, *Dua*'s "circuit" is the processing and control circuitry that executes the wallet application and controls the embedded RF interface or smart card. EX1014, ¶¶100-01. 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. *Id.* Thus, by making the wallet application functionality and transmission of financial credentials (financial transactions) responsive to a fingerprint sensor (biometric sensor), *Dua* discloses Claim 8. *Id.*

Claim 9: wherein the circuit is configured to communicate an account number via the inductive coupling to facilitate the financial transaction

Dua discloses that the circuit is configured to communicate credentials via the inductive coupling to facilitate a financial transaction. *See* § VII.A.ii (Claim 5). *Dua* explains that such credentials include an “Account number.” EX1023, [0297], [0302]-[0304], [0383].

Thus, *Dua* discloses Claim 9.

Claim 10: an input configured for a user to enter a personal identification number, wherein the financial transaction is responsive to entry of the personal identification number and a signal communicated via the inductive coupling is responsive to the personal identification number

Dua discloses that its device includes a key pad (input) for entry of a PIN and that “PIN-entry is required before...credentials [are] transmitted to an external device.” *See supra* §VII.A.ii (Claim 7); EX1023, [0366], [0395].

As discussed above, when RFID transmission is enabled, the circuit can communicate financial account information via the inductive coupling to facilitate the financial transaction. *See* §VII.A.ii (Claim 5).

Thus, *Dua* discloses Claim 10.

Claim 11: a key memory configured to store an encryption key used to facilitate the financial transaction

Dua explains that credentials “transmitted from the wireless device to the reader may be encrypted using the issuer’s encryption key,” which is provided by

the issuer when a credential is issued. EX1023, [0362]. A POSITA would have understood that such a key would necessarily be stored in memory after it is received from the credential issuer, such that the key can later be read from memory and used to encrypt the credential and facilitate the financial transaction. EX1014, ¶¶107-08.

Thus, *Dua* discloses Claim 11.

Claim 12: a key memory configured to store a key required to change the states of the circuit to facilitate the financial transaction via the inductive coupling

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 ¶¶109-10. 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.* Thus, the reader key, which is stored in memory, is used to transition the circuit to an ON state that enables RFID communication, via the

inductive coupling, with the issuer-associated reader. EX1014, ¶¶109-10; *see supra* §§VII.A.i.1[a]–[b].

Thus, *Dua* discloses Claim 12.

Claim 13: a mechanical switch configured to approve the financial transaction

Dua’s device includes a “wallet button,” which can be pressed to “enable[] communication via the RFID interface.” EX1023, [0383], [0386]. *Dua*’s wallet button discloses a mechanical switch because it controls circuit components by making or breaking an electrical connection in the device circuitry, responsive to its components being pressed (moved) by a user. EX1014, ¶¶111-12 *see supra* §V.B (a POSITA would have understood “mechanical switch” to mean “a control device that makes or breaks an electrical connection in a circuit responsive to movement of one or more components of the control device.”). Further, the wallet button is configured to approve the financial transaction, because its actuation by a user is required to enable the RFID communication necessary to facilitate a transaction. EX1023, [0383], [0386].

Thus, *Dua* discloses Claim 13.

Claim 14: a reader configured to read a signal generated by the inductive coupling of the cellular telephone to perform the financial transaction

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...can simply be waved slowly in close proximity to a reader device to facilitate a transaction.” *Id.*

Thus, *Dua* discloses Claim 14.

Claim 15: a point of sale device including the reader

As discussed above, *Dua*’s device can communicate with a reader. *See supra* §VII.A.ii (Claim 14). *Dua* further explains that the reader is connected to “point of sale terminal 860.” EX1023, [0318], [0361], [0405], FIG. 8. It would have been obvious to a POSITA to combine the disclosed reader and point of sale terminal together, to reduce complexity and cost. EX1014, ¶¶115-16.

Thus, *Dua* renders obvious Claim 15.

Claim 16: wherein the circuit is configured to operate in at least a first ON state and a second ON state of the states, responsive to the electronic switch

Dua explains that the circuit can operate in multiple ON states that differ in whether authentication is required and in which credentials can be transmitted. EX1014, ¶¶117-21. *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.*, [0366] (biometric authentication can also be used in place of PIN authentication), [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.” *Id.*, [0370]. A POSITA would understand that this functionality necessarily discloses that the underlying processing and control circuitry executing the wallet application is in an ON state. EX1014, ¶¶117-21.

