

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. IPR2026-00510
U.S. Patent No. 11,989,612

**PETITION FOR INTER PARTES REVIEW OF U.S. PATENT NO.
11,989,612**

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.	'612 PATENT.....	2
	A. SPECIFICATION	2
	B. FILE HISTORY	2
IV.	LEVEL OF ORDINARY SKILL IN THE ART.....	4
V.	CLAIM CONSTRUCTION	4
	A. “RESPONSIVE”	4
	B. “SWITCH”	4
VI.	SUMMARY OF PRIOR ART.....	5
	A. <i>DUA</i> (EX1023).....	5
	B. <i>WATERS</i> (EX1024).....	7
VII.	INVALIDITY	8
	A. GROUNDS 1-2: <i>DUA</i>	8
	i. Independent Claim 1	9
	ii. Dependent Claims 2-5.....	15
	B. GROUND 3: <i>WATERS</i> IN VIEW OF <i>DUA</i> RENDERS OBVIOUS CLAIMS 1-5.....	17
	i. Motivation to Combine	18
	ii. Independent Claim 1	19
	iii. Dependent Claims 2-5.....	25
VIII.	CONCLUSION	29

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. 11,989,612 (“’612 patent”) is currently asserted by Patent Owner (“PO”) against Petitioners in the case styled: *SureCell Transactions LLC v. Samsung Electronics Co., Ltd.*, No. 2:26-cv-00106, (E.D. Tex), which was originally filed on February 12, 2026.

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

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

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

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

CLAIMS LISTING

Claim 1:

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

Claim 2:

2	The method of claim 1, wherein the cellular telephone includes the biometric sensor.
----------	--

Claim 3:

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

Claim 4:

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

Claim 5:

5	The method of claim 2, wherein the circuit is configured to communicate financial account information responsive to the biometric sensor.
----------	---

I. INTRODUCTION

The Office materially erred in granting U.S. Patent No. 11,989,612 (“the ’612 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 1–3 disclose or render obvious every claimed element of the ’612 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 ’612 Patent is eligible for IPR and that Petitioners are not barred or estopped from requesting IPR on Grounds 1-3.

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 1-5
Ground 2	<i>Dua</i> renders obvious claims 1-5
Ground 3	<i>Waters</i> with <i>Dua</i> renders obvious claims 1-5

III. '612 PATENT

A. SPECIFICATION

The '612 Patent relates to methods for performing a financial transaction using a switchable circuit to control communication of financial information using an inductive coupling. EX1001, Cl. 1. While the specification describes a switchable RFID tag, “[v]arious embodiments of the invention include a portable communication device such as a cellular telephone.” *Id.*, 9:63-64. The communication device includes a user interface used “to turn on or off operation of the RFID tag, to enter security data into the RFID tag, to enter financial information (e.g., a credit or debit card number[]) into the RFID tag, to enter an identifying number (e.g., telephone number) into the RFID Tag, or to enter account number into the RFID tag.” *Id.*, 10:11-17. The communication device is further “configured to use voice recognition to approve an RFID based financial transaction. For example, in some embodiments voice recognition authentication may be required before an RFID tag is activated.” *Id.*, 11:25-29.

B. FILE HISTORY

The '612 Patent issued on May 21, 2024 from App. No. 17/728,412 (the “'412 Application”), filed April 25, 2022. On its face, the '612 Patent purports to claim priority to a provisional application filed on May 6, 2005, and is subject to a terminal disclaimer over U.S. Patent No. 11,599,734 (the '734 Patent). *Id.* Independent claim 1 as originally presented recited:

What is claimed is:

1. A method of performing a financial transaction, the method comprising:

placing a cellular telephone within reading range of a wireless point of sale device, the cellular telephone being configured to communicate wirelessly using an inductive coupling, wherein the inductive coupling is responsive to 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 state of the circuit;

activating the electronic switch within the cellular telephone to change the state of the circuit, activation of the electronic switch being responsive to a biometric sensor; and

communicating financial account information from the cellular telephone to the point of sale device responsive to the state of the circuit to facilitate the financial transaction, the communication of the account information using the inductive antenna.

