

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. IPR2026-00511
U.S. Patent No. 12,039,396

**PETITION FOR INTER PARTES REVIEW OF
U.S. PATENT NO. 12,039,396**

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.	'396 PATENT.....	2
	A. SPECIFICATION	2
	B. FILE HISTORY	2
IV.	LEVEL OF ORDINARY SKILL IN THE ART.....	6
V.	CLAIM CONSTRUCTION	6
	A. TERMS CONSTRUED IN <i>MYNETTE</i>	6
	B. “MECHANICAL SWITCH”	7
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).....	12
VII.	INVALIDITY	12
	A. GROUNDS 1–2: <i>DUA</i> ANTICIPATES AND/OR RENDERS OBVIOUS CLAIMS 1–10 AND 12–20	12
	i. Independent Claim 1	12
	ii. Dependent Claims 2–10 and 12–20	16
	B. GROUND 3: <i>DUA</i> IN VIEW OF <i>WOIKE</i> RENDERS OBVIOUS CLAIM 11	25
	i. Motivation to Combine	25
	ii. Claim 11: a slot of the cellular telephone configured to accept a memory device configured to store a key, the key being configured to allow the cellular phone to engage in the financial transactions	26
	C. GROUND 4: <i>WATERS</i> IN VIEW OF <i>DUA</i> RENDERS OBVIOUS CLAIMS 1–4, 6–20.....	27
	i. Motivation to Combine	27

ii.	Independent Claim 1	29
iii.	Dependent Claims 2–4, 6–20	31
VIII.	CONCLUSION	39

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. 12,039,396 (“’396 patent”) is currently asserted by Patent Owner (“PO”) against Petitioners in the case styled: *SureCell Transactions LLC v. Samsung Electronics Co., Ltd.*, No. 2:26-cv-00106 (E.D. Tex.), which was originally filed on February 12, 2026.

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

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

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

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

CLAIMS LISTING

Claim 1:

1[pre]	A cellular telephone configured to use two or more different wireless communication modes, the cellular telephone comprising:
1[a]	circuits configured to operate in a first wireless mode for cellular operation and in a second wireless mode for short range communication,
1[b]	wherein the first and second modes are characterized by use of different radio frequency ranges and the circuits are configured to perform financial transactions;
1[c]	a biometric sensor, wherein the circuits are configured to approve the financial transactions responsive to the biometric sensor; and
1[d]	an inductive antenna configured for communication of signals in the second mode.

Claim 2:

2[a]	The cellular telephone of claim 1, further comprising a mechanical switch configured to approve the financial transactions,
2[b]	wherein the financial transactions are responsive to both the biometric sensor and the mechanical switch.

Claim 3:

3	The cellular telephone of claim 1, wherein the financial transactions are performed in the second mode.
----------	---

Claim 4:

4	The cellular telephone of claim 1, wherein the financial transactions are performed in the first mode.
----------	--

Claim 5:

5	The cellular telephone of claim 1, wherein the circuits are configured to communicate the financial transactions over WiFi.
----------	---

Claim 6:

6	The cellular telephone of claim 1, wherein the circuits are configured to communicate the financial transactions over a cellular network.
----------	---

Claim 7:

7	The cellular telephone of claim 1, wherein the circuits are configured to communicate with a point-of-sale device in the second mode to perform the financial transactions.
----------	---

Claim 8:

8	The cellular telephone of claim 1, further comprising a user interface configured to enter a credit or debit card number.
----------	---

Claim 9:

9	The cellular telephone of claim 1, further comprising a user interface configured for a user to select between financial accounts.
----------	--

Claim 10:

10	The cellular telephone of claim 1, further comprising a user interface configured for a user to enter amounts of the financial transactions.
-----------	--

Claim 11:

11	The cellular telephone of claim 1, further comprising a slot of the cellular telephone configured to accept a memory device configured to store a key, the key being configured to allow the cellular phone to engage in the financial transactions.
-----------	--

Claim 12:

12	The cellular telephone of claim 1, further comprising encryption logic configured to encrypt data prior to transmission of the data.
-----------	--

Claim 13:

13	The cellular telephone of claim 1, further comprising keys within the cellular phone configured to turn on and off transmission in the second mode.
-----------	---

Claim 14:

14	The cellular telephone of claim 1, further comprising keys within the cellular phone configured to operate a lock in the second mode.
-----------	---

Claim 15:

15	The cellular telephone of claim 1, further comprising memory configured to store a first financial account identifier and a second financial account identifier, the first and second financial account identifiers being identifiers of different financial accounts.
-----------	--

Claim 16:

16	The cellular telephone of claim 1, wherein the circuits are further configured to unlock a car.
-----------	---

Claim 17:

17	The cellular telephone of claim 1, wherein the circuits include an identity device, the identity device including a driver's license.
-----------	---

Claim 18:

18	The cellular telephone of claim 1, wherein recognition of a biometric is required to approve the financial transaction.
-----------	---

Claim 19:

19[a]	The cellular telephone of claim 1, wherein the biometric sensor is configured to switch between first and second ON modes of the circuits,
19[b]	wherein the financial transactions are approved in the first ON mode but not approved in the second ON mode.