Dua explains that the wallet application can prompt the user to enter a PIN or biometric to access authentication-protected credentials. *See, e.g.*, EX1023, [0366]. In one embodiment including 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.*, [0366]. As discussed above in §VII.A.i, 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, ¶¶117-21. A POSITA would understand this state of the circuit to be another ON state, in which different credentials can be transmitted to the reader. *Id.*

A POSITA would have understood these two states to be a first ON state and a second ON state as recited in Claim 16, because different credentials are transmitted in each state (e.g., more sensitive credentials requiring PIN/biometric entry, or less sensitive PIN-less credentials). *Id.*; 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 a second ON state (i.e., wallet application is launched and communication of PIN-less credentials is enabled) to a first ON state (i.e., authenticated and communication of PIN/biometric-protected credentials is enabled). EX1014, ¶¶117-21; EX1023, [0366], [0368], [0384].

Thus, *Dua* discloses Claim 16.

Claim 17: wherein the circuit is configured to facilitate a financial transaction in the first ON state but not in the second ON state

Dua discloses a second ON state (e.g., PIN-less state) and a first ON state (e.g., authenticated state). *See* §VII.A.ii (Claim 16). As discussed above, 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.” EX1023, [0368]. In the PIN-less state (second ON state), the device transmits only certain designated credentials, which *Dua* describes as including non-payment information such as

“Personal Information—Name, billing address, shipping address, home phone number, business phone number, fax number, social security number, and date of birth.” *Id.*, [0343], [0392]-[0393]. In the authenticated state (first ON state), by contrast, the device transmits PIN-protected payment credentials in order to carry out a credit card or debit card transaction. *Id.*, [0393], [0395].

Thus, *Dua* discloses Claim 17.

Claim 18: wherein the circuit includes a state memory configured to store the states of the circuit

Dua’s device circuitry includes memory, and it would have been obvious to a POSITA to store the current state of the circuit in this memory (state memory), reflecting the current device state. EX1014, ¶¶124-25; *see supra* §VII.A.ii (Claim 2). Alternatively, it would have been obvious to a POSITA to store the current state in memory (state memory), to enable implementation of the logic described above. *See supra* §§VII.A.ii (Claims 16 and 17). For example, the circuit enables a “wallet application,” which controls the wireless device to carry out such logic. EX1023, [0333], [0354]. As described above, the circuit determines state transitions based on PIN or biometric authentication. *See supra* §§VII.A.i, VII.A.ii (Claims 16 and 17). These logical transitions require reading an input and applying logic based on the status thereof. A POSITA would have understood that to implement such functionality, the control software of the device would store the current state in a variable, according to logic based on input values, such that state transitions can be

implemented. EX1014, ¶¶124-25. Such techniques were well-known at the time of invention. *See* EX1026, 72 (storing switch state in a “Sw_state” variable), 74 (applying logic to “Sw_state” variable and storing output state in an “Output_port” variable). The value of the state variable would be stored in memory (state memory), such that the software can use the state variable during operation, to control the RFID circuitry to output jamming, transaction, or no data. *See id.*, 26.

Thus, *Dua* renders obvious Claim 18.

Claim 19: wherein the circuit is configured to store transaction logs

Dua states that “the wallet application will log all transactions made in proximity, personal, or remote mode,” and that “[t]he log will display information [s]uch as date/time, name of retailer/organization, location ID, list of credentials used in the transaction, and purchase price.” EX1023, [0489]. *Dua* further discloses digital receipts containing “the transaction amount, date/time of the transaction, merchant name, [and] payment method used.” *Id.*, [0430]. Thus, the wallet application stores transaction logs including details such as date, time, merchant, location, credential, and amount. *Id.*, [0489], [0430].

To the extent that *Dua* does not explicitly recite “the circuit is configured to store transaction logs,” it would have been obvious to a POSITA that the circuit would store transaction logs. EX1014, ¶¶126-28. Indeed, during prosecution of the '949 Patent, Applicant expressly admitted that “implementation of a circuit to

store transaction logs would be well understood by one of ordinary skill in the art.”

See supra §III.B.

Thus, *Dua* discloses, or otherwise renders obvious, Claim 19.

Claim 20: wherein the electronic switch is responsive to a biometric sensor

As discussed above, *Dua* discloses that its circuitry includes a fingerprint scanner (biometric sensor), which authenticates a user. *See supra* §§VII.A.ii (Claims 7 and 8). As further discussed above, the electronic switch enables RFID communication depending on whether a user is authenticated. *See* §VII.A.i.1[b]; EX1014, ¶¶129-30. Accordingly, the electronic switch is responsive to the fingerprint scanner (biometric sensor).

Thus, *Dua* discloses Claim 20.

Claim 21: an input configured for a user to enter a personal identification number (PIN), communication via the inductive coupling being responsive to the personal identification number

Dua discloses Claim 21, because as discussed above, *Dua* discloses a key pad (input) for entry of a PIN, and that RFID communication via the inductive coupling is responsive to the PIN. *See supra* §VII.A.ii (Claim 10).