EX1011, 350.

In a first Non-Final Office Action dated January 19, 2024, the Examiner rejected all claims for nonstatutory double patenting over claims 1-14 of the '734 Patent. *Id.*, 45-47. The Examiner further rejected claims 6-8 as obvious over U.S. Patent No. 6,859,650 ("Ritter") in view of U.S. Patent Pub. No. 2001/0044321 ("Ausems"). *Id.*, 47-48. In response, Applicant filed a terminal disclaimer to the '734 Patent and cancelled claims 6-8. *Id.*, 39-41. On April 16, 2024, the Office issued a Notice of Allowance for all claims. *Id.*, 10-17.

IV. LEVEL OF ORDINARY SKILL IN THE ART

A Person of Ordinary Skill in the Art (“POSITA”) at the time of the ’612 Patent would have had either (i) a Master of Science in Electrical Engineering or an equivalent field, or (ii) a Bachelor of Science in Electrical Engineering or an equivalent field and two years of experience in the field of RFID communications. EX1014, ¶¶59-60.

V. CLAIM CONSTRUCTION

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

A. “RESPONSIVE”

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

B. “SWITCH”

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

VI. SUMMARY OF PRIOR ART

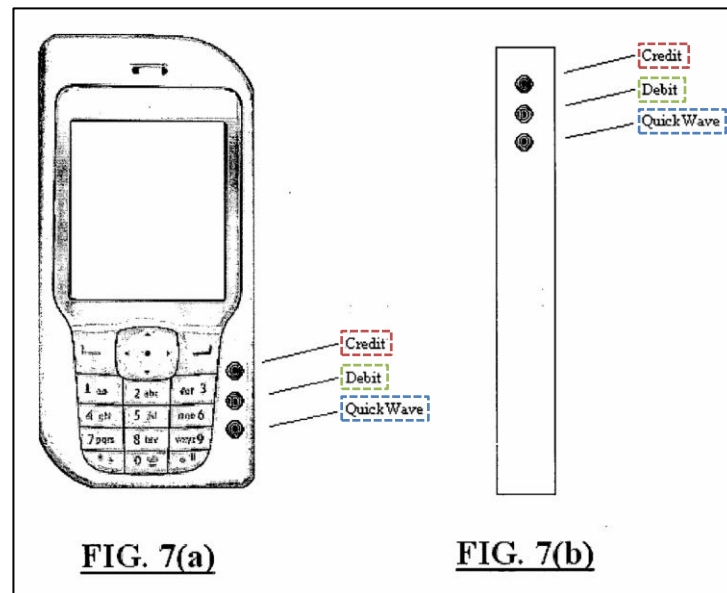
Petitioners assume, without conceding, that claims 1-5 of the '612 Patent ("Challenged Claims") are entitled to a May 6, 2005 priority date and are subject to pre-AIA provisions.

A. *DUA* (EX1023)

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

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

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



EX1023, FIG. 7.

B. *WATERS* (EX1024)

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

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

Id., FIG. 2.

A. GROUNDS 1-2: *DUA*

8

i. **Independent Claim 1**

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

To the extent the preamble is limiting, *Dua* discloses it. *Dua* describes a “mobile device” “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]: placing a cellular telephone within reading range of a wireless point of sale device,

Dua’s wireless device can be a cellular phone. *See id.*, FIG. 6, claim 92. *Dua* explains that “[d]uring a proximity transaction, the wireless device can transmit payment, identification, or other confidential information to a reader using the short-range transmission capability of the wireless device (e.g. RF).” EX1023, [0315]. For example, “a wireless device loaded with a wallet application, that also has an integrated RFID chip can simply be waved slowly in close proximity to a reader device to facilitate a transaction.” *Id.* The reader device is connected to “point of sale terminal 860.” *Id.*, [0405], FIG. 8. A POSITA would have understood *Dua*’s reader and associated point of sale terminal to be a “wireless point of sale device” as recited in Claim 1. EX1014, ¶548. Thus, *Dua* discloses Limitation 1[a].