Claim 20:

20	The cellular telephone of claim 1, wherein the circuits are configured to communicate the financial transactions using RFID.
-----------	--

I. INTRODUCTION

The Office materially erred in granting U.S. Patent No. 12,039,396 (“the ’396 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 ’396 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 ’396 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 1–2	<i>Dua</i> anticipates and/or renders obvious claims 1–10, 12–20
Ground 3	<i>Dua</i> with <i>Woike</i> renders obvious claim 11
Ground 4	<i>Waters</i> with <i>Dua</i> renders obvious claims 1–4, 6–20

III. '396 PATENT

A. SPECIFICATION

The '396 Patent relates to systems for performing a financial transaction using a switchable circuit to control communication of financial information using inductive coupling or an RF antenna. EX1006, Cl. 1. While the specification describes a switchable RFID tag, “[v]arious embodiments of the invention include a portable communication device such as a cellular telephone.” *Id.*, 9:63-64. The communication device includes a user interface used “to turn on or off operation of the RFID tag, to enter security data into the RFID tag, to enter financial information (e.g., a credit or debit card number[]) into the RFID tag, to enter an identifying number (e.g., telephone number) into the RFID Tag, or to enter account number into the RFID tag.” *Id.*, 10:11-17.

B. FILE HISTORY

The '396 Patent was filed as App. No. 18/422,929 (the “'929 Application”) on January 25, 2024, and on its face, purports to claim priority to a provisional application filed on May 6, 2005. EX1006, Cover. In a Preliminary Amendment dated March 28, 2024, Applicant added certain claims, cancelled certain claims, and made amendments to pending claim 1. EX1012, 121–22. Independent claim 1 recited:

1. (Currently Amended) A cellular telephone configured to use two or more different wireless communication modes, the cellular telephone comprising:

circuits configured to operate in a first mode for cellular operation and in a second mode for short range communication, wherein the first and second modes are characterized by different radio frequency ranges;

a biometric sensor, financial transactions made using the circuits being responsive to the biometric sensor, wherein the circuits are configured to approve the financial transactions responsive to the biometric sensor; and

an inductive antenna configured for communication of signals in the second mode.

Id., 121.

In a first Non-Final Office Action dated April 22, 2024, the Examiner rejected pending claims 1 and 3–19 under 35 U.S.C. §112(b) or pre-AIA 35 U.S.C. §112 as indefinite, based on the limitations reciting “circuits configured to operate in a first mode for cellular operation and in a second mode for short range communication, wherein the first and second modes are characterized by different radio frequency ranges,” “a biometric sensor, financial transactions made using the circuits being responsive to the biometric sensor,” and “a biometric sensor, financial transactions made using the circuits being responsive to the biometric sensor, wherein the circuits are configured to approve the financial transactions responsive to the biometric sensor.” *Id.*, 67–68. Specifically, the Examiner noted that the claims did not set forth a clear understanding of “how the first and second modes are characterized by different radio frequency ranges,” “what is responsive to the biometric sensor,” or

“how the circuits are configured to approve the financial transactions responsive to the biometric sensor,” respectively. *Id.* Additionally, pending claims 1 and 3–19 were rejected under pre-AIA 35 U.S.C. §102(b) as being anticipated by U.S. Patent Publication No. 2006/0072542 (“Sinnreich”).

Later that same day, Applicant filed a Response to Non-Final Office Action. *Id.*, 58–64. As shown below, in the Response, Applicant amended independent claim 1 to recite “the first and second modes are characterized by use of different radio frequency ranges” and “and the circuits are configured to perform financial transactions.” *Id.*, 58, 61. Applicant argued that these amendments rendered moot the Examiner’s §112 rejections regarding the limitations “circuits configured to operate in a first mode for cellular operation and in a second mode for short range communication, wherein the first and second modes are characterized by different radio frequency ranges,” “a biometric sensor, financial transactions made using the circuits being responsive to the biometric sensor.” *Id.*, 61. Regarding the limitation “a biometric sensor, financial transactions made using the circuits being responsive to the biometric sensor, wherein the circuits are configured to approve the financial transactions responsive to the biometric sensor,” Applicant argued that this limitation is not indefinite, because “[t]here are a variety of ways in which the biometric sensor may be required for approval. For example, to retrieve a password or authorization code, to compare biometric data retrieved using the sensor to a

stored biometric (key), to change between ON states of the device, to unlock the cellular telephone, etc. One or more of these are discussed in the specification.” *Id.* Regarding the Examiner’s §102 rejection, Applicant argued that Sinnreich does not disclose “a cellular telephone...configured to use two or more different wireless communication modes,” “a biometric sensor, financial transactions made using the circuits being responsive to the biometric sensor, wherein the circuits are configured to approve the financial transactions responsive to the biometric sensor,” or “an inductive antenna configured for communication of signals in the second mode.” *Id.*, 62.

1. (Currently Amended) A cellular telephone configured to use two or more different wireless communication modes, the cellular telephone comprising: circuits configured to operate in a first <u>wireless</u> mode for cellular operation and in a second <u>wireless</u> mode for short range communication, wherein the first and second modes are characterized by <u>use of</u> different radio frequency ranges <u>and</u> <u>the circuits are configured to perform financial transactions;</u> a biometric sensor, ~~financial transactions made using the circuits being responsive to the biometric sensor;~~ wherein the circuits are configured to approve the financial transactions responsive to the biometric sensor; and an inductive antenna configured for communication of signals in the second mode.

Id., 58.

Thereafter, on May 30, 2024, the Office issued a Notice of Allowance for all pending claims 1, 3, and 5–22. *Id.*, 3–10.