Claim 22: wherein the cellular telephone further includes an antenna configured to communicate using WiFi, the antenna

being configured to operate at a different frequency than the inductive coupling

Dua discloses that “wireless device 200...is capable of wirelessly connecting to the Internet using network protocols such as...802.11a, 802.11b, [and] 802.11g.” EX1023, [0041], [0318], [0323], [0423]. Each of these are WiFi protocols. EX1014, ¶¶132-34. Thus, *Dua*’s device is configured to communicate via WiFi.

To the extent *Dua* does not expressly describe a separate WiFi antenna, providing one would have been obvious, and indeed necessary, to implement *Dua*’s 802.11 (WiFi) functionality. *Id.* Further, a POSITA would have understood that such a WiFi antenna would be tuned to 2.4 GHz or 5 GHz, both of which are different frequencies than the 13.56 MHz frequency used for *Dua*’s RFID communication described above. *Id.*

Thus, *Dua* renders obvious Claim 22.

Claim 23: wherein the inductive coupling is part of a radio frequency identification device

As discussed, *Dua*’s device includes an inductive coupling. *See supra* §VII.A.i.1[a]. *Dua*’s device is also capable of RFID communication, and is therefore an RFID device. *Id.*; EX1014, ¶¶135-36.

Thus, *Dua* renders obvious Claim 23.

Claim 26: wherein the circuit includes both the electronic switch and a mechanical switch configured to approve a financial transaction

As discussed above, *Dua* discloses (1) PIN and biometric authentication mechanisms, which include an electronic switch, and (2) a wallet button (mechanical switch). *See supra* §§VII.A.i.1[b], VII.A.ii (Claim 13). As further discussed above, both the electronic switch and the wallet button (mechanical switch) are configured to approve a financial transaction. *Id.*

Thus, *Dua* discloses Claim 26.

Claim 27: wherein the cellular phone is configured to purchase goods by placing the circuit within the reading range of a wireless point of sale device and communicating a financial account number to the wireless point of sale device using the induction coupling responsive to the states of the circuit

As discussed above, *Dua* discloses placing the wireless device (and the circuitry contained therein) within the reading range of a reader connected to a point-of-sale terminal to facilitate a transaction. *See supra* §VII.A.ii (Claims 14 and 15). *Dua* provides that an exemplary transaction includes “a grocery store POS purchase.” EX1023, [0352]. As further discussed above, *Dua* discloses that such a financial transaction is facilitated by communicating a financial account number to the reader via the inductive coupling responsive to the states of the circuit. *See supra* §§VII.A.i.1[b]-1[c], VII.A.ii (Claims 5 and 9).

Thus, *Dua* discloses Claim 27.

Claim 28: wherein the electronic switch is responsive to data stored in memory of the cellular telephone and the data stored in memory includes biometric data

As discussed above, *Dua* discloses an electronic switch responsive to fingerprint (biometric) authentication. *See supra* §§VII.A.i.1[b], VII.A.ii (Claims 8 and 20). A POSITA would have understood that, to enable the described fingerprint authentication, it would have been necessary, or at least obvious, to store the user's true fingerprint (biometric) data in device memory for comparison to the fingerprint (biometric) data received from the fingerprint scanner during a subsequent authentication attempt by the user. EX1023, [0041], [0366]; EX1014, ¶¶141-42.

Thus, *Dua* discloses or otherwise renders obvious Claim 28.

iii. **Independent Claim 29**

29[pre]: A cellular telephone configured to communicate wirelessly using an inductive coupling and also configured to communicate using WiFi

Dua discloses, or otherwise renders obvious, 29[pre], because as discussed above, its cellular telephone communicates wirelessly via RFID (using an inductive coupling) and WiFi. *See supra* §§VII.A.i.1[a], VII.A.ii (Claim 22).

29[a]: wherein the inductive coupling is part of a circuit configured to facilitate a financial transaction communicated via the inductive coupling

Dua discloses 29[a], because as discussed above, its device circuitry includes an inductive coupling, and facilitates RFID payments (financial transactions

communicated via the inductive coupling). *See supra* §§VII.A.i.1[b]-1[c], VII.A.ii (Claim 5).

29[b]: the circuit being configured to facilitate the financial transaction responsive to a biometric sensor

Dua discloses 29[b], because as discussed above, its device circuitry facilitates RFID payments (financial transactions) responsive to a fingerprint scanner (biometric sensor). *See supra* §VII.A.ii (Claim 8).

Accordingly, *Dua* discloses, or otherwise renders obvious, each element of independent Claim 29.

iv. **Independent Claim 30**

30[pre]: A cellular telephone configured to communicate wirelessly using an inductive coupling and also configured to communicate using WiFi

30[pre] is identical to 29[pre]. Thus, *Dua* discloses, or otherwise renders obvious, 30[pre] for the reasons discussed above. *See supra* §VII.A.iii.29[pre].