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

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

Dua’s wireless device includes an RFID interface configured to carry out transactions using RFID communication. *Id.*, [0378]. *Dua* also explains that ISO/IEC 14443, which describes the use of inductive coupling antennas to facilitate contactless payments, was known in the art. *Id.*, [0013]; EX1014, ¶549.

While *Dua* does not expressly use the phrase “inductive coupling,” inductive coupling naturally flows from *Dua*’s disclosure of such RFID communication, in particular because of *Dua*’s disclosure of NFC technology. EX1014, ¶549.

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

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

Dua explains that “[t]he wallet application handles processing of incoming credentials and extensions, the execution of extensions within the wallet framework,

controlling access to secure storage, enabling communication with an embedded RF interface or smart card, and facilitating the use of operating system and hardware features such as display and sound.” EX1023, [0309]. As discussed above, inductive coupling naturally flows from *Dua*'s disclosure of such RFID communication, in particular because of *Dua*'s disclosure of NFC technology. See § VII.A.i.1[b]. A POSITA would understand that the wireless device running the wallet application that enables communication with the embedded RF interface (*i.e.*, using inductive coupling) necessarily includes processing and control circuitry (*i.e.*, a circuit) that executes the wallet application and controls the embedded RF interface or smart card. EX1014, ¶550.

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 biometric authentication mechanism necessarily includes an electronic switch that, in response to 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, ¶550. A POSITA would understand that the electronic switch, in response to biometric entry, makes or breaks an electrical connection in the circuit, causing

an electronic signal to change between the operative states of the circuit (*e.g.*, from disabled to enabled; from PIN-less to authenticated). EX1014, ¶550; EX1023, [0367] (describing PIN-less state), [0395] (describing disabled/enabled states), [0397] (describing authenticated state), [0414] (biometrics can be used in lieu of PINs). Thus, *Dua* discloses Limitation 1[c].

1[d]: configured to communicate via the inductive coupling responsive to a first of the states of the circuit;

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

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

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

Thus, because the circuit can transmit a PIN-less credential (*e.g.*, communicate less sensitive financial account information) in a PIN-less state and a biometric protected credential (*e.g.*, communicate more sensitive financial account information) in an authenticated state, *Dua* discloses Limitation 1[d]. EX1014, ¶551.

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

Dua discloses Limitation 1[e] for the reasons discussed above in § VII.A.i.1[c]. Specifically, a POSITA would understand that the biometric authentication mechanism taught by *Dua* necessarily discloses an electronic switch that, in response to a correct biometric entry, is activated to make or break an electrical connection in the processing or control circuitry that executes the wallet application and controls the embedded RF interface (*i.e.*, a circuit). EX1014, ¶552. A POSITA would further understand that the electronic switch, in response to biometric entry, makes or breaks an electrical connection in the circuit, causing an electronic signal to change between the operative states of the circuit (*e.g.*, from disabled to enabled; from PIN-less to authenticated). Thus, *Dua* discloses Limitation 1[e]. EX1014, ¶552.

1[f]: communicating financial account information from the cellular telephone to the point of sale device responsive to the first of the states of the circuit to facilitate the financial

transaction, the communication of the account information using the inductive antenna.

Dua discloses communication by the cellular telephone to the point-of-sale device responsive to the state of the circuit to facilitate a financial transaction using an inductive coupling. *See* §§ VII.A.i.1[Pre], 1[b]-1[d]. As discussed above, while *Dua* does not expressly use the phrase “inductive coupling,” inductive coupling naturally flows from *Dua*'s disclosure of such RFID communication, in particular because of *Dua*'s disclosure of NFC technology. *See* § VII.A.i.1[b]. RFID communication using inductive coupling necessarily requires an inductive antenna. EX1014, ¶¶553-55.

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]. In these cases, communication of financial account information is responsive to the state of the circuit as explained above. §§ VII.A.i.1[c], 1[e]. For example, communicating

payment information (*i.e.*, financial information) to the point-of-sale device using the inductive antenna can be responsive to an enabled state (*i.e.*, a first state) of the circuit. EX1014, ¶¶553-55. Thus, *Dua* discloses Limitation 1[f]. EX1014, ¶¶553-55.