IV. LEVEL OF ORDINARY SKILL IN THE ART

A Person of Ordinary Skill in the Art (“POSITA”) at the time of the ’396 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*

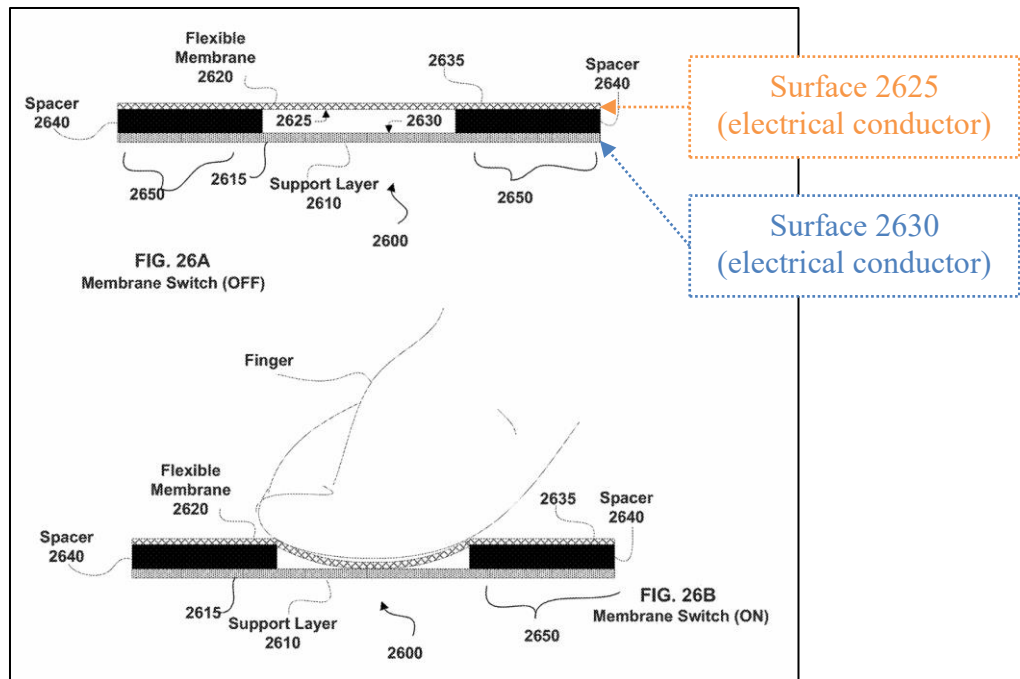
The following terms, which Petitioners identify for construction, were construed in prior litigation involving U.S. Patent No. 7,924,156, which is related to the ’396 Patent and is also asserted in *SureCell Transactions LLC v. Samsung Electronics Co., Ltd.*, No. 2:26-cv-00106 (E.D. Tex.):

Term	Proposed Construction
Responsive	Plain and ordinary meaning
Switch	A control device that makes or breaks an electrical connection in a circuit

EX1022, 15.

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.” EX1006, 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.



EX1006, FIGs. 26A–B.

VI. SUMMARY OF PRIOR ART

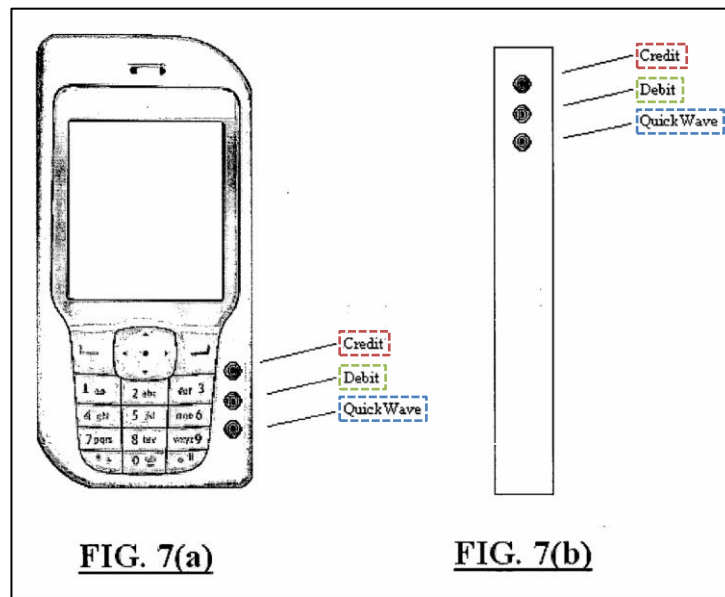
Petitioners assume, without conceding, that claims 1–20 of the ’396 Patent (“Challenged Claims”) are entitled to a May 6, 2005 priority date and are subject to pre-AIA provisions.

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.

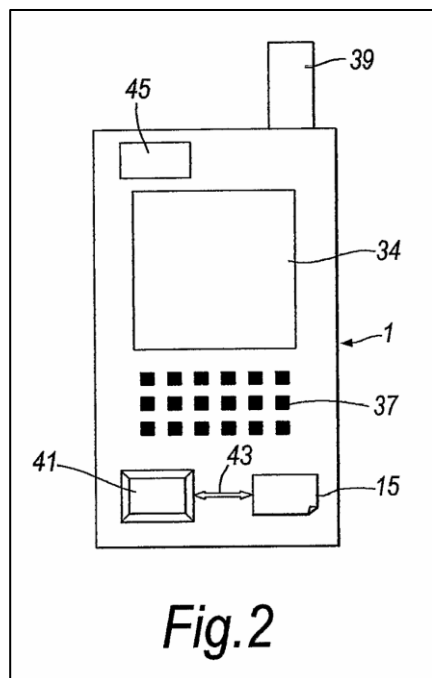
B. *WATERS* (EX1024)

U.S. Patent Publication No. 2009/0215385 (“*Waters*”) 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 1-10 AND 12-20

i. Independent Claim 1

1[pre]: cellular telephone configured to use two or more different wireless communication modes

Dua discloses that its device can be a “mobile telephone,” which a POSITA would understand to be a cellular telephone. EX1023, Abstract, [0026]; EX1014, ¶¶571-72. *Dua* further discloses that the device “is capable of wirelessly connecting

to the Internet using network protocols such as GSM/GPRS, CDMA2000, W-CDMA, EDGE, HDR, 1xRTT, UMTS, IMT-2000, 802.11a, 802.11b, 802.11g, or BLUETOOTH or other relevant protocols developed hereinafter.” *Id.*, [0041], [0314]–[0323]. GSM/GPRS, CDMA2000, W-CDMA, EDGE, HDR, 1xRTT, UMTS, and IMT-2000 are cellular communication protocols, and 802.11a, 802.11b, and 802.11g are WiFi communication protocols. EX1014, ¶¶571-72. Additionally, *Dua*’s device is equipped with an RFID interface, which enables short-range RFID communication. EX1023, [0378], [0383], [0495]. Each of these communication modes is wireless. EX1014, ¶¶571-72.

