

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

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

Petitioners

v.

SURECELL TRANSACTIONS LLC,
Patent Owner

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

Case No. IPR2026-00508
U.S. Patent No. 11,599,734

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

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

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

DECLARATION OF DR. SAYFE KIAEI

TABLE OF CONTENTS

I.	INTRODUCTION	5
II.	EXPERIENCE AND QUALIFICATIONS.....	6
III.	MATERIALS CONSIDERED	10
IV.	LEGAL STANDARDS	13
	A. Anticipation	13
	B. Obviousness.....	14
	C. Claim Construction.....	16
V.	OVERVIEW OF THE '949, '734, '741, '612, AND '396 PATENTS.....	17
	A. Subject Matter of the '949, '734, '741, '612, and '396 Patents.....	17
	B. Prosecution Histories '949, '734, '741, '612, and '396 Patents	18
	1. The '949 Patent.....	18
	2. The '734 Patent.....	21
	3. The '741 Patent.....	22
	4. The '612 Patent.....	24
	5. The '396 Patent.....	25
	C. RFID Communication Devices	28
VI.	LEVEL OF ORDINARY SKILL IN THE ART	31
VII.	CLAIM CONSTRUCTION	32
VIII.	SUMMARY OF PRIOR ART.....	35
	A. <i>Waters</i> (EX1024).....	35
	B. <i>Dua</i> (EX1023)	39
	C. <i>Woike</i> (EX1025) (Secondary Reference).....	41
IX.	The '949 PATENT	41
	A. SUMMARY OF PRIOR ART GROUNDS.....	41

D.	GROUND 4: <i>Waters</i> in View of <i>Dua</i> Renders Obvious Claims 1–4, 6–20	209
XIV.	CONCLUSION.....	217

Declaration of Dr. Sayfe Kiaei

I. INTRODUCTION

1. I, Dr. Sayfe Kiaei, make this declaration based upon my own personal knowledge and, if called upon to testify, would testify competently to the matters contained herein.

2. I have been retained by counsel for Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, “Samsung” or “Petitioners”) in connection with the above-captioned request for *inter partes* review of claims 1–30 of U.S. Patent No. 11,347,949 (the “’949 Patent”), claims 1–30 of U.S. Patent No. 11,599,734 (the “’734 Patent”), claims 1–30 of U.S. Patent No. 11,687,741 (the “’741 Patent”), claims 1–5 of U.S. Patent No. 11,989,612 (the “’612 Patent”), and claims 1–20 of U.S. Patent No. 12,039,396 (the “’396 Patent”), by named inventor Steven M. Colby. I understand that the ’949, ’734, ’741, ’612, and ’396 Patents are assigned to SureCell Transactions LLC (the “Patent Owner”). I have been asked to provide technical review, analysis, insights, and opinions regarding the ’949, ’734, ’741, ’612, and ’396 Patents and the prior art references that form the basis for the grounds of invalidity set forth in the Petition for *inter partes* review of the ’949, ’734, ’741, ’612, and ’396 Patents (the “Petitions”). This declaration is a statement of my opinions on issues related to the unpatentability of the claims listed above of the ’949, ’734, ’741, ’612, and ’396 Patents.

3. I am being compensated at my normal rate of \$550 per hour, plus reimbursement for expenses, for my analysis. My compensation does not depend on the content of my opinions or the outcome of this proceeding. I have no other interests in this proceeding or with Petitioners or Patent Owner.

II. EXPERIENCE AND QUALIFICATIONS

4. In formulating my opinions, I have relied upon my knowledge, training, and experience in the relevant art. My qualifications are stated more fully in my curriculum vitae, which has been provided as EX1034. Here, I provide a brief summary of my qualifications and relevant information regarding my education, technical experience, and publications.

5. I received my Ph.D., M.S., and B.S. degrees, all in Electrical and Computer Engineering, in 1987, 1984, and 1982, respectively, from Washington State University. My M.S. and Ph.D. thesis was on the development of signal and audio processing filters and systems. My specialization was in signal processing, audio processing, communications, and integrated circuits for analog and digital signal processing.

6. I have been employed by Arizona State University since 2001 and currently hold the position of Motorola Endowed Chair Professor in Analog and Radio Frequency Integrated Circuitry at the School of Electrical, Computer, and Energy Engineering.

7. I am also the Director of the National Science Foundation Center “Connection One,” which is an industry/university cooperative research center with over thirty industrial members and five university members focused on developing communication system and networking technologies.

8. From 1987 through 1993, I was a Professor at Oregon State University (tenured) in the Electrical and Computer Engineering Department. In my over thirty years of teaching experience, I have taught courses in networking, communication systems, RF, and electronics.

9. From 1993 to 2001, I was a Senior Member of Technical Staff with the Wireless Technology Center and Broadband Operations at Motorola Inc. where I was responsible for the development of wireless system, cellular system, RF integrated circuits, GPS, and Digital Subscriber Lines (DSL) transceivers. From 1985 through 1987, I worked with Boeing on the development of signal processing and control systems. I have also been a consultant on various projects with Intel (designing 2G, 3G cellular transceivers), Texas Instrument (developing 3G cellular and Bluetooth technologies), Sony Wireless (developing GPS technologies), Tektronix (designing wireless systems), and various other consultancies.

10. From 1997-2001 I was the standards technical analyst for Motorola and attended various standard-setting committees, including ITU, IEEE, and ETSI related to DSL, OFDM, CDMA, 2G, and 3G systems. I was also involved with the

Bluetooth standards and Bluetooth working group.

11. I have graduated over 100 MS and PhD students working under my supervision on their thesis, and many of them are professors in academia, or have senior positions in the industry. Currently I have 8 MS, PhD and postdoc students working in my lab on research related to communication and networking systems, wireless and wireline systems, RF, and integrated circuits. My research is funded by various industry, federal agencies including NSF, DARPA, ONR, DOE, etc., with an average research funding of \$1M per year.

12. I have been involved with communication and networking systems, wireless and wireline systems, cellular systems, RF Integrated circuits, RFID, Analog and Digital Integrated Circuits, HDL, Verilog, VHDL, communications, digital signal processing, and related areas for the last 30 years. I have also worked on wireless cellular systems including 2G, 4G, CDMA, UMTS, wireless connectivity including Bluetooth, WiFi, and RFID and sensors. I have also worked on other wireless data communication technologies including Bluetooth, the global positioning system (GPS), Wireless local area networks (LAN) and related areas.

13. During my work in industry, I have designed and contributed to the design of many radio transceivers for commercial products, including designs for radio transceiver integrated circuits. Many of my designs are still in use today in products manufactured by the companies I have worked for, including Motorola,

Intel, Sony, and more.

14. I have published over a hundred journal and conference papers covering topics such as communication systems, signal processing, radio frequency, integrated circuits (IC), filter design, and related areas. A list of my publications can be found in my CV (EX1034).

15. I am an IEEE Fellow, a distinction and the highest level of IEEE membership awarded by the IEEE directors to recognize a high level of demonstrated extraordinary accomplishments. The IEEE is the Institute of Electrical and Electronics Engineers, the world's largest association of technical professionals whose objectives include the educational and technical advancement of electrical and electronic engineering, telecommunications, computer engineering, and related disciplines. I am a member of the IEEE Circuits and Systems Society, IEEE Solid State Circuits Society, and IEEE Communication Society, IEEE RF and Microwave committees, IEEE Low Power Symposium Committee, IEEE Signal Processing Society, IEEE Fellow Selection Committee, and many other International Electrical Engineering societies. I was one of the key organizers to establish the IEEE Radio Frequency Integrated Circuits (RFIC) symposium in 1995, and have been on the executive committee, and technical committee of RFIC for the last 16 years. The RFIC Symposium has grown and is now the premier international symposium in the world where the latest RF circuits and components are presented. I have been

involved in several international conferences in the areas of RF, Communication, Signal Processing, and IC design.

16. I have received several awards including the Carter Best Teacher Award, the IEEE Darlington Award (which is given for the best technical paper on circuits and systems in the IEEE Circuits and Systems Society), and the Motorola 10X Rapid Design Cycle Reduction Award.