Accordingly, *Dua* discloses or renders obvious each element of independent Claim 1. EX1014, ¶¶553-55.

ii. Dependent Claims 2-5

Claim 2: The method of claim 1, wherein the cellular telephone includes the biometric sensor.

Dua discloses every element of Claim 1. *See* § VII.A.i. *Dua* expressly contemplates that the biometric sensor resides in the wireless device itself, explaining that devices “with embedded biometric technologies could use a fingerprint in lieu of a PIN code to authenticate a user to the wallet application.” EX1023, [0366]. A POSITA would have understood “embedded biometric technologies” capable of fingerprint authentication (*e.g.*, a fingerprint sensor) to be a biometric sensor included in the cellular telephone. EX1014, ¶556. Thus, *Dua* discloses Claim 2. EX1014, ¶556.

Claim 3: The method of claim 2, wherein the circuit is configured to facilitate the financial transaction responsive to the biometric sensor.

Claim 5: The method of claim 2, wherein the circuit is configured to communicate financial account information responsive to the biometric sensor.

Dua discloses every element of Claim 2. *See* § VII.A.ii (Claim 2). *Dua*'s wallet is "the core" of the platform and "handles...enabling communication with an embedded RF interface," including performance of financial transactions. EX1023, [0309], [0315]. The "default security setting in the wallet application is that PIN-entry is required before the wallet application can be 'opened' and any credentials transmitted to an external device." EX1023, [0366]. *Dua* further discloses that the PIN-entry can be replaced with "a fingerprint in lieu of a PIN code to authenticate a user to the wallet application" in phones with "embedded biometric technologies." EX1023, [0366].

As identified in § VII.A.i, *Dua*'s "circuit" is the processing and control circuitry that executes the wallet application and controls the embedded RF interface or smart card. EX1014, ¶557. That circuitry is configured to facilitate the financial transaction and to communicate financial account information based on the functionality of the wallet application it executes. EX1014, ¶557. Thus, by making the wallet application functionality and transmission of financial credentials responsive to a fingerprint sensor, *Dua* discloses Claims 3 and 5. EX1014, ¶557.

Claim 4: The method of claim 2, wherein the circuit is configured to approve the financial transaction responsive to the biometric sensor.

Dua discloses every element of Claim 2. *See* § VII.A.ii (Claim 2). As noted above, *Dua* discloses that a biometric sensor can be used to enable financial transactions. *See* §§ VII.A.i.1[e], VII.A.ii (Claims 3 and 5). *Dua* also explains that “[t]he wallet application displays the PIN Approval Request received from Sample Bank, and prompts the user to enter his PIN in order to approve the transaction.” EX1023, [0419], Fig. 9. *Dua* further explains that “biometrics could also be used in lieu of PINs” in such verification methods. *Id.*, [0414] (“For example, a user may be prompted to scan his fingerprint using an integrated scanner in the wireless device **800** instead of inputting a PIN as described earlier.”).

As identified in § VII.A.i, *Dua*’s “circuit” is the processing and control circuitry that executes the wallet application and controls the embedded RF interface or smart card. EX1014, ¶558. That circuitry is configured to approve the financial transaction based on the functionality of the wallet application it executes. EX1014, ¶558. Thus, by making the wallet application’s user authentication and financial transaction approval responsive to a fingerprint sensor, *Dua* discloses Claim 4. EX1014, ¶558.

B. GROUND 3: *WATERS* IN VIEW OF *DUA* RENDERS OBVIOUS CLAIMS 1-5

i. Motivation to Combine

Waters and *Dua* are both directed to mobile payment systems using wireless communication technology. EX1014, ¶559. *Waters* discloses a mobile terminal including a near field or RFID tag, wherein the mobile terminal is operable to obtain security data from the user to confirm the identity of the user before enabling the near field tag to make a payment. EX1024, Abstract. *Dua* discloses a comprehensive mobile wallet application with RFID capabilities. See § VI.A; EX1023, [0011], [0336], [0383]. Both references address the goal of improving data security in RFID applications. EX1023, [0382]–[0383]; EX1024, [0049]–[0050], [0053]. Each of these references teaches that PIN or biometric authentication can be implemented to enable or disable RFID communication, to prevent skimming. EX1014, ¶559.