Thus, *Dua* discloses 1[pre].

1[a]: circuits configured to operate in a first wireless mode for cellular operation and in a second wireless mode for short range communication

A POSITA would understand that the wireless device running the wallet application that enables communication with the embedded communications interfaces necessarily includes processing and control circuitry (a circuit) that executes the wallet application and controls the embedded communications interfaces or smart card. EX1014, ¶¶573-74.

Thus, as explained above with 1[pre], *Dua* discloses 1[a].

1[b]: the first and second modes are characterized by use of different radio frequency ranges and the circuits are configured to perform financial transactions

Dua's cellular mode operates at a different frequency than its RFID mode. *Dua* discloses that the **cellular** communication functionality (first mode) can be compliant with the GSM/GPRS, CDMA2000, W-CDMA, EDGE, HDR, 1xRTT, UMTS, or IMT-2000 protocols. EX1023, [0041]. *Dua* additionally discloses that its device is also compliant with ISO/IEC 14443, which was a known **RFID** communication protocol (second mode) at the time of invention. *Id.*, [0013]. The GSM protocol for cellular communication operates at 800 MHz, 900 MHz, 1800 MHz, and 1900 MHz, while ISO/IEC 14443 specifies RFID communication operating at 13.56 MHz. EX1014, ¶¶575-77; EX1033, 108; EX1032, 3. Thus, the cellular mode (first wireless mode) and RFID mode (second wireless mode) use different radio frequency ranges. *See also supra* §§VII.A.i.1[pre]–[a].

Further, *Dua* discloses that the circuits are configured to perform financial transactions. For example, *Dua* discloses that the circuits of the device can be used to transmit payment information. EX1023, [0041], [0296]–[0306].

Thus, *Dua* discloses 1[b].

1[c]: a biometric sensor, wherein the circuits are configured to approve the financial transactions responsive to the biometric sensor

Dua discloses that its device can include an integrated fingerprint scanner (biometric sensor), such that the device can “use a fingerprint...to authenticate a user to the wallet application” which enables transmission of payment information. *Id.*, [0366], [0395], [0414].

Thus, *Dua* inherently discloses 1[c].

1[d]: an inductive antenna configured for communication of signals in the second mode

As discussed above with reference to 1[pre] and 1[a], *Dua*’s device can operate in an RFID mode (second wireless mode), in which RFID signals are communicated. *See supra* §§VII.A.i.1[pre]–[a]. While *Dua* does not expressly disclose “an inductive antenna,” *Dua*’s disclosure of RFID technology renders inherent or obvious an inductive antenna for communication in the second mode, because RFID technology uses an RFID antenna (using inductive coupling) to enable such RFID communication. EX1014, ¶¶579-80; EX1031, 7-10.

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

Accordingly, *Dua* discloses, or otherwise renders obvious, each element of independent Claim 1. EX1014, ¶581.

ii. **Dependent Claims 2–10 and 12–20**

Claim 2[a]: a mechanical switch configured to approve the financial transactions

Dua discloses that, in addition to the fingerprint sensor, the device can include a “wallet button” (mechanical switch) that can “control the transmission of information to an external device via RFID.” EX1023, [0383]–[0385]. Specifically, when the wallet button (mechanical switch) is pressed, RFID communication is enabled, such that a transaction can be carried out by the device. *Id.*, [0383], [0385]. *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, ¶582; *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, *Dua* discloses 2[a].

Claim 2[b]: the financial transactions are responsive to both the biometric sensor and the mechanical switch

Dua discloses that the fingerprint sensor (biometric sensor) and wallet button (mechanical switch) can be implemented together, such that both are required to carry out a transaction. Specifically, *Dua* discloses that when the wallet button is pressed, “the application is ready to communicate with a reader, and simultaneously prompts the user for his Wallet PIN.” EX1023, [0384]. *Dua* further discloses that

the PIN authentication mechanism can be replaced with a fingerprint sensor (biometric sensor). *Id.*, [0366] (“wireless device[s] with embedded biometric technologies could use a fingerprint in lieu of a PIN code to authenticate a user to the wallet application”), [0414] (“a user may be prompted to scan his fingerprint using an integrated scanner in the wireless device 800 instead of inputting a PIN”). Accordingly, when the wallet button (mechanical switch) is pressed, *Dua*’s device can enable RFID communication and require successful authentication via the fingerprint sensor (biometric sensor) before a financial transaction is carried out.

Thus, *Dua* discloses 2[b].

Claim 3: the financial transactions are performed in the second mode

Dua discloses that in the RFID mode (second wireless mode), the cellular phone “can transmit payment...information to a reader” using RFID communication. *Id.*, [0315], [0383]–[0395].

Thus, *Dua* discloses Claim 3.

Claim 4: the financial transactions are performed in the first mode

Dua also discloses that in the cellular mode (first wireless mode), “transactions are conducted with a remote server over a wireless network” using cellular communication. *Id.*, [0041], [0323], [0497].