17. My analyses set forth in this declaration are informed by my experience in the field of RFID communication. Based on my above-described experience, I am an expert in the field relevant to the '949, '734, '741, '612, and '396 Patents at issue here and have been an expert in the relevant field since before the claimed priority date of the '949, '734, '741, '612, and '396 Patents. I am familiar with how a person of ordinary skill in the art ("POSITA") would have understood and used the terminology found in the '949, '734, '741, '612, and '396 Patents before and at the time of their filing.

III. MATERIALS CONSIDERED

18. The analysis that I provide in this declaration is based on my education and professional experience, as well as the documents I have considered, including the '949, '734, '741, '612, and '396 Patents (EX1002-EX1006) and their respective prosecution histories (EX1008-EX1012). I have reviewed and am familiar with the specification of the '949, '734, '741, '612, and '396 Patents. I have reviewed and

am familiar with the prosecution histories of the '949, '734, '741, '612, and '396 Patents.

19. In preparing this declaration, I have also reviewed and am familiar with the following prior art used in the Petitions and this declaration. I have considered the following documents, and have also considered any other documents that are otherwise discussed in this declaration:

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	[Reserved]
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 Osai-fu-Keitai - CNBC Interview</i> , https://www.eurotechnology.com/2014/09/18/applepay-vs-osai-fu-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. 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	[Reserved]
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 (“ <i>Woike</i> ”), 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

IV. LEGAL STANDARDS

20. My opinions are also informed by my understanding of the relevant law. I understand that the patentability analysis is conducted on a claim-by-claim and element-by-element basis, and that there are several possible reasons that a patent claim may be found to be unpatentable.

21. I understand that earlier publications and patents may act to render a patent unpatentable for one of two reasons: (1) anticipation and (2) obviousness.

A. Anticipation

22. It is my understanding that the claims of a patent are anticipated by a prior art reference if each and every element of the claim is found either explicitly or inherently in a single prior art reference or system. I understand that inherency requires a showing that the missing descriptive matter in the claim is necessarily or implicitly present in the allegedly anticipating reference, and that it would have been so recognized by a POSITA. In addition, I understand that an enabling disclosure is a disclosure that allows a POSITA to make the invention without undue experimentation. Although anticipation typically involves the analysis of a single prior art reference, I understand that additional references may be used to show that the primary reference has enabling disclosure, to explain the meaning of a term used in the primary reference, and/or to show that a characteristic is inherent in the primary reference.

B. Obviousness

23. I understand that the prior art may render a patent claim “obvious.” I understand that two or more prior art references (e.g., prior art articles, patents, or publications) that each disclose fewer than all elements of a patent claim may nevertheless be combined to render a patent claim obvious if the combination of the prior art collectively discloses all elements of the claim and one of ordinary skill in the art at the time would have been motivated to combine the prior art in such a way. I understand that this motivation to combine need not be explicit in any of the prior art, but may be inferred from the knowledge of one of ordinary skill in the art at the time the patent was filed. I also understand that one of ordinary skill in the art is not an automaton, but is a person having ordinary creativity. I further understand that one or more prior art references, articles, patents or publications that disclose fewer than all of the elements of a patent claim may render a patent claim obvious if including the missing element would have been obvious to one of skill in the art (e.g., the missing element represents only an insubstantial difference over the prior art or a reconfiguration of a known system).

24. Under the doctrine of obviousness, a claim may be invalid if the differences between the invention and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a POSITA to which the subject matter pertains.

25. To assess obviousness, I understand that I am to consider the scope and content of the prior art, the differences between the prior art and the claim, the level of ordinary skill in the art, and any secondary considerations to the extent they exist.

26. I understand that there must be a nexus between any such secondary indicia and the claimed invention.

27. It is also my understanding that there are additional considerations that may be used as further guidance as to when the above factors will result in a finding that a claim is obvious, including the following:

- the claimed subject matter is simply a combination of prior art elements according to known methods to yield predictable results;
- the claimed subject matter is a simple substitution of one known element for another to obtain predictable results;
- the claimed subject matter uses known techniques to improve similar devices or methods in the same way;
- the claimed subject matter applies a known technique to a known device or method that is ready for improvement to yield predictable results;
- the claimed subject matter would have been “obvious to try” choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;

- there is known work in one field of endeavor that may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to a POSITA;
- there existed at the time of conception and reduction to practice a known problem for which there was an obvious solution encompassed by the patent's claims; and
- there is some teaching, suggestion, or motivation in the prior art that would have led a POSITA to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed subject matter.

28. Finally, I understand that a claim may be deemed invalid for obviousness in light of a single prior art reference, without the need to combine references, if the elements of the claim that are not found in the reference can be supplied by the knowledge or common sense of one of ordinary skill in the relevant art.

C. Claim Construction

29. I understand that "claim construction" is the process of determining a patent claim's meaning. I also understand that, during an *inter partes* review, claims are given their ordinary and accustomed meaning as understood by one of ordinary

skill in the art in view of the patent and its file history. I also understand that the claims of a patent must be interpreted in light of the specification—that is, the claim language itself, the written description, and the figures in the patent—as well as the patent’s prosecution history and/or any reexamination history. I understand that a patentee may act as his own lexicographer and clearly set forth a definition of the claim term in the specification. In such a case, the claim term will receive the definition set forth in the patent.

V. OVERVIEW OF THE ’949, ’734, ’741, ’612, AND ’396 PATENTS

30. I have reviewed the ’949, ’734, ’741, ’612, and ’396 Patents. I understand that the ’949, ’734, ’741, ’612, and ’396 Patents were filed between November 9, 2021 and January 25, 2024 and issued between May 31, 2022 and July 16, 2024. *See* EX1002-EX1006. For purposes of this declaration, I have been asked to assume that the ’949, ’734, ’741, ’612, and ’396 Patents have a priority date of May 6, 2005 based on a provisional application filed on that date.

31. I provide the following technology overview for context, the subject matter of which was well-known to persons of ordinary skill in the art before May 6, 2005.

A. Subject Matter of the ’949, ’734, ’741, ’612, and ’396 Patents

32. The ’949, ’734, ’741, ’612, and ’396 Patents share a specification. *See* EX1002-1006.

33. The '949, '734, '741, '612, and '396 Patents relate to an electronic communication system capable of communicating via an inductive coupling and/or an RF antenna, and methods of performing financial transactions using the same. *Id.*, Cl. 1. While the specification describes a switchable RFID tag, “[v]arious embodiments of the invention include a portable communication device such as a cellular telephone.” *Id.*, 9:54–55. The communication device includes a user interface used “to turn on or off operation of the RFID tag, to enter security data into the RFID tag, to enter financial information (e.g., a credit or debit card number into the RFID tag, to enter an identifying number (e.g., telephone number) into the RFID Tag, or to enter account number into the RFID tag.” *Id.*, 10:3–8.

B. Prosecution Histories '949, '734, '741, '612, and '396 Patents

1. The '949 Patent

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

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

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

Id., 305.

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

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

Id., 308.

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

36. Later that same day, Applicant filed a Response to the Non-Final Office Action, alleging that Beeson is not valid prior art, because the disclosures relied upon by the Examiner were not entitled to a priority date earlier than the priority date of the ’697 Application. *Id.*, 73. Together therewith, Applicant submitted an

Amendment to correct a typographical error in claim 2. *Id.*, 70–72.

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

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

than the priority date of the '697 Application. *Id.*

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

2. The '734 Patent

40. The '734 Patent was filed as App. No. 17/697,923 (the "'923 Application") on March 18, 2022, and on its face, purports to claim priority to a provisional application filed on May 6, 2005. EX1003, Cover. In a Preliminary Amendment dated May 19, 2022, Applicant canceled certain claims, added certain claims, and made short amendments throughout. EX1009, 329-32. Independent claim 1 recited:

1. (Currently Amended) 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;
and

communicating ~~an~~ 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 financial account information using the inductive antenna.

Id., 329.