Both *Waters* and *Dua* address the problem of enabling secure financial transactions using mobile devices. EX1014, ¶559. *Waters* teaches using a mobile terminal with wireless capabilities to perform financial transactions using a near field tag read by a reader. EX1024, [0041]–[0045], [0052]. *Dua* provides detailed implementation of a wallet application with credential management and RFID communication. EX1023, [0295]–[0305], [0334]–[0347].

A POSITA would have been motivated to combine *Waters* with *Dua* because *Dua* provides detailed implementation guidance for the wallet application functionality that *Waters* describes at a higher level. EX1014, ¶559. Specifically,

Dua's detailed disclosures regarding credential storage, user authentication, and RFID communication would have provided a POSITA with implementation details for *Waters*'s mobile payment system to make it commercially useful. *Id.* Thus, a POSITA would have been motivated to incorporate *Dua*'s wallet application, including the processing and control circuitry that executes it (*see* § VII.A.i.1[c]), into the mobile terminal of *Waters*. *Id.* This combination would enable *Dua*'s wallet application and associated circuitry to provide additional functionality and control using the RFID enabling mechanisms and near field tag 41 of *Waters*'s mobile terminal. *Id.*

A POSITA would have had a reasonable expectation of success in combining these references because both describe compatible mobile payment technologies using RFID/NFC for contactless transactions. EX1014, ¶559. The combination would involve using *Dua*'s wallet application implementation within *Waters*'s mobile transaction framework. *Id.*

ii. **Independent Claim 1**

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

To the extent the preamble is limiting, *Waters* in view of *Dua* renders it obvious. *Waters* teaches a mobile terminal including a near field or RFID tag, wherein the mobile terminal is operable to facilitate financial transactions. EX1024,

Abstract (“use the near field tag (41) to make a payment”), [0045] (“use their RF tag to make payments”). Thus, *Waters* in view of *Dua* renders obvious 1[Pre].²

1[a]: placing a cellular telephone within reading range of a wireless point of sale device,

Waters states that its “mobile terminal 1 may be a handheld mobile telephone, a personal digital assistant (PDA) or a laptop computer equipped with a datacard.” *Id.*, [0020] (emphasis added). *Waters* explains that its RFID tag 41 can “exchange information with a tag reader when the two are brought into close proximity.” EX1024, [0035]. *Waters* further teaches that the mobile terminal can be used to “make a payment” at a reader (e.g., a point-of-sale terminal). *Id.*, Abstract; *see also id.*, [0041]–[0043], [0045]. A POSITA would understand that the tag reader disclosed in *Waters* corresponds to “a wireless communication device” as recited in Claim 1. EX1014, ¶561. Thus, *Waters* in view of *Dua* renders obvious Limitation 1[a].

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

Waters teaches that its device includes an “inbuilt inductive antenna” configured to “exchange information with a tag reader when the two are brought in close proximity.” EX1024, [0035]. *Waters* further explains its “near field tag 41 may operate in accordance with ISO-IEC 14443 and ISO-IEC 15693 standards.” *Id.* A

² *Dua* also discloses each limitation of Claims 1-5 for the reasons discussed above in Grounds 1-2. *See supra* § VII.A.

POSITA would understand that inductive coupling naturally flows from *Waters's* “near field tag” including an “inbuilt inductive antenna” operating “in accordance with ISO-IEC 14443 and ISO-IEC 15693 standards.” EX1014, ¶562. Thus, *Waters* in view of *Dua* renders obvious Limitation 1[b].