Thus, *Dua* discloses Claim 4.

Claim 5: the circuits are configured to communicate the financial transactions over WiFi

Dua discloses that “[c]onnectivity between the wireless device and the reader/POS terminal could be made via 802.11a/b/g [(WiFi)]...protocols.” *Id.*, [0318]; EX1014, ¶¶588-89. Such connectivity can include “facilitat[ing] transactions.” EX1023, [0333].

Thus, *Dua* discloses Claim 5.

Claim 6: the circuits are configured to communicate the financial transactions over a cellular network

Dua discloses Claim 6 for the same reasons discussed above, with reference to Claim 4. *See supra* §VII.A.ii (Claim 4).

Claim 7: the circuits are configured to communicate with a point-of-sale device in the second mode to perform the financial transactions

Dua discloses Claim 7 for the same reasons discussed above with reference to Claim 3. *See supra* §VII.A.ii (Claim 3); EX1023, [0318] (the “reader” discussed with reference to Claim 3 is a “POS” (point-of-sale) device), [0361].

Claim 8: a user interface configured to enter a credit or debit card number

Dua’s device is equipped with a key pad (a type of user interface) “for alphanumeric and special character input.” EX1023, [0041]. 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, it would have been obvious to a POSITA that *Dua*'s key pad (user interface) could be configured to enter credit card or debit card account data (credit or debit card number). EX1014, ¶592.

Thus, *Dua* renders obvious Claim 8.

Claim 9: a user interface configured for a user to select between financial accounts

Dua discloses that its device includes a "Credential Selector" (user interface), which "allows for one credential or multiple credentials to be selected from the credential tree...for transmission to a reader device." EX1023, [0371]. *Dua* further explains that "[u]sers can scroll through the credential tree and select credentials by using the visual navigation system of the wallet application and designated buttons on the wireless device for making selections. The credential tree as it appears in the 'Credential Selector' screen may provide visual information about the credentials to aid a user in the selection of specific credentials." *Id.*, [0371], FIGs. 6A, 7A (showing the device's (1) display screen, which a POSITA would understand to display the "visual navigation system of the wallet application," and (2) up, down, left, and right buttons, which a POSITA would understand to be used to "scroll through the credential tree and select credentials"); EX1014, ¶593. The disclosed credentials can include credit and debit card accounts (financial accounts). EX1023, [0048], [0297]–[0306], [0336].

Thus, *Dua* discloses Claim 9.

Claim 10: a user interface configured for a user to enter amounts of the financial transactions

Dua discloses that its device can facilitate “person-to-person, person-to-company, or company-to-company electronic payments or fund transfers.” *Id.*, [0048], [0311]. Such functionality includes a “mechanism by which a user could transfer funds to another user.” *Id.*, [0311]. *Dua* further explains that an “an over-the-air reload tool” associated with a stored value credential can be programmed into the wallet application. EX1023, [0293]. It would have been obvious to a POSITA that these mechanisms would include a user interface (for example, *Dua*’s display screen showing a transaction amount field, in combination with *Dua*’s key pad, with which the user can enter an amount into the field) for a user to enter an amount of money to transfer to another user, company, or reload card, as the device would require such information, in order to facilitate a transaction. EX1023, [0041]; EX1014, ¶¶594-95.

Thus, *Dua* renders obvious Claim 10.

Claim 12: encryption logic configured to encrypt data prior to transmission of the data

Dua’s device is equipped with “[c]ryptographic functions” (encryption logic), such that it can “transfer encrypted credentials.” EX1023, [0050], [0263]–[0269], [0318]. Specifically, *Dua* discloses that the “credentials transmitted from the

wireless device to the reader may be encrypted using the issuer's encryption key (that may have been provided during the issuance process or through other means).” *Id.*, [0362].

Thus, *Dua* discloses Claim 12.

Claim 13: keys within the cellular phone configured to turn on and off transmission in the second mode

Dua discloses that its device (cellular phone) stores reader keys (keys), which enable and disable transmission of certain data in the RFID mode (second wireless mode). Specifically, *Dua* discloses that a reader key is transmitted by a credential issuer to the device during the issuance process of a credential that is associated with the reader key. *Id.*, [0353], [0365]. The key is then stored in the wireless device's memory. *Id.*, [0354]. At the start of a transaction, an RFID reader associated with the issuer transmits its key to the wireless device. *Id.* The wireless device then passes the key to the wallet application, 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]. Then, if there is a successful match, the wallet application completes a transaction using the associated credential. *Id.*

Thus, *Dua* discloses Claim 13.

Claim 14: keys within the cellular phone configured to operate a lock in the second mode

Dua discloses that its device can store credentials including “[e]lectronic keys for offices, apartments, parking garages, cars, and other secure facilities.” *Id.*, [0340]. *Dua* further discloses that the RFID communications technology incorporated in its device is “typically used for...access control.” *Id.*, [0011]. It would have been obvious to a POSITA that *Dua*’s electronic keys (keys) would be configured to operate a lock in the RFID mode (second wireless mode), because locks are used to control access to “offices, apartments, parking garages, cars, and other secure facilities.” *Id.*, [0340]; EX1014, ¶¶600-01.

Thus, *Dua* renders obvious Claim 14.

Claim 15: memory configured to store a first financial account identifier and a second financial account identifier, the first and second financial account identifiers being identifiers of different financial [sic] accounts

Dua discloses that its device is equipped with memory, which can store the following information for each credential: “Name of credential,” “Account specific information,” “Account number,” “Special security information related to credential,” and “‘Reader Key’ for credential.” EX1023, [0295], [0297]–[0306], [0412]. Each of these information categories corresponds to a “financial account identifier,” because they are unique to a respective financial account, and thus, the financial account can be identified by the information. EX1014, ¶¶602-03. *Dua*

further discloses that its device can store multiple credentials associated with different financial accounts, for example, a credit card account and a debit card account. EX1023, [0336]–[0345], [0392]–[0393].