41. In a first Non-Final Office Action dated June 8, 2022, the Examiner

rejected claims 25-30 as being anticipated by U.S. Patent No. 6,859,650, (“Ritter ’650”). *Id.*, 129-30. The Examiner found claims 1-9 and 11-24 to be allowable. *Id.*, 130-31. In response, Applicant cancelled claims 25-30, amended certain claims and added new claims. *Id.*, 123. On July 18, 2022, the Office issued a Notice of Allowance for all claims. *Id.*, 98-107. On October 27, 2022, the Office issued a Withdrawal from Issue and reopened prosecution. *Id.*, 88-89. In a second Non-Final Office Action dated November 2, 2022, the Examiner (1) rejected all claims for double patenting over 11,347,949; (2) rejected all claims being anticipated by Ritter, and (3) rejected claims 24, 36, and 44 as being unpatentable over Ritter ’650 in view of U.S. Patent No. 6,934,689 (“Ritter ’689”), while finding that the claims are entitled to an earliest priority date of November 9, 2021. *Id.*, 64-80. In response, Applicant traversed the rejections and argued that the claims were entitled to a priority date of May 6, 2005. *Id.*, 51-60. On January 18, 2023, the Office issued a Notice of Allowance for all claims. *Id.*, 19-28.

3. The ’741 Patent

42. The ’741 Patent was filed as App. No. 17/952,176 (the “’176 Application”) on September 23, 2022, and on its face, purports to claim priority to a provisional application filed on May 6, 2005. EX1004, Cover. In a Preliminary Amendment dated December 23, 2022, Applicant canceled certain claims, added certain claims, and made short amendments throughout. EX1010, 265-69.

Independent claim 1 recited:

1. (Currently Amended) A method of performing a financial transaction using a cellular telephone, the method comprising:

placing the cellular telephone within reading range of a wireless communication device, the cellular telephone being configured to communicate wirelessly using an inductive coupling and an RF antenna, wherein ~~the~~ communication ~~(verb)~~by the cellular telephone is responsive to a circuit including an electronic switch configured to change a state of the circuit, the circuit being configured to communicate responsive to the state of the circuit;

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

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

Id., 265.

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

4. The '612 Patent

44. 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). EX1005, Cover. 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.

45. 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.

5. The ’396 Patent

46. 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.

47. 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 radiofrequency 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”).

48. 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 wireless mode for cellular operation and in a second wireless mode for short range communication, wherein the first and second modes are characterized by use of different radio frequency ranges and the circuits are configured to perform financial transactions;

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.

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

C. RFID Communication Devices

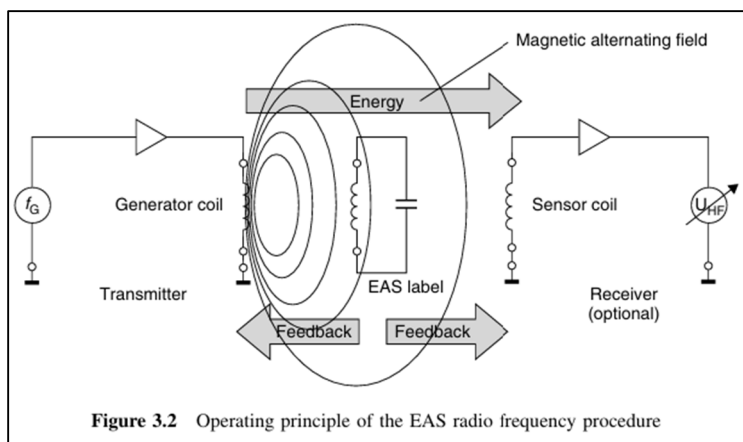
50. Based on my experience in the industry, I am familiar with the design of RFID communication devices of the type relevant to the '949, '734, '741, '612, and '396 Patents.

i. RFID

51. The abbreviation “RFID” stands for radio frequency identification, i.e., information carried by radio waves. EX1029, 7. RFID systems generally include two communication devices: a transponder, which is the data-carrying device, and a reader, which is the data-capture device. *Id.* Both the reader and transponder include

an inductive coupling element, such as an inductive antenna, and a controller implemented as an integrated circuit. *Id.*

52. RFID communication devices can transmit a signal by generating a magnetic alternating field in the radio frequency range. *Id.*, 31. When a receiving device is placed within this field, current is induced in its resonant circuit via its inductive coupling element. *Id.* The transmitting device can encode binary data in a transmission by activating and deactivating the magnetic field over time. *Id.*



Id.

53. In addition to data, certain RFID systems are capable of transferring operating power between devices. *Id.*, 9. Generally, power is transferred from the reader to the transponder. *Id.* Devices which operate their RFID circuitry using such received power are commonly referred to as “passive” devices. *Id.*, 13. Alternatively, “active” devices can rely entirely on battery power. *Id.* Mixed-power devices are also common, which include a battery to power the controller and other non-RFID functionality, but use power received from a reader to energize the RFID

communication circuitry. *Id.*

54. In 2003, Sony and Royal Philips Electronics (“Philips”) jointly developed and standardized the Near Field Communication (“NFC”) protocol (ISO/IEC 18092), which utilizes RFID technology to transfer data wirelessly. EX1015, at 1. NFC operates at the 13.56 MHz frequency, and allows devices in close proximity to communicate with each other. *Id.* Upon release of the specification, it was envisioned that NFC technology would be incorporated in a wide variety of communications devices, including computers, personal digital assistants (“PDAs”), cameras, and mobile phones. *Id.*

ii. Mobile Payment Applications

55. Starting in the early 2000s, developers began incorporating NFC technology into mobile phones. For example, in 2004, Nokia released the Nokia Mobile RFID Kit, which provided its phones with NFC communication capabilities. EX1016, at 3–4. That same year, NTT-DoCoMo, a Japanese mobile phone carrier, released a “Osai-fu-Keitai” (which translates to “Wallet Mobile”)-enabled handset, which was configured to facilitate NFC payments. EX1017, at 2–3; EX1018, at 2–7.

56. Such early NFC-enabled mobile phones relied on “smart card” technology, which included integrated circuit packages specifically designed for transmitting payment information via NFC communication. EX1018, at 2–7. One

popular smart card chip, “FeliCa,” was introduced by Sony and Philips for various applications as early as 1995. *Id.*; EX1015, at 1. In early 2004, Sony and DoCoMo formed a joint venture to adapt the FeliCa chip specifically for use in mobile phone payment applications. EX1018, at 2–7. This joint venture produced chips for DoCoMo, as well as several of its competitors. *Id.*

57. FeliCa-enabled phones were equipped with an “e-wallet” application, with which a user could load money onto their phone using a credit card. *Id.* Once the balance was loaded, the user could then use the application to transfer money to a POS device, or another user’s phone via NFC communication. *Id.*

58. Thus, in the early 2004 timeframe, NFC-enabled mobile phones, which utilized RFID communication to facilitate financial transactions, were well-known and available on the public market. *Id.* Such devices merely implemented longstanding communication techniques, which were available as early as 1995, in mobile phone and payment applications.

VI. LEVEL OF ORDINARY SKILL IN THE ART

59. I am informed and understand that the person having ordinary skill in the art (“POSITA”) is a hypothetical person who is presumed to know the relevant prior art. I understand that the actual inventor’s skill is not determinative of the level of ordinary skill. I further understand that factors that may be considered in determining level of skill include: (i) type of problems encountered in art; (ii) prior

art solutions to those problems; (iii) rapidity with which innovations are made; (iv) sophistication of the technology; and (v) educational level of active workers in the field. I understand that not all such factors may be present in every case, and one or more of them may predominate.

60. In my opinion, a POSITA, as of May 6, 2005, would have 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. Before the priority date of the '949, '734, '741, '612, and '396 Patents, I had this level of skill. Around the time of alleged priority date of May 6, 2005, I was familiar with this level of skill for RFID communication devices. This is the education and experience level that I encountered for people working in the field at the time. The opinions I express herein are provided from the perspective of a POSITA at the time of the alleged priority date of these patents.

VII. CLAIM CONSTRUCTION

61. I understand that “claim construction” is the process of determining a patent claim term’s meaning. I also understand that, during an *inter partes* review, a claim construction analysis begins with the plain meaning of the claim term, which is the ordinary and customary meaning given to the term by those of ordinary skill in the art at the time of the invention. I also understand that the claims of a patent

must be interpreted in light of the specification—that is, the claim language itself, the written description, and the figures in the patent—as well as the patent’s prosecution history and/or any reexamination history.