30[a]: wherein the inductive coupling is part of a circuit configured to facilitate a financial transaction communicated via the inductive coupling

30[a] is identical to 29[a]. Thus, *Dua* discloses, or otherwise renders obvious, 30[a] for the reasons discussed above. *See supra* §VII.A.iii.29[a].

30[b]: the circuit being configured to facilitate the financial transaction being responsive to a personal identification number entered by a user

Dua discloses 30[b], because as discussed above, its device circuitry facilitates RFID payments (financial transaction) responsive to a PIN entered by a user. *See supra* §VII.A.ii (Claim 10).

Accordingly, *Dua* discloses, or otherwise renders obvious, each element of independent Claim 30.

B. GROUND 3: *DUA* IN VIEW OF *WOIKE* RENDERS OBVIOUS CLAIMS 24 AND 25

i. Motivation to Combine

Dua and *Woike* are both directed to electronic systems for conducting financial transactions using portable electronic devices. EX1014, ¶¶151-53. *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, ll. 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, ¶¶151-53.

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. *Id.* 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. **Claims 24 and 25**

Claim 24: an electronic key configured to be inserted into the cellular telephone, the electronic key including an account identifier and a signal communicated via the inductive coupling being responsive to the account identifier

Dua’s wireless device discloses and/or renders obvious the limitations of Claim 1, from which Claim 24 depends, for the reasons discussed above. *See supra* § VII.A.i.

Woike further 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, ¶¶154-57.

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, ¶¶154-57. Accordingly, a POSITA would have understood that the PIN code is an account identifier, because through the authentication process, the PIN would be used to identify an account as belonging (or not belonging) to a user. *Id.* 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-Woike* renders obvious Claim 24.

Claim 25: wherein the electronic key is configured to store a password

Dua-Woike renders obvious Claim 25, because *Woike*'s SIM card, which requires a PIN code, is configured to store a password for the reasons discussed above in §VII.B.ii (Claim 24). EX1025, p. 2, ll. 24-26; EX1014, ¶158.

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, ¶¶159-62. *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 a mechanical switch (whether implemented as a wallet button or pressure sensor) can be implemented to enable or disable RFID communication, to prevent skimming. EX1014, ¶¶159-62.

Both *Waters* and *Dua* address the problem of enabling secure financial transactions using mobile devices. *Id.* *Waters* teaches using a mobile device 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, ¶¶159-62. 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.*

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. *Id.* The combination would involve using *Dua*’s wallet application implementation within *Waters*’s mobile transaction framework. *Id.*

ii. **Independent Claim 1**

1[pre]: An electronic communication system

Waters discloses a mobile terminal (electronic communication system) 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

discloses that “[t]he mobile terminal 1 may be a handheld mobile telephone.” *Id.*, [0020].

Thus, *Waters-Dua* renders obvious 1[pre].²

1[a]: a cellular telephone configured to communicate wirelessly using an inductive coupling

Waters discloses that its device is a “[m]obile terminal...registered with [a] GSM/GPRS or UMTS (3G) mobile or cellular telecommunications network.” EX1024, [0020]. Accordingly, *Waters*’s device is a cellular telephone. EX1014, ¶¶165-67.

Waters further discloses that its device “includes a near field or RFID tag...[that] operates in the unregulated RF band of 13.56 MHz.” *Id.*, [0034]. *Waters*’s device carries out wireless RFID communication via 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 a “near field tag” including an “inbuilt inductive antenna” operating “in accordance with ISO-IEC 14443 and ISO-IEC 15693 standards” explicitly or inherently discloses an inductive coupling. EX1014, ¶¶165-67.

² *Dua* also discloses and/or renders obvious each limitation of Claims 1–23 and 26–30 for the reasons discussed above in Grounds 1–2. *See supra* §VII.A.

Thus, *Waters-Dua* renders obvious 1[a].

1[b]: wherein the inductive coupling is part of a circuit including an electronic switch configured to change between states of the circuit

Similar to *Dua*, *Waters* discloses the use of PIN or biometric authentication to implement RFID communication logic responsive to a PIN or biometric sensor. EX1024, [0052] (“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”). 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, ¶¶168-69. 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). *Id.*

Thus, *Waters-Dua* renders obvious 1[b].

1[c]: configured to communicate via the inductive coupling responsive to the states of the circuit

A POSITA would understand that the near field tag 41 and its associated control circuitry (as identified in §VII.C.ii.1[b]) 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 is activated by correct PIN or biometric entry. *Id.*, [0051]–[0052]; EX1014, ¶¶170-73.

As discussed above, it would have been obvious to a POSITA that such communication would occur via an inductive coupling. *See supra* § VII.C.ii.1[a].

Thus, *Waters-Dua* renders obvious 1[c].