Thus, *Dua* discloses Claim 15.

Claim 16: the circuits are further configured to unlock a car

Dua renders obvious Claim 16 for the same reasons discussed above, with respect to Claim 14. *See supra* §VII.A.ii (Claim 14).

Claim 17: the circuits include an identity device, the identify [sic] device including a driver’s license

Dua discloses that its device can store credentials including a “[d]river’s license.” EX1023, [0048], [0056], [0180], [0342]. *Dua*’s credentials can correspond to an “identity device,” because they can be used to identify an individual person. EX1014, ¶¶605-06.

Thus, *Dua* discloses Claim 17.

Claim 18: recognition of a biometric is required to approve the financial transaction

Dua discloses Claim 18 for the same reasons discussed above, with reference to 1[c]. *See supra* §VII.A.i.1[c].

Claim 19[a]: the biometric sensor is configured to switch between first and second ON modes of the circuits

Dua discloses that when a user is authenticated by the fingerprint sensor (biometric sensor), an authenticated transmission can be enabled, wherein the device

can transmit any credential. EX1023, [0366], [0395], [0414]. *Dua* further discloses that when a user is not authenticated by the fingerprint sensor (biometric sensor), an unauthenticated transmission can be enabled, wherein the device can only transmit a credential associated with a reader key. EX1023, [0354], [0366], [0370], [0383], [0414]. The authenticated and unauthenticated modes correspond to first and second ON modes, respectively, because different credentials can be transmitted in each mode. EX1014, ¶608.

Thus, *Dua* discloses 19[a].

Claim 19[b]: the financial transactions are approved in the first ON mode but not approved in the second ON mode

Dua discloses that “a slight risk” is assumed by a user when designating a credential for unauthenticated use, and that “[e]ach individual will have their own risk tolerance and as such will want the flexibility to designate specific credentials in their wallet as requiring advance [authentication] and others to function without [authentication].” EX1023, [0368]. Accordingly, in view of this risk, it would have been obvious to a POSITA that a user would require authentication for sensitive payment credentials, such as credit cards and debit cards, and would not designate such credentials for unauthenticated use. EX1014, ¶¶609-11; *see* EX1023, [0336]–[0343], [0392].

Thus, *Dua* renders obvious 19[b].

Claim 20: the circuits are configured to communicate the financial transactions using RFID

Dua discloses Claim 20 for the same reasons discussed above, with reference to Claim 3. *See supra* §VII.A.ii (Claim 3).

B. GROUND 3: *DUA* IN VIEW OF *WOIKE* RENDERS OBVIOUS CLAIM 11

i. Motivation to Combine

Dua and *Woike* are both directed to electronic systems for conducting financial transactions using portable electronic devices. EX1014, ¶613. *Dua* discloses a mobile device wallet application that uses RFID technology for contactless payments. EX1023, [0011], [0336], [0383]. *Woike* discloses a method for contactless payments using a mobile telephone and a computer. EX1025, Abstract, p. 2, ll. 14-16.

A POSITA would have been motivated to combine the wireless device of *Dua* and the methods of *Woike* because the methods of *Woike* allow the wireless device of *Dua* to be used without requiring a merchant “to set up an expensive and complex payment system with a card reader.” *Id.*, p. 2, 28-29. “Another advantage is that the previously required printout and signing of receipts, filling out checks, or entering a PIN code is no longer necessary, thus preventing long lines at checkout. A connection to the authorization computer and entering of the ID number of the payment receiver can be completed by the purchaser shortly before paying, such that the purchaser only has to enter and verify the amount in the cell phone.” *Id.*, p. 3, ll.

7-12. Implementing these methods with the mobile device and wallet application of *Dua* would allow *Dua*'s mobile device to facilitate contactless transactions with a broader group of vendors and in a broader range of environments. EX1014, ¶¶613.

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. **Claim 11: a slot of the cellular telephone configured to accept a memory device configured to store a key, the key being configured to allow the cellular phone to engage in the financial transactions**

Dua's wireless device discloses and/or renders obvious the limitations of claim 1, from which claim 11 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 (key) is a separate component that is mechanically inserted into a SIM slot of a cellular phone, such as *Dua*'s device. EX1014, ¶¶614-15.

Woike explains that the SIM card requires a stored PIN, which prevents misuse of its payment methods. EX1025, p. 2, ll. 24-26. It would have been obvious to a POSITA that the PIN included in *Woike*'s SIM is used to authenticate a user prior to facilitating the described financial transactions. EX1014, ¶¶614-15. When implementing the methods of *Woike* using the mobile device of *Dua*, a PIN stored in a SIM can be used to authenticate a user and permit use of *Dua*'s wallet application to facilitate a financial transaction. *Id.*

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

C. GROUND 4: *WATERS* IN VIEW OF *DUA* RENDERS OBVIOUS CLAIMS 1–4, 6–20

i. Motivation to Combine

Waters and *Dua* are both directed to mobile payment systems using wireless communication technology. EX1014, ¶616. *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, ¶616.

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, ¶616. 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]: cellular telephone configured to use two or more different wireless communication modes

Waters discloses that its device is a “[m]obile terminal...registered with [a] GSM/GPRS or UMTS (3G) mobile or cellular telecommunications network,” which a POSITA would understand to be a cellular telephone. EX1024, [0020]; EX1014, ¶¶617-18. *Waters* further discloses that its device additionally “includes a near field or RFID tag...[that] operates in the unregulated RF band of 13.56 MHz.” *Id.*, [0034].