62. I have been informed that the U.S. Patent No. 7,924,156, a parent application of the ’949, ’734, ’741, ’612, and ’396 Patents, was at issue in a prior litigation, *Mynette Techs., Inc. and Steven M. Colby v. The United States and Unisys Corp.*, No. 16-1647 (COFC Aug. 17, 2018). I understand that in the *Mynette* litigation, the following claim constructions were adopted:

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

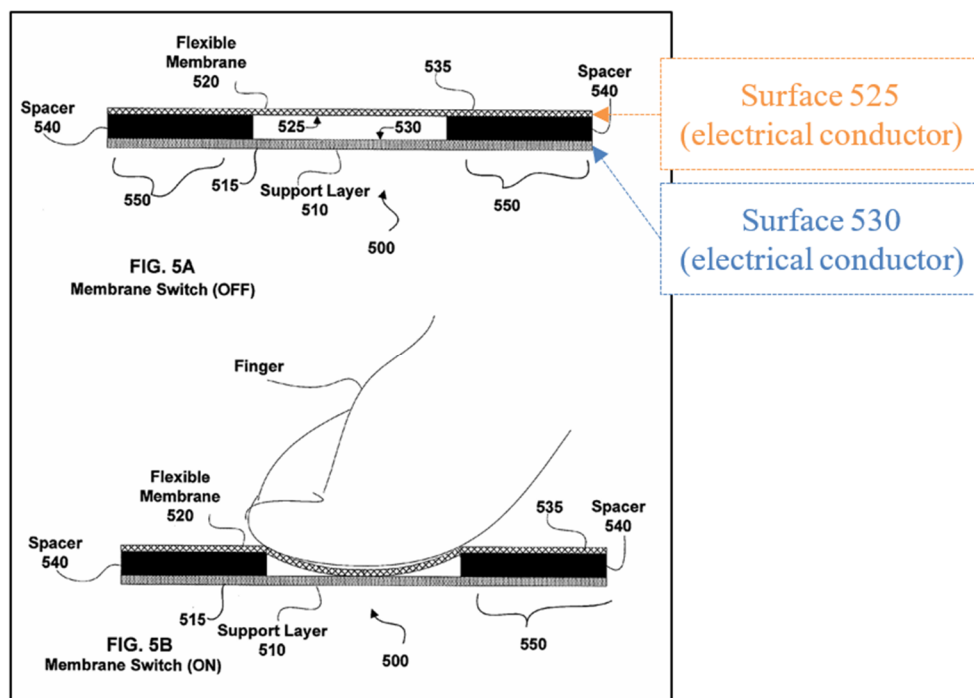
EX1022, at 15, 20, 41.

63. In my opinion, these claim constructions align with the interpretations

that a POSITA would have assigned to the corresponding claim terms. Thus, my below analysis of the '949, '734, '741, '612, and '396 Patents claims is based on these claim constructions.

64. Further, it is my opinion that a POSITA would have understood “mechanical switch” as “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.” For example, the shared specification describes switch 2270, which corresponds to the claimed mechanical switch, as “a sliding switch, a flip switch, a rotating switch, membrane switch, pushbutton switch, or other mechanical switch.” EX1002, 25:17–20. Each of these switch types makes or breaks an electrical connection responsive to movement of its components, for example, a sliding, flipping, rotating, or pressing of its components. As described in the specification, the mechanical switch can be “a mechanical contact switch activated by applying pressure to an outside surface of Switchable RFID Device 2200.” *Id.*, 25:29–31. The mechanical switch can also be “configured to be moved between the on position and the off position, for example using a finger.” *Id.*, 26:39–41. Further, Figures 26A–B (reproduced below) illustrate a “membrane switch,” which is a type of mechanical switch. *Id.*, 25:17–20, 26:51–60. In this example, the switch is illustrated as making or breaking an electrical connection between surfaces 2625 and 2630, which are both electrical conductors, responsive to a user pressing flexible membrane 2620. Thus,

in each of these embodiments, the mechanical switch is 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.



EX1002, FIGs. 26A–B.

VIII. SUMMARY OF PRIOR ART

A. *Waters* (EX1024)

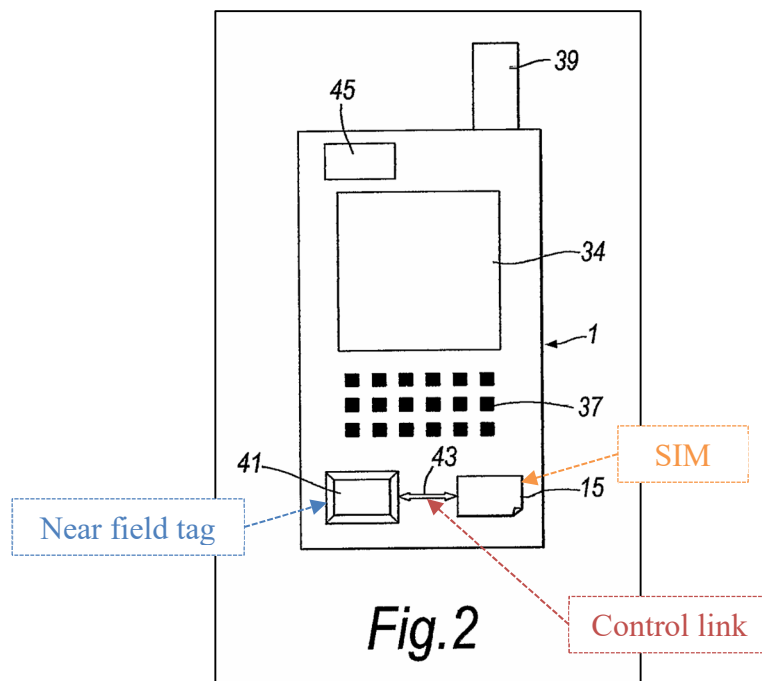
65. U.S. Patent Publication No. 2009/0215385 (“*Waters*”) published on August 27, 2009 and claims priority to WO 2006/087503, which was filed on February 15, 2005. WO 2006/087503 was filed as a PCT application in Great Britain, was published in English, and designated the United States. EX1024, at Cover. *Waters* thus predates the ’949, ’734, ’741, ’612, and ’396 Patents.

66. *Waters* relates to an RFID-enabled cellphone having a SIM 15 which includes¹ a near field tag 41 and control link 43, for facilitating financial transactions. *Id.*, Abstract, [0057]. Specifically, *Waters* provides that “the near field tag 41 is selectively enabled or disabled for communication with the reader under control of the SIM 15, by means of communication link 43.” *Id.*, [0037]. *Waters* further discloses that control link 43 can be responsive to interface means for “selectively enabl[ing] and disabl[ing] [near field tag 41] in order to reduce the opportunity to obtain information from the near field tag 41 by an unauthorised reader.” *Id.*, [0050]. These can include pressure sensors, PINs, biometrics, light sensors, heat sensors, skin resistance sensors, and inertial sensors to authenticate a user and enable RFID communication. *Id.*, [0051] (“(1) Personal identification number (PIN) entry—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. The user's PIN may be stored in a secure location in the mobile terminal 1 or in the SIM 15. When the user enters their PIN using the keypad 37, the entered PIN is compared with the stored PIN. If the PINs match, the SIM transmits a message, via link 43, to the near field

¹ While Figure 2 of *Waters* illustrates the SIM 15, control link 43, and near field tag 41 as three separate components, *Waters* explicitly provides that “the mechanism for activating/deactivating the tag [(i.e., control link 43)] may be incorporated directly into the smart card or SIM 15 itself. Also, the tag 41 or part of the tag 41 may be incorporated into the SIM 15.” EX1024, [0057].

tag **41** to activate the near field tag. (2) Biometric data entry—the mobile terminal **1** may incorporate a fingerprint reader **45**. The fingerprint reader **45** scans the fingerprint of the user when the user's finger is placed on the reader **45** and compares it to the user's fingerprint stored in the memory of the mobile terminal **1** or the SIM **15**. If the fingerprints are determined to match, the message is sent from the SIM **15**, via link **43**, to the RF tag **41**. As an alternative to a fingerprint, other biometric data could be used—for example, voice recognition (using the mobile terminal's built-in microphone and a voice recognition algorithm within the mobile terminal **1** or SIM card **15**) or retinal scanning (using the mobile terminal's built-in camera).”), [0052] (“Arrangements (1) and (2) above 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**.”), [0053] (“(1) Light sensor . . . (2) Pressure sensor—a pressure sensor on the casing of mobile terminal **1** acts as a switch. The RF tag **41** is only enabled when the user physically presses the pressure sensor. Therefore, when the mobile terminal is in a case or the user's pocket, the pressure sensor is disabled. The pressure sensor may itself be deactivated

by the user, for example, when a function of the mobile terminal **1** is selected such that the keypad **37** is inoperative. The pressure sensor may be combined with the fingerprint scanner **45**. The combined sensor detects, not only that pressure is applied, but also that an authorised person is pressing the sensor. Alternatively, the pressure sensor could be combined with an electrical resistance meter and used to detect that it is a human hand pressing the pressure sensor, rather than some other object. . . . (3) Heat sensors . . . (4) Skin resistance sensor . . .”).