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

Dua explains that “[t]he wallet application handles processing of incoming credentials and extensions, the execution of extensions within the wallet framework, controlling access to secure storage, enabling communication with an embedded RF interface or smart card, and facilitating the use of operating system and hardware features such as display and sound.” EX1023, [0309]; *see also* § VII.A.i.1[c]. A POSITA would understand that the mobile terminal of *Waters* incorporating the wallet application of *Dua* that enables communication with the embedded RF interface necessarily includes processing and control circuitry (*i.e.*, a circuit) that executes the wallet application and controls the embedded RF interface or smart card (*i.e.*, comprising the inbuilt inductive antenna). EX1014, ¶563; *see also* §§ VII.A.i.1[c], VII.B.ii.1[b].

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

advantageously be combined with an RF tag **41** that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal **1** into proximity to the reader. After successful reading of the RF tag **41**, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal **1** is lost or stolen, an unauthorised person cannot use the RF tag **41**.” *Id.*, [0052]. It would have been obvious to a POSITA incorporating the wallet application of *Dua* into the mobile terminal of *Waters* to include the multiple ON states (*e.g.*, PIN-less state, authenticated state) discussed above (*see* §§ VII.A.i.1[c]-[d], VII.A.ii (Limitation 5[a]) controlled by these PIN and/or biometric authentication mechanism. EX1014, ¶563. A POSITA would understand that the biometric authentication mechanism necessarily includes an electronic switch that, in response to biometric entry, makes or breaks an electrical connection in the processing or control circuitry that executes the wallet application of *Dua* (*i.e.*, the circuit) and controls the embedded RF interface (*i.e.*, automatic deauthorization after use). EX1014, ¶563. A POSITA would further understand that the electronic switch, in response to biometric entry, makes or breaks an electrical connection in the circuit, causing an electronic signal to change between the operative states of the circuit (*e.g.*, from disabled to enabled; from PIN-less to

authenticated). EX1014, ¶563. Thus, *Waters* in view of *Dua* renders obvious Limitation 1[c].

1[d]: configured to communicate via the inductive coupling responsive to a first of the states of the circuit;

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

A POSITA would understand that the circuit identified in § VII.B.ii.1[c]—the processing or control circuitry that executes the wallet application of *Dua* and controls the embedded RF interface—is configured to communicate via inductive coupling 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 (*i.e.*, a first state), and it enters that state when the electronic switch identified in § VII.B.ii.1[c] is activated by correct biometric entry. *Id.*, [0051]-[0052]; EX1014, ¶564. A POSITA would further understand that, by incorporating the two ON states discussed above in § VII.B.ii.1[c], the circuit can transmit a PIN-less credential in a PIN-less state and a PIN/biometric protected credential in an authenticated state. EX1014, ¶564; *see also supra* § VII.A.i.1[d]. Thus, *Waters* in view of *Dua* renders obvious Limitation 1[d].

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

Waters discloses Limitation 1[e] for the reasons discussed above in § VII.B.ii.1[c]. Specifically, a POSITA would understand that the biometric authentication mechanism taught by *Waters* necessarily discloses an electronic switch that, in response to a correct biometric entry, is activated to make or break an electrical connection in the processing or control circuitry that executes the wallet application of *Dua* (*i.e.*, a circuit) and controls the embedded RF interface. EX1014, ¶565. A POSITA would further understand that the making or breaking of an electrical connection in the processing and control circuitry by the electronic switch changes between the states of the circuit (*e.g.*, from disabled to enabled; from PIN-less to authenticated). *Id.* Thus, *Waters* in view of *Dua* renders obvious Limitation 1[e].

1[f]: communicating financial account information from the cellular telephone to the point of sale device responsive to the first of the states of the circuit to facilitate the financial transaction, the communication of the account information using the inductive antenna.

Waters in view of *Dua* renders obvious communication by the cellular telephone to the point-of-sale device responsive to the state of the circuit to facilitate a financial transaction using an inbuilt inductive antenna. *See* §§ VII.B.ii.1[Pre], 1[b]-1[d].