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

1[a]: circuits configured to operate in a first wireless mode for cellular operation and in a second wireless mode for short range communication

A POSITA would understand that *Waters*’s device running *Dua*’s wallet application that enables communication with *Waters*’s communications interfaces necessarily includes processing and control circuitry (a circuit) that executes the wallet application and controls the embedded communications interfaces or smart card. EX1014, ¶¶619-20.

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

² *Dua* also discloses and/or renders obvious each limitation of Claims 1–10 and 12–20 for the reasons discussed above in Grounds 1–2. *See supra* §VII.A.

1[b]: the first and second modes are characterized by use of different radio frequency ranges and the circuits are configured to perform financial transactions

As discussed above with reference to Grounds 1–2, cellular communications, such as GSM/GPRS communications, use a different radio frequency range than RFID communications. *See supra* §VII.A.i.1[b]. Thus, the cellular mode (first wireless mode) and RFID mode (second wireless mode) use different radio frequency ranges. *See also supra* §§VII.C.ii.1[pre]–[a].

Further, *Waters* discloses that the circuits are configured to perform financial transactions. For example, *Waters* discloses that the circuits of the device can be used to transmit payment information. EX1024, [0041]–[0045].

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

1[c]: a biometric sensor, wherein the circuits are configured to approve the financial transactions responsive to the biometric sensor

Similar to the disclosure of *Dua*, which is discussed above with reference to Grounds 1–2, *Waters* discloses that its device can include a fingerprint reader (biometric sensor), which can be used to authenticate a user and enable RFID communication of payment information. *See supra* §VII.A.i.1[c]; EX1024, [0041]–[0045], [0051].

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

1[d]: an inductive antenna configured for communication of signals in the second mode

Waters discloses that its device includes “an inbuilt inductive antenna” that enables RFID communication in the RFID mode (second wireless mode). EX1024, [0035].

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

Accordingly, *Waters-Dua* renders obvious each element of independent Claim 1. EX1014, ¶627.

iii. Dependent Claims 2–4, 6–20

Claim 2[a]: a mechanical switch configured to approve the financial transactions

Similar to the disclosure of *Dua*, which is discussed above with reference to Grounds 1–2, *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, ¶628; *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 2[a].

Claim 2[b]: the financial transactions are responsive to both the biometric sensor and the mechanical switch

Waters discloses that both the fingerprint reader (biometric sensor) and the pressure sensor (mechanical switch) can be implemented “in series.” *Id.*, [0056]. Accordingly, RFID communication can be enabled only when a user is first successfully authenticated by the fingerprint reader (biometric sensor) and then subsequently presses the pressure sensor (mechanical switch). *Id.*, [0051], [0053], [0056].

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

Claim 3: the financial transactions are performed in the second mode

Waters discloses that in the RFID mode (second wireless mode), payment information can be transmitted to a reader using RFID communication. *Id.*, [0041]–[0045].

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

Claim 4: the financial transactions are performed in the first mode

As discussed above with reference to Grounds 1–2, *Dua*’s wallet application controls a cellular telephone to perform financial transactions using cellular

communication. *See supra* §VII.A.ii (Claim 4). Accordingly, it would have been obvious to a POSITA that in the *Waters-Dua* combination, which implements the wallet application of *Dua* in the cellular telephone of *Waters*, the wallet application would control the device to perform financial transactions using cellular communication. EX1014, ¶¶632-34; *see supra* §VII.C.ii.1[pre] (the device of *Waters* is configured for cellular communication).

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

Claim 6: the circuits are configured to communicate the financial transactions over a cellular network

Waters-Dua renders obvious Claim 6 for the same reasons discussed above, with reference to Claim 4. *See supra* §VII.C.iii (Claim 4).

Claim 7: the circuits are configured to communicate with a point-of-sale device in the second mode to perform the financial transactions

Waters-Dua renders obvious Claim 7 for the same reasons discussed above, with reference to Claim 3. *See supra* §VII.C.iii (Claim 3).

Claim 8: a user interface configured to enter a credit or debit card number

As discussed above with reference to Grounds 1–2, it would have been obvious to a POSITA that *Dua*’s key pad would be used to enter a credit or debit card number, such that the number could be received and stored by *Dua*’s wallet application. *See supra* §VII.A.ii (Claim 8). *Waters* discloses that its device also includes a key pad (a type of user interface). EX1024, [0034]. Accordingly, it would

have been similarly obvious to a POSITA that in the *Waters-Dua* combination, the key pad of *Waters*'s device would be configured for a user to enter a credit or debit card number, such that the number could be received and stored by *Dua*'s wallet application, which is implemented on *Waters*'s device. EX1014, ¶637.

Thus, *Waters-Dua* renders obvious Claim 8.

Claim 9: a user interface configured for a user to select between financial accounts

As discussed above with respect to Grounds 1–2, *Dua*'s wallet application includes a “Credential Selector” (user interface), which “allows for one credential or multiple credentials to be selected from the credential tree...for transmission to a reader device.” EX1023, [0371]. These credentials can include credit and debit card account information (financial accounts). *Id.*, [0048], [0297]–[0306], [0336].

Thus, *Waters-Dua* renders obvious Claim 9.