Id., FIG. 2.

67. As an additional security mechanism, the near field tag **41** can “jam/disrupt the low level communications of all other RF tags within range of the jamming device.” *Id.*, [0055]. To do so, the near field tag **41** “attempt[] to create collisions and other forms of interference,” “[i]nstead of following the anti-collision

protocol commonly used in near field tag technology.” *Id.* Then, “when authorized use is required,” “[t]he jamming device is disabled,” to permit uninterrupted communication between the near field tag 41 and the RFID reader. *Id.*

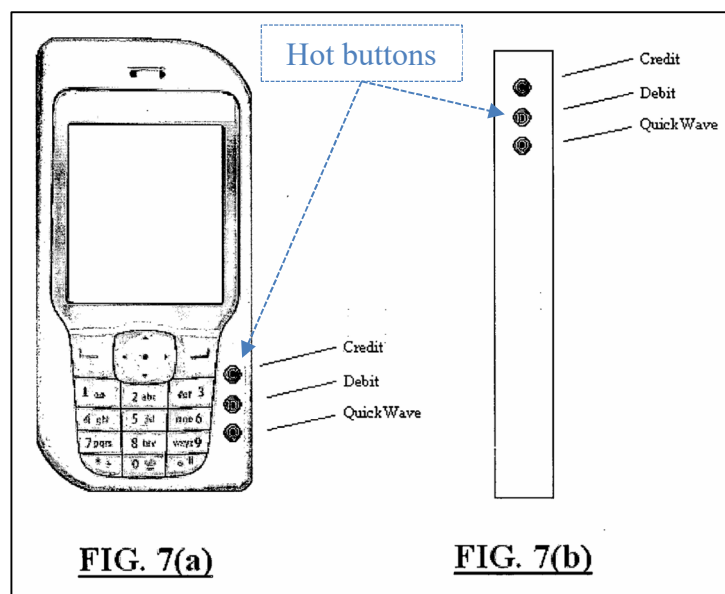
68. *Waters* is in the same field of endeavor as the ’949, ’734, ’741, ’612, and ’396 Patents—RFID-enabled communication devices—and in my opinion, a POSITA would have understood that *Waters* provides an alternative design that would have been available to a POSITA at the time of invention.

B. *Dua* (EX1023)

69. U.S. Patent Publication No. US 2006/0165060 (“*Dua*”) was filed on January 21, 2005 and published on July 27, 2006. EX1023, at Cover. Thus, *Dua* predates the ’949, ’734, ’741, ’612, and ’396 Patents by over a year.

70. Similar to *Waters*, *Dua* relates to an RFID-enabled cellphone, suitable for facilitating financial transactions. *Id.*, [0026], [0041], [0296], FIG. 7. *Dua*’s device includes a wallet application, which manages a user interface, storage, processing, and communication functions associated with RFID transactions. *Id.*, [0288], [0309]–[0311]. *Dua*’s device also includes hot buttons, which can enable/disable RFID communication and select a mode in which a transaction can be carried out. *Id.*, [0388]–[0395]. In one example provided by the specification, the hot buttons, and corresponding modes, can include “QuickWave,” “Debit,” and “Credit.” *Id.*, [0392], FIG. 7. When the “QuickWave” hot button is pressed, the

device can enter a QuickWave mode, in which certain credentials can be transmitted to certain RFID readers, which have been pre-registered using a “reader key,” without requiring the user to enter a PIN or otherwise authenticate themselves. *Id.*, [0392]. When the “Debit” hot button is pressed, the device can enter a debit card mode, in which debit card credentials can be transmitted to an RFID reader, after a user has entered a PIN or otherwise authenticated themselves. *Id.*, [0392], [0395]. Similarly, when the “Credit” hot button is pressed, the device can enter a credit card mode, in which credit card credentials can be transmitted to an RFID reader, after a user has entered a PIN or otherwise authenticated themselves. *Id.* In any of the above cases, a button press can enable RFID communication, and place the wallet application in a corresponding mode, for a 30-second period, after which RFID communication will be disabled. *Id.*, [0383], [0395].



EX1023, FIG. 7.

71. *Dua* is in the same field of endeavor as the '949, '734, '741, '612, and '396 Patents—RFID-enabled communication devices—and in my opinion, a POSITA would have understood that *Dua* provides an alternative design that would have been available to a POSITA at the time of invention.

C. *Woike* (EX1025) (Secondary Reference)

72. *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).

IX. The '949 PATENT

A. SUMMARY OF PRIOR ART GROUNDS

Ground	Claims	Basis	Prior Art
1	1–23, 26–30	Anticipation	<i>Dua</i>
2	1–23, 26–30	Obviousness	<i>Dua</i>
3	24, 25	Obviousness	<i>Dua</i> with <i>Woike</i>
4	1–30	Obviousness	<i>Dua</i> with <i>Waters</i>

B. GROUNDS 1-2: *Dua* Anticipates and/or Renders Obvious Claims 1–23 and 26–30

i. Independent Claim 1

1[pre]: An electronic communication system comprising:

73. *Dua* describes a “mobile device” (an electronic communication system)

“with a wallet application” that can “transmit payment, identification, or other confidential information to a reader using the short-range transmission capability of the wireless device (e.g. RF).” EX1023, [0315].

74. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses 1[pre].

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

75. In my opinion, a POSITA would have understood that *Dua*’s “mobile telephone” is a cellular telephone. For example, *Dua* explains that its mobile telephone is “capable of wirelessly connecting to the Internet using network protocols such as GSM/GPRS, CDMA2000, W-CDMA, EDGE, HDR, 1xRTT, UMTS, [and] IMT-2000.” EX1023, [0026] (“According to a preferred embodiment of the invention, credentials are ultimately supplied to a handheld device such as a mobile telephone via a wireless network.”), [0041]. Each of these protocols is a cellular communication protocol. Thus, *Dua*’s device is a cellular telephone.

76. *Dua* discloses that its device “communicates wirelessly” since it is a “wireless device,” which includes an RFID interface configured to carry out transactions using wireless RFID communication. EX1023, Abstract, [0041] (“Wireless device **200** also preferably 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.”), [0378] (“When the wireless device is placed in proximity to the reader, the selected credential(s) are automatically transmitted by the RFID chip in the wireless device to the reader.”). *Dua* also explains that ISO/IEC 14443, which describes the use of inductive coupling antennas to facilitate wireless RFID communication, was known in the art. *Id.*, [0013]. In my opinion, while *Dua* does not expressly use the term “inductive coupling,” a POSITA would have understood that inductive coupling naturally flows or is a natural result of the RFID technology disclosure of *Dua* because RFID technology uses an RFID antenna (using inductive coupling) to enable such RFID communication. *See* EX1031, 7-10.

77. Therefore, in my opinion, a POSITA would have understood that *Dua* inherently anticipates, or otherwise renders obvious, 1[a].

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

78. *Dua* explains that its “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]. In my opinion, a POSITA would have understood that the wireless device running the wallet application that enables communication with the embedded RF interface necessarily

includes processing and control circuitry that executes the wallet application and controls the embedded RF interface.