Accordingly, *Waters-Dua* renders obvious each element of independent Claim 1.

iii. **Dependent Claims 2–28**

Claim 2: wherein the circuit includes a switchable RFID tag, input logic, processing logic, a return signal generator, switch logic, a switch state monitor, encryption logic, one or more antenna, memory or a power supply

Waters-Dua renders obvious Claim 2, because *Waters* discloses that its device circuitry has memory and a power supply. EX1024, [0035]–[0036], [0051]; *see Brown v. 3M*, 265 F.3d 1349, 1352 (Fed. Cir. 2001) (construing “or” as meaning that the apparatus was capable of meeting only one of the preceding elements or any combination of the preceding elements).

Further, to the extent that *Waters* and *Dua* do not expressly disclose a switchable RFID tag, input logic, processing logic, a return signal generator, switch

logic, a switch state monitor, encryption logic, or one or more antenna, it would have been obvious to a POSITA to implement each of these components in the device of *Waters-Dua*, as these are necessary to enable the RFID payment functionality described above. EX1014, ¶¶174-75; *see supra* §§VII.C.i–ii.

Claim 3: wherein the memory is configured to store a financial account balance

As discussed above with respect to Grounds 1–2, *Dua*’s wallet application is configured such that when such a stored value credential “is waved in front of a reader at the turnstile, the electronic balance is automatically debited from the onboard chip” and “an over-the-air reload tool” can be programmed into the wallet application. EX1023, [0290], [0293]. As further discussed above, when applied to the device of *Waters*, a POSITA would have understood that debiting and reloading an electronic balance on the device similarly requires that the balance be stored in the device’s memory. EX1014, ¶¶176-77; *see supra* §VII.A.ii (Claim 3).

Thus, *Waters-Dua* renders obvious Claim 3.

Claim 4: wherein the cellular telephone further includes a user interface configured to enter a financial account number and the memory is configured to store the financial account number for use in the financial transaction

Similar to *Dua*, *Waters* discloses that its device includes a “keypad” (a type of user interface). EX1024, [0034], [0051]. As discussed above with respect to Grounds 1–2, *Dua* discloses that its wallet application is configured to receive a

financial account number inputted by a user via a keypad. *See supra* § VII.A.ii (Claim 4). Accordingly, a POSITA would understand that when implemented in *Waters's* device, the wallet application would receive a financial account number inputted by a user via *Waters's* keypad (user interface). EX1014, ¶¶178-80.

As further discussed above, *Dua's* wallet application controls the device to store a financial account number in memory. *See supra* §VII.A.ii (Claim 4). Accordingly, when implemented in *Waters's* device, a POSITA would understand that the financial account number would be stored in memory. EX1014, ¶¶178-80.

Thus, *Waters-Dua* renders obvious Claim 4.

Claim 5: wherein the circuit is configured to facilitate a financial transaction responsive to the states of the circuit via the inductive coupling

As discussed above with respect to 1[c], *Waters-Dua* renders obvious that the circuit is configured to control communication via the inductive coupling, responsive to the states of the circuit. *See supra* §VII.C.ii.1[c].

Further, *Waters* and *Dua* both teach that such communication can facilitate a financial transaction. For example, *Waters* provides that the communication can be used to “make a payment.” EX1024, Abstract, [0043]. Similarly, *Dua* discloses that its circuitry can control a device to “transmit payment...information to a reader using the short-range transmission capability of the wireless device (e.g., RF).” EX1023, [0315].

Thus, *Waters-Dua* renders obvious Claim 5.

Claim 6: wherein the electronic switch 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 6 for the same reasons discussed above in Grounds 1–2. *See* §VII.A.ii (Claim 6).

Claim 7: a user interface configured to approve the financial transaction via the electronic switch

Similar to *Dua*, *Waters* discloses that its PIN and biometric authentication mechanisms include a keypad (used to capture a user’s PIN) and a fingerprint reader (used to capture a user’s fingerprint), respectively. EX1024, [0034], [0051]. Accordingly, *Waters*’s key pad and fingerprint scanner are user interfaces for the PIN and biometric authentication mechanisms, respectively, because they interface with the user to capture data (PIN or fingerprint) to enable these mechanisms. EX1014, ¶¶185-87.

Additionally, as explained above, the *Waters-Dua* device includes an electronic switch that enables transmission of certain credentials, responsive to the PIN or biometric authentication mechanisms. *See supra* §§VII.C.ii.1[b]–1[c], VII.C.iii (Claim 6). As discussed above, when the user is successfully authenticated using PIN or biometric authentication (via the key pad and fingerprint reader user

interfaces), RFID communication of payment credentials is enabled (a financial transaction is approved) via the electronic switch. *Id.*

Thus, *Waters-Dua* renders obvious Claim 7.