Claim 10: a user interface configured for a user to enter amounts of the financial transactions

As discussed above with respect to Grounds 1–2, *Dua*'s wallet application controls a device to facilitate person-to-person, person-to-company, or company-to-company electronic payments or fund transfers, and it would have been obvious to a POSITA that such functionality would require a user interface for a user to enter an amount of money to transfer to another party. *See supra*, §VII.A.ii (Claim 10); EX1014, ¶¶639–41. For the same reasons, it would have been similarly obvious to a

POSITA that the wallet application in the *Waters-Dua* combination would include such a user interface, such that the wallet application can control the device to facilitate peer-to-peer payments. *Id.*

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

Claim 11: a slot of the cellular telephone configured to accept a memory device configured to store a key, the key being configured to allow the cellular phone to engage in the financial transactions

Waters discloses that RFID communication can be enabled responsive to PIN authentication. EX1024, [0051]. Specifically, a PIN entered by a user can be compared to a PIN (key) stored on a SIM (memory device). *Id.* If the PINs match, RFID communication can be enabled (the cellular phone can engage in financial transactions). *Id.* Further, as discussed above with reference to Ground 3, a SIM is a separate component that is mechanically inserted into a SIM slot of a cellular phone, such as the *Waters-Dua* device. *See supra* §VII.B.ii; EX1014, ¶¶642-43.

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

Claim 12: encryption logic configured to encrypt data prior to transmission of the data

Waters discloses that “[i]t is...known to encrypt the communication between the [RFID] tag and the reader.” EX1024, [0004]. Accordingly, it would have been obvious to a POSITA to implement encryption logic to enable such encryption of data prior to transmission. EX1014, ¶¶644-45.

Thus, *Waters-Dua* renders obvious Claim 12.

Claim 13: keys within the cellular phone configured to turn on and off transmission in the second mode

As discussed above with reference to Grounds 1–2, *Dua*’s wallet application controls a device to store reader keys (keys), which are used to enable and disable communication of designated credentials in the RFID mode (second wireless mode). *See supra* §VII.A.ii (Claim 13).

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

Claim 14: keys within the cellular phone configured to operate a lock in the second mode

As discussed above with reference to Grounds 1–2, *Dua* discloses that its device can store credentials including “[e]lectronic keys for offices, apartments, parking garages, cars, and other secure facilities.” EX1023, [0340]. *Waters* similarly discloses that the RFID technology incorporated into its device is suitable for use “in obtaining entry to buildings.” EX1024, [0002]. Accordingly, similar to Grounds 1–2, it would have been obvious to a POSITA that the *Waters-Dua* device would store electronic keys (keys) that are configured to operate a lock in the RFID mode (second wireless mode), because locks are typically used to control access to offices, apartments, parking garages, cars, buildings, and other secure facilities. EX1014, ¶¶647-48.

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

Claim 15: memory configured to store a first financial account identifier and a second financial account identifier, the first and second financial account identifiers being identifiers of different financial [sic] accounts

As discussed above with reference to Grounds 1–2, *Dua* discloses that its wallet application stores in memory the following information categories, each of which corresponds to a “financial account identifier”: “Name of credential,” “Account specific information,” “Account number,” “Special security information related to credential,” and “‘Reader Key’ for credential.” *See supra* §VII.A.ii (Claim 15). *Dua* further discloses that its device can store multiple credentials associated with different financial accounts, for example, a credit card account and a debit card account. EX1023, [0336]–[0345], [0392]–[0393].

Thus, *Waters-Dua* renders obvious Claim 15.

Claim 16: the circuits are further configured to unlock a car

Waters-Dua renders obvious Claim 16 for the same reasons discussed above, with respect to Claim 14. *See supra* §VII.C.iii (Claim 14).

Claim 17: the circuits include an identify [sic] device, the identify device including a driver’s license

As discussed above with reference to Grounds 1–2, *Dua* discloses that the wallet application can store a credential (identity device), including a “[d]river’s license.” *See supra* §VII.A.ii (Claim 17).

Thus, *Waters-Dua* renders obvious Claim 17.

Claim 18: recognition of a biometric is required to approve the financial transaction

Waters-Dua renders obvious Claim 18 for the same reasons discussed above, with reference to 1[c]. *See supra* §VII.C.ii.1[c].

Claim 19[a]: the biometric sensor is configured to switch between first and second ON modes of the circuits

As discussed above with reference to Grounds 1–2, *Dua*’s wallet application can control the device to operate in an authenticated mode and an unauthenticated mode, responsive to *Dua*’s fingerprint sensor. *See supra* §VII.A.ii (Claim 19[a]). *Waters* discloses a similar fingerprint reader. EX1024, [0051]. Accordingly, it would have been obvious to a POSITA that when implemented in the device of *Waters*, the wallet application would control the device to operate in an authenticated mode (first ON mode) and an unauthenticated mode (second ON mode), responsive to the fingerprint reader (biometric sensor). EX1014, ¶653; *see supra* §VII.A.ii (Claim 19[a]).

Thus, *Waters-Dua* renders obvious 19[a].

Claim 19[b]: the financial transactions are approved in the first ON mode but not approved in the second ON mode

As discussed above with reference to Grounds 1–2, it would have been obvious to a POSITA that a user would require authentication for sensitive payment credentials, such as credit cards and debit cards, and would not designate such credentials for use in the unauthenticated mode. *See supra* §VII.A.ii (Claim 19[b]).

Thus, *Waters-Dua* renders obvious 19[b].

Claim 20: the circuits are configured to communicate the financial transactions using RFID

Waters-Dua renders obvious Claim 20 for the same reasons discussed above, with reference to Claim 3. *See supra* §VII.C.iii (Claim 3).

VIII. CONCLUSION

For the foregoing reasons, Petitioners respectfully request that the Board institute *inter partes* review and cancel Claims 1–20 of the '396 Patent as unpatentable.

Respectfully submitted,

Dated: September 22, 2026

/ 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 7,358 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