79. *Dua* further discloses the use of PIN or biometric authentication to implement RFID communication logic responsive to a PIN or biometric sensor. *Id.*, [0395] (“Pressing buttons **1** or **2**, may prompt the user to input a PIN before RF communication can be enabled. As such, a user may be required to input a PIN and click ‘OK’ to enable RF communication for a 30 second window. Alternatively, the user may be required to input his PIN, click ‘OK’ to initiate PIN verification, and upon positive confirmation be prompted to hold down either button **1** or **2** while placing the device in close proximity to a reader.”), [0414] (“While the above description calls for the use of over-the-air PIN verification, it should be noted that biometrics could also be used in lieu of PINs, while still falling within the scope of the present invention. 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.”). In my opinion, a POSITA would have understood that the PIN and biometric authentication mechanisms necessarily include an electronic switch that, in response to PIN or biometric entry, makes or breaks an electrical connection in the processing or control circuitry that executes the wallet application and controls the embedded RF interface (i.e., the circuit). In my opinion, a POSITA would have understood that the electronic switch, in response to PIN or biometric entry, makes

or breaks an electrical connection in the circuit, causing an electronic signal to change the operative state of the circuit (e.g., from disabled to enabled, from PIN-less to authenticated). EX1023, [0367] (describing PIN-less state—“A user can at their own discretion, choose to designate certain credentials within the wallet application to be used without requiring entry of the wallet application PIN. Registered credentials that can be designated by the user as not requiring entry of a wallet PIN are those that have a ‘reader key’ associated with them. Credentials with a ‘reader key’ associated with them will be flagged as such in the wallet application to help a user identify them.”), [0395] (describing disabled/enabled states—“Pressing buttons **1** or **2**, may prompt the user to input a PIN before RF communication can be enabled. As such, a user may be required to input a PIN and click ‘OK’ to enable RF communication for a 30 second window. Alternatively, the user may be required to input his PIN, click ‘OK’ to initiate PIN verification, and upon positive confirmation be prompted to hold down either button **1** or **2** while placing the device in close proximity to a reader.”), [0397] (describing authenticated state—“Certain credential issuers such as financial institutions may require that users validate their identity during a transaction by providing a PIN that was established with or set by the financial institution.”), [0414] (“While the above description calls for the use of over-the-air PIN verification, it should be noted that biometrics could also be used in lieu of PINs, while still falling within the scope of

the present invention. 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.”).

80. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses 1[b].

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

81. As discussed above, *Dua* anticipates, or otherwise renders obvious, that its processing and control circuitry executes the wallet application and controls RFID communication (*i.e.*, is configured to communicate) via the inductive coupling. *See supra* §§ IX.B.i.1[a]–[b] (’949 Patent Claim 1); EX1023, [0309]. As further discussed above, such communication is responsive to the states of the circuit, because the circuit can transmit a credential (communicate) in an enabled state, but not in a disabled state, or the circuit can transmit only PIN-less credentials in a PIN-less state and PIN-protected credentials in an authenticated state. *See supra* § IX.B.i.1[b] (’949 Patent Claim 1).

82. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses 1[c].

83. As such, in my opinion, a POSITA would have understood that *Dua* anticipates or renders obvious independent Claim 1.

ii. Dependent Claims 2–23 and 26–28

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

84. *Dua* discloses every element of Claim 1. *See supra* § IX.B.i ('949 Patent Claim 1). It is my understanding that this limitation is recited in the alternative (using the word “or”), and it is therefore disclosed if at least one of the recited elements is met. *Dua*'s wireless device includes at least memory. For example, *Dua* explains that “wireless device **200** has processing and secure storage capabilities allowing it to host and operate a wallet application capable of receiving, storing, managing and transmitting multiple payment, identification, and other confidential information electronically.” EX1023, [0041]. As discussed above, in my opinion, it would have been obvious to a POSITA that including memory in the processing and control circuitry that executes the wallet application necessarily flows from these “processing and secure storage capabilities.”

85. As to the other elements, to the extent that *Dua* does not expressly disclose a switchable RFID tag, input logic, processing logic, a return signal generator, switch logic, a switch state monitor, encryption logic, one or more antenna, or a power supply, in my opinion, it would have been obvious to a POSITA to implement each of these components in the device of *Dua*, because these are

necessary to enable its RFID payment functionality. *See supra* §IX.B.i ('949 Patent Claim 1).

86. Therefore, in my opinion, a POSITA would have understood that *Dua* anticipates, or otherwise renders obvious, Claim 2.

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

87. *Dua* discloses every element of Claim 1. *See supra* § IX.B.i ('949 Patent Claim 1). As discussed above, *Dua*'s memory is configured to "to host and operate a wallet application capable of receiving, storing, managing and transmitting multiple payment, identification, and other confidential information electronically." EX1023, [0041]. Specifically, *Dua*'s wallet application stores several types of electronic credentials in the device's memory, including stored value credentials, such as a "Starbucks S-Value" card. EX1023, [0295] ("Extensions may reside on the device memory, in an embedded smart card, in a removable storage media, or on a remote server, securely accessible through the wallet application protocols."), [0334] ("The wallet application is specifically designed to store several types of electronic credentials."), [0345], [0429] ("The data stored inside the wireless device is encrypted and protected with the wallet PIN code (or other biometric security information), which is used to allow the user access to the application."). *Dua* provides example payment credentials:

Payment Methods	
<u>Credit</u>	
Sample Bank MasterCard	XXX4321
CapitalOne Visa	XXX1234
Home Depot Card	XXX9865
Gap Card	XXX5432
ExxonMobil Card	XXX4564
<u>Debit/ATM</u>	
Sample Bank Stored Value	XXX5432
Starbucks S-Value	XXX9876
<u>Electronic Check</u>	
Sample Bank Checking	XXX7654
<u>RF Tokens</u>	
Speedpass	XXX3456

EX1023, [0345]. *Dua* explains that when such a stored value credential “is waved in front of a reader at the turnstile, the electronic balance is automatically debited from the onboard chip,” and that “an over-the-air reload tool” can be programmed into the wallet application. *Id.*, [0290], [0293]. In my opinion, it would have been obvious to a POSITA to store the value and account balance of such credentials in memory, to enable the account debiting and reloading functionality described by *Dua*.

88. Therefore, in my opinion, a POSITA would have understood that *Dua* renders obvious Claim 3.

Claim 4: The system of claim 2, wherein the cellular telephone further includes a user interface configured to

enter a financial account number and the memory is configured to store the financial account number for use in the financial transaction.

89. *Dua* discloses every element of Claim 2. *See supra* § IX.B.ii ('949 Patent Claim 2). *Dua*'s device is equipped with a key pad (a type of user interface) "for alphanumeric and special character input." EX1023, [0041]. *Dua* explains that the wallet application may request the user to enter "such information as the user's account number with the issuer." *Id.*, [0444]. Additionally, *Dua* discloses that its device can store and use credit card and debit card numbers, and that the wallet application can request that a user enter a "card account number." *Id.*, [0180] ("The user would see such a request for information within the wallet application screen on the device display. This could include a request for such information such as an existing card account number, card expiration date, cardholder name, mother's maiden name, billing address, social security number, account balance, transaction history, driver's license number, or business identification."); *see also id.*, [0019], [0336], [0345], [0392]. Therefore, in my opinion, a POSITA would have understood that *Dua*'s key pad (user interface) is used to enter a financial account number.

90. Further, as discussed above, *Dua*'s memory is configured to store such "payment...information," to enable the wallet application and associated circuitry to carry out a financial transaction. EX1023, [0041] ("It is further preferred that wireless device **200** has processing and secure storage capabilities allowing it to host

and operate a wallet application capable of receiving, storing, managing and transmitting multiple payment, identification, and other confidential information electronically.”).

91. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 4.

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

92. *Dua* discloses every element of Claim 1. *See supra* § IX.B.i (’949 Patent Claim 1). *Dua* explains that the circuitry of its device is configured such that “[e]lectronic credentials issued to a user and stored in the wallet application can be used” in a proximity transaction, where “the wireless device can transmit payment...information to a reader.” *Id.*, [0313] (“Electronic credentials issued to a user and stored in the wallet application can be used in all three environments.”), [0315] (“During 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). 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.”). Such financial transactions are communicated via the inductive coupling when the RFID circuitry is enabled (*i.e.*, responsive to the states of the

circuit), for the reasons discussed above with reference to Claim 1. *See supra* §§ IX.B.i.1[b]-1[c] ('949 Patent Claim 1).

93. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 5.