Claim 8: the cellular telephone includes a biometric sensor and the circuit is configured to facilitate the financial transaction responsive to the biometric sensor

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, ¶¶188-89. *Dua* also discloses making its wallet application functionality and transmission of financial credentials responsive to a fingerprint sensor. *See supra* §VII.A.ii (Claim 8). *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, ¶¶188-89. 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. *Id.* Thus, by making the wallet application functionality and transmission of financial credentials responsive to a fingerprint sensor, *Waters* in view of *Dua* renders obvious Claim 8.

Claim 9: wherein the circuit is configured to communicate an account number via the inductive coupling to facilitate the financial transaction

Waters-Dua renders obvious Claim 9, because as discussed above with reference to Grounds 1–2, *Dua*’s wallet application (which, in the *Waters-Dua*

combination, is implemented in *Waters's* device) controls the device circuitry to communicate financial account information, including an “Account number,” via the inductive coupling to facilitate the financial transaction. EX1023, [0297], [0302]-[0304], [0383]; *see supra* §VII.A.ii (Claim 9).

Claim 10: an input configured for a user to enter a personal identification number, wherein the financial transaction is responsive to entry of the personal identification number and a signal communicated via the inductive coupling is responsive to the personal identification number

As discussed above, the *Waters-Dua* device includes a keypad (input) for entry of a PIN, which is required to enable a financial transaction. *See supra* §VII.C.iii (Claim 7).

As further discussed above, when RFID transmission is enabled, the circuit can communicate financial account information via the inductive coupling to facilitate the financial transaction. *See* §VII.C.iii (Claim 5).

Thus, *Waters-Dua* renders obvious Claim 10.

Claim 11: a key memory configured to store an encryption key used to facilitate the financial transaction

Waters discloses that the SIM stores “authentication information” in memory (key memory), which is used as an encryption key during an authentication process. EX1024, [0023]. For example, *Waters* provides that a telecommunications network can send a challenge to the SIM. *Id.* Then, the SIM “calculates a reply” “dependent on” the authentication information. *Id.* A processor connected to the

telecommunications network then “calculates the expected value of the reply” and compares it to the reply sent by the SIM. *Id.* If these match, then the SIM is authenticated. *Id.*

A POSITA would have understood that the process described above would require the SIM to “calculate” the reply by encrypting the challenge message using the authentication information. EX1014, ¶¶195-98. Thus, the authentication information is an encryption key. *Id.*

Waters further discloses that the RFID functionality (which, as discussed above, is carried out via an inductive coupling) can be enabled or disabled, depending on whether the SIM is authenticated by this process (i.e., responsive to the authentication information). EX1024, [0036], [0046]-[0047]; *see supra* §VII.C.ii.1[b]. Accordingly, RFID transactions are facilitated by successful authentication using the authentication information. EX1014, ¶¶195-98.

Thus, *Waters-Dua* renders obvious Claim 11.

Claim 12: a key memory configured to store a key required to change the states of the circuit to facilitate the financial transaction via the inductive coupling

Waters-Dua renders obvious Claim 12, because as discussed above, its device includes a key memory configured to store authentication information (key), which is required to enable RFID communication (change the states of the circuit) to

facilitate a financial transaction, which is made via the inductive coupling. *See supra* §§VII.C.ii.1[a]–[c], VII.C.iii (Claim 11).

Claim 13: a mechanical switch configured to approve the financial transaction

Similar to *Dua*, *Waters* discloses that its device can include a “pressure sensor...[that] acts as a switch” to enable RFID communication. EX1024, [0053], [0056]. Specifically, when the user “physically presses” the pressure sensor, RFID communication is enabled, such that payment information can be transmitted. *Id.*, [0041]–[0045], [0053]. The pressure sensor discloses a mechanical switch because it controls circuit components by making or breaking an electrical connection in the device circuitry, responsive to its components being pressed (moved) by a user. *Id.*, [0053]; EX1014, ¶¶200-01; *see supra* §V.B (a POSITA would have understood “mechanical switch” to mean “a control device that makes or breaks an electrical connection in a circuit responsive to movement of one or more components of the control device.”).

Thus, *Waters-Dua* renders obvious Claim 13.

Claim 14: a reader configured to read a signal generated by the inductive coupling of the cellular telephone to perform the financial transaction

Waters discloses that its device can “exchange information with a tag reader when the two are brought into close proximity.” EX1024, [0035]. Such an

information exchange can be used to “make a payment” at a reader. *Id.*, Abstract; *see also id.*, [0041]–[0043], [0045].

Thus, *Waters-Dua* renders obvious Claim 14.

Claim 15: a point of sale device including the reader

Waters-Dua renders obvious Claim 15 for the same reasons discussed above, with respect to Claim 14, because it would have been obvious to a POSITA that *Waters*’s reader would be located within a point of sale, to reduce complexity and cost. *See supra* §VII.C.iii (Claim 14); EX1014, ¶204.