A POSITA would have understood that to facilitate a financial transaction, financial account information would have to be exchanged between the cellular telephone and the wireless communication device, otherwise a vendor would not be able to charge the user's account. EX1014, ¶566. *Dua* also discloses this limitation. *See* § VII.A.i.1[f]. *Dua* explains that the wallet application “is specifically designed to store several types of electronic credentials,” including “Payment Methods” such as “[c]redit, debit/ATM, stored value, electronic check, and RFID payment methods.” EX1023, [0334], [0336]. The “credential record” contains “Account number” among other account-specific information. *Id.*, [0297], [0302]-[0304]. *Dua* further states that “[e]lectronic credentials issued to a user and stored in the wallet application can be used” in a proximity transaction, where “the wireless device can transmit payment, identification, or other confidential information to a reader using the short-range transmission capability of the wireless device (e.g. RF).” *Id.*, [0313]-[0315]. Thus, *Waters* in view of *Dua* renders obvious Limitation 1[f].

Accordingly, *Waters* in view of *Dua* renders obvious each element of independent Claim 1. EX1014, ¶567.

iii. Dependent Claims 2-5

Claim 2: The method of claim 1, wherein the cellular telephone includes the biometric sensor.

Waters in view of *Dua* renders obvious every element of Claim 1. *See* § VII.B.ii. *Waters* teaches that “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.” EX1024, [0051]. *Dua* likewise teaches devices “with embedded biometric technologies” that “could use a fingerprint in lieu of a PIN code to authenticate a user to the wallet application.” EX1023, [0366]. A POSITA would have understood the fingerprint reader of *Waters*’s mobile terminal to be a biometric sensor included in the cellular telephone. EX1014, ¶568. Thus, *Waters* in view of *Dua* renders obvious Claim 2.

Claim 3: The method of claim 2, wherein the circuit is configured to facilitate the financial transaction responsive to the biometric sensor.

Claim 5: The method of claim 2, wherein the circuit is configured to communicate financial account information responsive to the biometric sensor.

Waters in view of *Dua* renders obvious every element of Claim 2. *See* § VII.B.iii (Claim 2). *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, ¶569. *Dua* also discloses making its wallet application functionality and transmission of financial credentials responsive to a fingerprint sensor. *See supra* § VII.A.ii (Claims 3 and 5). *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.B.ii, the “circuit” is the processing and control circuitry that executes the wallet application of *Dua* and controls the embedded RF interface.

EX1014, ¶569. That circuitry is configured to facilitate the financial transaction and to communicate financial account information based on the functionality of the wallet application it executes. EX1014, ¶569. Thus, by making the wallet application functionality and transmission of financial credentials responsive to a fingerprint sensor, *Waters* in view of *Dua* renders obvious Claims 3 and 5.

Claim 4: The method of claim 2, wherein the circuit is configured to approve the financial transaction responsive to the biometric sensor.

Waters in view of *Dua* renders obvious every element of Claim 2. See § VII.B.iii (Claim 2). As noted above, *Waters* in view of *Dua* discloses or renders obvious that a biometric sensor can be used to enable financial transactions. §§ VII.B.ii.1[e], VII.B.iii (Claims 3 and 5). *Waters* states that “the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered.” EX1024, [0052]. *Waters* explains that in the disabled state, “a reader is not able to obtain any information from the near field tag 41” but when enabled, the tag “is then able to communicate with readers to allow use of” financial services. *Id.*, [0037], [0042]. This biometric authentication scheme is also disclosed by *Dua*, where the fingerprint sensor is used to “authenticate a user to the wallet application,” and the processing and control

circuitry executing that wallet application approves the transaction. *See* § VII.A.ii (Claim 4).

As identified in § VII.B.ii, the “circuit” is the processing and control circuitry that executes the wallet application of *Dua* and controls the embedded RF interface. EX1014, ¶570. That circuitry is configured to approve the financial transaction responsive to the biometric sensor based on the functionality of the wallet application it executes. EX1014, ¶570. Thus, by making the wallet application’s user authentication and financial transaction approval responsive to a fingerprint sensor, the combination of *Waters* in view of *Dua* renders obvious Claim 4.

VIII. CONCLUSION

For the foregoing reasons, Petitioners respectfully request that the Board institute *inter partes* review and cancel Claims 1-5 of the ’612 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 5,859 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