Claim 16: wherein the circuit is configured to operate in at least a first ON state and a second ON state of the states, responsive to the electronic switch

Waters-Dua renders obvious Claim 16, because as discussed above, *Dua*’s wallet application (which, in the *Waters-Dua* combination, is implemented in *Waters*’s device) controls the device circuitry to operate in an authenticated state (first ON state) and a PIN-less state (second ON state), responsive to the electronic switch. *See supra* §VII.A.ii (Claim 16).

Claim 17: wherein the circuit is configured to facilitate a financial transaction in the first ON state but not in the second ON state

Waters-Dua renders obvious Claim 17, because as discussed above, *Dua*’s wallet application (which, in the *Waters-Dua* combination, is implemented in *Waters*’s device) controls the device circuitry to facilitate a financial transaction in

the authenticated state (first ON state) but not in the PIN-less state (second ON state).

See supra §§VII.A.ii (Claims 16 and 17).

Claim 18: wherein the circuit includes a state memory configured to store the states of the circuit

Waters-Dua renders obvious Claim 18, because as discussed above in Grounds 1–2, a POSITA would have understood that, to enable implementation of the software-based logic described above, it would have been necessary, or at least obvious, for the processing and control circuitry to store its states in memory (state memory). *See* §VII.A.ii (Claim 18).

Claim 19: wherein the circuit is configured to store transaction logs

Waters-Dua renders obvious Claim 19, because as discussed above with respect to Grounds 1–2, *Dua*’s wallet application (which, in *Waters-Dua*, is implemented in *Waters*’s device) controls the device circuit to store transaction logs. *See supra* §§III.B (during prosecution, Applicant expressly admitted that “implementation of a circuit to store transaction logs would be well understood by one of ordinary skill in the art”), VII.A.ii (Claim 19).

Claim 20: wherein the electronic switch is responsive to a biometric sensor

As discussed above, the *Waters-Dua* circuitry includes a fingerprint reader (biometric sensor), which authenticates a user. *See supra* §§VII.C.iii (Claims 7 and 8). As further discussed above, the electronic switch enables RFID communication

depending on whether a user is authenticated. *See* §VII.C.ii.1[b]; EX1014, ¶¶209-10. Accordingly, the electronic switch is responsive to the fingerprint scanner (biometric sensor).

Thus, *Waters-Dua* renders obvious Claim 20.

Claim 21: an input configured for a user to enter a personal identification number (PIN), communication via the inductive coupling being responsive to the personal identification number

Waters-Dua renders obvious Claim 21, because as discussed above, its device includes a keypad (input) for entry of a PIN, and RFID communication via the inductive coupling is responsive to the PIN. *See supra* §VII.C.iii (Claim 10).

Claim 22: wherein the cellular telephone further includes an antenna configured to communicate using WiFi, the antenna being configured to operate at a different frequency than the inductive coupling

Waters discloses that its device can communicate “with a network...via a UMA ‘access point.’” EX1024, [0024]. Unlicensed Mobile Access (“UMA”) is a telecommunications standard that enables mobile phones to route data over unlicensed IP-based networks, including WiFi networks. EX1014, ¶¶212-13. To the extent *Waters* does not expressly describe a separate WiFi antenna, providing one would have been necessary, or at least obvious, in order to implement the UMA connectivity *Waters* describes. *Id.* Further, a POSITA would have understood that such a WiFi antenna would be tuned to 2.4 GHz or 5 GHz, both of which are different

frequencies than the 13.56 MHz frequency used for *Waters*'s RFID communication described above. *Id.*; EX1024, [0034].

Thus, *Waters-Dua* renders obvious Claim 22.

Claim 23: wherein the inductive coupling is part of a radio frequency identification device

As discussed, the *Waters-Dua* device includes an inductive coupling. *See supra* §VII.C.ii.1[a]. The *Waters-Dua* device is also capable of RFID communication, and is therefore an RFID device. *Id.*; EX1014, ¶¶214-16.

Thus, *Waters-Dua* renders obvious Claim 23.

Claim 24: an electronic key configured to be inserted into the cellular telephone, the electronic key including an account identifier and a signal communicated via the inductive coupling being responsive to the account identifier

Waters discloses that its device includes a “subscriber identity module (SIM) 15.” EX1024, [0023]. A SIM card is a component that is inserted into a device, such as a cellular telephone. EX1014, ¶¶217-20.

Waters discloses that the SIM can store “authentication information,” which can be used to authenticate whether “a particular user...has a particular pre-paid account with a network.” EX1024, [0023], [0026]; *see also supra* §VII.C.iii (Claim 11). Accordingly, the authentication information is an account identifier, because it can be used to identify a user's account. EX1014, ¶¶217-20. *Waters* further discloses that the RFID functionality (which, as discussed above, is carried out via an

inductive coupling) can be enabled or disabled, depending on whether the SIM is successfully authenticated using the authentication information (account identifier). EX1024, [0036], [0046]-[0047]; *see supra* §VII.C.ii.1[b].

Thus, *Waters-Dua* renders obvious Claim 24.

Claim 25: wherein the electronic key is configured to store a password

Waters discloses that the “PIN may be stored in a secure location in...SIM 15.” EX1024, [0051], [0060]. As discussed above, the PIN is used as a password to enable RFID communication. *Id.*; *see supra* §VII.C.iii (Claim 7).

Thus, *Waters-Dua* renders obvious Claim 25.

Claim 26: wherein the circuit includes both the electronic switch and a mechanical switch configured to approve a financial transaction

As discussed above, the *Waters-Dua* device includes (1) PIN and biometric authentication mechanisms, which include an electronic switch, and (2) a pressure sensor (mechanical switch). *See supra* §§VII.C.ii.1[b], VII.C.iii (Claim 13). As further discussed above, both the electronic switch and the pressure sensor (mechanical switch) are configured to approve a financial transaction. *Id.*

Thus, *Waters-Dua* renders obvious Claim 26.

Claim 27: wherein the cellular phone is configured to purchase goods by placing the circuit within the reading range of a wireless point of sale device and communicating a financial account number to the wireless point of sale device

using the induction coupling responsive to the states of the circuit

As discussed above, *Waters* discloses placing the wireless device (and the circuitry contained therein) within the reading range of a reader connected to a point-of-sale terminal to facilitate a transaction. *See supra* §VII.C.iii (Claims 14 and 15). *Waters* provides that an exemplary transaction includes “a school child...pay[ing] for their lunch.” EX1024, [0043]. As further discussed above, a financial transaction is facilitated by communicating a financial account number to the reader via the inductive coupling responsive to the states of the circuit. *See supra* §§VII.C.ii.1[b]-1[c], VII.C.iii (Claims 5 and 9).

Thus, *Waters-Dua* renders obvious Claim 27.

Claim 28: wherein the electronic switch is responsive to data stored in memory of the cellular telephone and the data stored in memory includes biometric data

As discussed above, *Waters* discloses an electronic switch responsive to fingerprint (biometric) authentication. *See supra* §§VII.C.ii.1[b], VII.C.iii (Claims 8 and 20). In one example, a “fingerprint reader 45 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.” EX1024, [0051]. If the captured fingerprint matches the stored fingerprint, then RFID communication is enabled. *Id.*

Thus, *Waters-Dua* renders obvious Claim 28.

iv. Independent Claim 29

29[pre]: A cellular telephone configured to communicate wirelessly using an inductive coupling and also configured to communicate using WiFi

Waters-Dua renders obvious 29[pre], because as discussed above, its cellular telephone communicates wirelessly via RFID (using an inductive coupling) and WiFi. *See supra* §§VII.C.ii.1[a], VII.C.iii (Claim 22).

29[a]: wherein the inductive coupling is part of a circuit configured to facilitate a financial transaction communicated via the inductive coupling

Waters-Dua renders obvious 29[a], because as discussed above, its device circuitry includes an inductive coupling, and facilitates RFID payments (financial transactions communicated via the inductive coupling). *See supra* §§VII.C.ii.1[b]-1[c], VII.C.iii (Claim 5).

29[b]: the circuit being configured to facilitate the financial transaction responsive to a biometric sensor

Waters-Dua renders obvious 29[b], because as discussed above, its device circuitry facilitates RFID payments (financial transactions) responsive to a fingerprint scanner (biometric sensor). *See supra* §VII.C.iii (Claim 8).

Accordingly, *Waters-Dua* renders obvious each element of independent Claim 29.

v. **Independent Claim 30**

30[pre]: A cellular telephone configured to communicate wirelessly using an inductive coupling and also configured to communicate using WiFi

30[pre] is identical to 29[pre]. Thus, *Waters-Dua* renders obvious 30[pre] for the reasons discussed above. *See supra* §VII.C.iv.29[pre].

30[a]: wherein the inductive coupling is part of a circuit configured to facilitate a financial transaction communicated via the inductive coupling

30[a] is identical to 29[a]. Thus, *Waters-Dua* renders obvious 30[a] for the reasons discussed above. *See supra* §VII.C.iv.29[a].

30[b]: the circuit being configured to facilitate the financial transaction being responsive to a personal identification number entered by a user

Waters-Dua renders obvious 30[b], because as discussed above, its device circuitry facilitates RFID payments (financial transaction) responsive to a PIN entered by a user. *See supra* §VII.C.iii (Claim 10).

Accordingly, *Waters-Dua* renders obvious each element of independent 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 '949 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 11,514 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