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

94. *Dua* discloses every element of Claim 5. *See supra* § IX.B.ii ('949 Patent Claim 5). *Dua* explains that its wallet application can store multiple payment credentials (financial accounts), including “[c]redit, debit/ATM, stored value, electronic check, and RFID payment methods.” EX1023, [0336]. *Dua* further explains that a user can designate certain of these credentials as “requiring advance PIN-entry and others to function without the prior input of the wallet PIN.” *Id.*, [0366] (“While this document references the use of PIN codes throughout, wireless device's with embedded biometric technologies could use a fingerprint in lieu of a PIN code to authenticate a user to the wallet application.”), [0368] (“Each individual will have their own risk tolerance and as such will want the flexibility to designate specific credentials in their wallet as requiring advance PIN-entry and others to function without the prior input of the wallet PIN.”).

95. As discussed above, *Dua*'s device also includes an electronic switch that controls the RFID communication responsive to the PIN or biometric

authentication mechanism. *See supra* § IX.B.i.1[b] ('949 Patent Claim 1). For example, when the user is authenticated, the electronic switch can cause a transition from a PIN-less state (in which only credentials “designated by the user as not requiring entry of a wallet PIN” can be transmitted) to an authenticated state (in which other credentials “requiring advance PIN-entry” can be transmitted). *See supra* §IX.B.i.1[b] ('949 Patent Claim 1); EX1023, [0367] (“A user can at their own discretion, choose to designate certain credentials within the wallet application to be used without requiring entry of the wallet application PIN.”), [0368] (“Each individual will have their own risk tolerance and as such will want the flexibility to designate specific credentials in their wallet as requiring advance PIN-entry and others to function without the prior input of the wallet PIN.”). In my opinion, a POSITA would have understood that, by authenticating themselves, the user selects between credentials (which can be financial accounts) “designated by the user as not requiring entry of a wallet PIN” and credentials (which can also be financial accounts) “requiring advance PIN-entry,” via the electronic switch. EX1023, [0367]-[0368]. The selected credentials are then used for a subsequent financial transaction.

96. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 6.

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

97. *Dua* discloses every element of Claim 5. *See supra* § IX.B.ii ('949 Patent Claim 5). *Dua* explains that its PIN and biometric authentication mechanisms include a key pad (used to capture a user's PIN) and a fingerprint scanner (used to capture a user's fingerprint), respectively. EX1023, [0041] (describing a "key pad for alphanumeric and special character data input"), [0414] ("PINs can be entered directly into the user's wireless device....a user may be prompted to scan his fingerprint using an integrated scanner in the wireless device 800 instead of inputting a PIN as described earlier."). In my opinion, a POSITA would have understood that *Dua*'s key pad and fingerprint scanner are each user interfaces for the PIN and biometric authentication mechanisms, respectively, because they interface with the user to capture data (PIN or fingerprint) to enable these mechanisms.

98. Additionally, as explained above, *Dua*'s device includes an electronic switch that enables transmission of certain credentials, responsive to the PIN or biometric authentication mechanisms. *See supra* §§IX.B.i.1[b] ('949 Patent Claim 1), IX.B.ii ('949 Patent Claim 6). As discussed above, when the user is successfully authenticated using PIN or biometric authentication (via the key pad and fingerprint scanner user interfaces), RFID communication of payment credentials is enabled (a financial transaction is approved) via the electronic switch. *See supra* §§IX.B.i.1[b] ('949 Patent Claim 1), IX.B.ii ('949 Patent Claim 6).

99. Therefore, in my opinion, a POSITA would have understood that *Dua*

discloses Claim 7.

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

100. *Dua* discloses every element of Claim 5. *See supra* § IX.B.ii ('949 Patent Claim 5). *Dua* explains that its wallet is “the core” of the platform and “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,” 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 describes 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].

101. As discussed above, *Dua*’s “circuit” is the processing and control circuitry that executes the wallet application and controls the embedded RF interface or smart card. In my opinion, a POSITA would have understood that the circuitry is configured to facilitate the financial transaction and to communicate financial account information based on the functionality of the wallet application it executes. Thus, by making the wallet application functionality and transmission of financial

credentials (financial transactions) responsive to a fingerprint sensor (biometric sensor), in my opinion, a POSITA would have understood that *Dua* discloses Claim 8.

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

102. *Dua* discloses every element of Claim 5. *See supra* § IX.B.ii ('949 Patent Claim 5). *Dua* discloses that its circuit is configured to communicate credentials via the inductive coupling to facilitate a financial transaction for the reasons discussed above in § IX.B.ii ('949 Patent Claim 5). *Dua* explains that such credentials include an “Account number.” EX1023, [0297], [0302] (“Account number”), [0303] (“Expiration date of credential”), [0304] (“Special security information related to credential (e.g. CVV/CVC/CVV2/CVC2, etc)”), [0383].

103. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 9.

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

104. *Dua* discloses every element of Claim 5. *See supra* § IX.B.ii ('949 Patent Claim 5). *Dua* discloses that its device includes a key pad (input) for entry of a PIN and that “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.” *See supra* §IX.B.ii (’949 Patent Claim 7); EX1023, [0366], [0395].

105. Further, as discussed above, when RFID transmission is enabled, the circuit can communicate financial account information via the inductive coupling to facilitate the financial transaction. *See supra* §IX.B.ii (’949 Patent Claim 5).

106. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 10.

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

107. *Dua* discloses every element of Claim 5. *See supra* § IX.B.ii (’949 Patent Claim 5). *Dua* explains that credentials “transmitted from the wireless device to the reader may be encrypted using the issuer’s encryption key,” which is provided by the issuer when a credential is issued. EX1023, [0362]. In my opinion, a POSITA would have understood that such a key would necessarily be stored in memory after it is received from the credential issuer, such that the key can later be read from memory and used to encrypt the credential and facilitate the financial transaction.

108. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 11.

Claim 12: The system of claim 5, further comprising a key memory configured to store a key required to change the

states of the circuit to facilitate the financial transaction via the inductive coupling.

109. *Dua* discloses every element of Claim 5. *See supra* § IX.B.ii ('949 Patent Claim 5). *Dua* explains that a reader key “is sent with an electronic credential record to a wireless device during the issuance process.” EX1023, [0353] (“The key is sent with an electronic credential record to a wireless device during the issuance process. The same reader key is programmed in all reader devices employed by an organization. In the case of an RFID reader, the key is transmitted from the reader to the wireless device's RFID chip during a proximity transaction. The receipt of the key by the RFID chip in the wireless device may initiate...transfer of the key to the application. The key is subsequently received by the wallet application and is used as a search string by the application to locate a specific credential for transmission back to the reader via the device's RF capability.”). In my opinion, a POSITA would have understood that such a key would necessarily be stored in the wireless device's memory “with the electronic credential to which it is linked.” *Id.*, [0354] (“The wallet application stores the ‘reader key’ with the electronic credential to which it is linked. When transmitted to the wireless device from the reader, the key is used by the wallet application as a search string for locating the linked credential. If a matching key is found within the wallet application, the corresponding loyalty information will be transmitted to the reader from the wireless device via RF.”). All RFID readers associated with the issuer also store a corresponding key. *Id.*, [0353].

At the start of a transaction, an RFID reader associated with the issuer transmits its key to the wireless device. *Id.* The circuit identified in § IX.B.i ('949 Patent Claim 1) then passes the key to the wallet application it executes, which uses the key to look up a credential associated with the corresponding reader key, which was received and stored during the issuance process. *Id.*, [0353], [0354]. The circuit then completes a transaction using the relevant credential. *Id.* In my opinion, a POSITA would have understood that the reader key, which is stored in memory, is used to transition the circuit to an ON state that enables RFID communication, via the inductive coupling, with the issuer-associated reader. *See supra* §§IX.B.i.1[a]–[b] ('949 Patent Claim 1).

110. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 12.

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

111. *Dua* discloses every element of Claim 5. *See supra* § IX.B.ii ('949 Patent Claim 5). *Dua*'s device includes a "wallet button," which can be pressed to "enable[] communication via the RFID interface." EX1023, [0383], [0386]. In my opinion, a POSITA would have understood that *Dua*'s wallet button corresponds to the recited 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. *See supra* §V.B (a POSITA would have understood “mechanical switch” to mean “a control device that makes or breaks an electrical connection in a circuit responsive to movement of one or more components of the control device.”). Further, the wallet button is configured to approve the financial transaction, because its actuation by a user is required to enable the RFID communication necessary to facilitate a transaction. EX1023, [0383], [0386].

112. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 13.

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

113. *Dua* discloses every element of Claim 5. *See supra* § IX.B.ii (’949 Patent Claim 5). *Dua* discloses that “[d]uring a proximity transaction, the wireless device can transmit payment, identification, or other confidential information to a reader using the short-range transmission capability of the wireless device (e.g. RF).” EX1023, [0315]. For example, “a wireless device...can simply be waved slowly in close proximity to a reader device to facilitate a transaction.” *Id.*

114. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 14.

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

115. *Dua* discloses every element of Claim 14. *See supra* § IX.B.ii ('949 Patent Claim 14). As discussed above, *Dua*'s device can communicate with a reader. *See supra* §IX.B.ii ('949 Patent Claim 14). *Dua* further explains that the reader is connected to "point of sale terminal 860." EX1023, [0318], [0361], [0405], FIG. 8. In my opinion, it would have been obvious to a POSITA to combine the disclosed reader and point of sale terminal together, so that the point of sale device "include[es]" the reader, to reduce complexity and cost.

116. Therefore, in my opinion, a POSITA would have understood that *Dua* renders obvious Claim 15.

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

117. *Dua* discloses every element of Claim 1. *See supra* § IX.B.i ('949 Patent Claim 1). In my opinion, a POSITA would have understood that *Dua* explains that the circuit can operate in multiple ON states that differ in whether authentication is required and in which credentials can be transmitted. For example, *Dua* teaches that a user may "designate specific credentials in their wallet as requiring advance PIN-entry and others to function without the prior input of the wallet PIN." EX1023, [0368]; *see also id.*, [0366] (biometric authentication can also be used in place of PIN authentication), [0367], [0369]-[0370].

118. *Dua* explains that “[t]he PIN-less option for certain credentials that have a ‘reader key’ associated with them allows users to complete time-sensitive transactions by simply passing their wireless device in front of a reader without any further key entry.” *Id.*, [0370]. In my opinion, a POSITA would have understood that this functionality necessarily discloses that the underlying processing and control circuitry executing the wallet application is in an ON state, because it is in a state where it can complete a transaction with a reader.

119. *Dua* explains that the wallet application can prompt the user to enter a PIN or biometric to access authentication-protected credentials. *See, e.g.*, EX1023, [0366]. In one embodiment including a “wallet button,” the wallet application is first activated without authentication and then prompts the user to enter a PIN. *Id.*, [0384]. And “if the user wants to open the wallet application to select credentials or make changes to settings, the user can simply enter his wallet PIN when prompted.” *Id.* *Dua* further explains that the PIN-entry can be replaced with “a fingerprint in lieu of a PIN code to authenticate a user to the wallet application” in phones with “embedded biometric technologies.” *Id.*, [0366]. As discussed above in §IX.B.i (’949 Patent Claim 1), this authentication mechanism is used to change the operative state of the circuit (*i.e.*, from a PIN-less state to an authenticated state enabling RF communication of secured credentials). In my opinion, a POSITA would have understood this state of the circuit to be another ON state, in which different

credentials can be transmitted to the reader.

120. In my opinion, a POSITA would have understood these two states to be a first ON state and a second ON state as recited in Claim 16, because different credentials are transmitted in each state (*e.g.*, more sensitive credentials requiring PIN/biometric entry, or less sensitive PIN-less credentials). EX1023, [0383] (“Under one design, when the ‘wallet button’ is pressed and released, the wallet application...enables communication via the RFID interface in the device; RF communication might be enabled for a period of 30 seconds during which time the device should be placed in proximity of the reader to allow for transmission of a credential that has a ‘reader key’ and is approved for PIN-less transactions”), [0384], [0394] (“To summarize, pressing the ‘wallet button’ and releasing it could enable RF communication for 30 seconds....As such the application is ready to communicate with a reader, and simultaneously prompts the user for his Wallet PIN.”). In my opinion, a POSITA would further have understood that successful PIN or biometric authentication activates the electronic switch, which makes or breaks an electrical connection in the circuit, causing an electronic signal to change the operative state of the circuit from a second ON state (*i.e.*, communication of PIN-less credentials is enabled) to a first ON state (*i.e.*, authenticated and communication of PIN/biometric-protected credentials is enabled). EX1023, [0366], [0368], [0384].

121. Therefore, in my opinion, a POSITA would have understood that *Dua*

discloses Claim 16.

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

122. *Dua* discloses every element of Claim 16. *See supra* § IX.B.ii ('949 Patent Claim 16). *Dua* discloses a second ON state (e.g., PIN-less state) and a first ON state (e.g., authenticated state). *See supra* §IX.B.ii ('949 Patent Claim 16). As discussed above, a user can “designate specific credentials in their wallet as requiring advance PIN-entry and others to function without the prior input of the wallet PIN.” EX1023, [0368]. In the PIN-less state (second ON state), the device transmits only certain designated credentials, which *Dua* describes as including non-payment information such as “Personal Information—Name, billing address, shipping address, home phone number, business phone number, fax number, social security number, and date of birth.” *Id.*, [0343], [0392]-[0393]. In the authenticated state (first ON state), by contrast, the device transmits PIN-protected payment credentials in order to carry out a credit card or debit card transaction. *Id.*, [0393], [0395] (“Pressing buttons **1** or **2**, may prompt the user to input a PIN before RF communication can be enabled. As such, a user may be required to input a PIN and click ‘OK’ to enable RF communication for a 30 second window. Alternatively, the user may be required to input his PIN, click ‘OK’ to initiate PIN verification, and upon positive confirmation be prompted to hold down either button **1** or **2** while

placing the device in close proximity to a reader. The press/release or hold down scenarios would also apply to button 3.”).

123. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 17.

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

124. *Dua* discloses every element of Claim 1. *See supra* § IX.B.i (’949 Patent Claim 1). *Dua*’s device circuitry includes memory, and in my opinion, it would have been obvious to a POSITA to store the current state of the circuit in this memory (state memory), reflecting the current device state. *See supra* §IX.B.ii (’949 Patent Claim 2). Alternatively, it would have been obvious to a POSITA to store the current state in memory (state memory), to enable implementation of the logic described above. *See supra* §§IX.B.ii (’949 Patent Claims 16 and 17). For example, the circuit enables a “wallet application,” which controls the wireless device to carry out such logic. EX1023, [0333] (“The wallet application is designed to facilitate transactions in a proximity, personal, and remote environment using the device's short-range or long-range transmission capability.”), [0354] (“The wallet application stores the ‘reader key’ with the electronic credential to which it is linked. When transmitted to the wireless device from the reader, the key is used by the wallet application as a search string for locating the linked credential. If a matching key is found within the wallet application, the corresponding loyalty information will be

transmitted to the reader from the wireless device via RF.”). As described above, the circuit determines state transitions based on PIN or biometric authentication. *See supra* §§IX.B.i (’949 Patent Claim 1), IX.B.ii (’949 Patent Claims 16 and 17). These logical transitions require reading an input and applying logic based on the status thereof. In my opinion, a POSITA would have understood that to implement such functionality, the control software of the device would store the current state in a variable, according to logic based on input values, such that state transitions can be implemented. Such techniques were well-known at the time of invention. *See* EX1029, 72 (storing switch state in a ‘Sw_state’ variable), 74 (applying logic to ‘Sw_state’ variable and storing output state in an ‘Output_port’ variable). The value of the state variable would be stored in memory (state memory), such that the software can use the state variable during operation, to control the RFID circuitry to output jamming, transaction, or no data. *See id.*, 26.

125. Therefore, in my opinion, a POSITA would have understood that *Dua* renders obvious Claim 18.

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

126. *Dua* discloses every element of Claim 1. *See supra* § IX.B.i (’949 Patent Claim 1). *Dua* states that “the wallet application will log all transactions made in proximity, personal, or remote mode. The log will display information such as date/time, name of retailer/organization, location ID, list of credentials used in the

transaction, and purchase price (if transaction had a financial component).” EX1023, [0489]. *Dua* further discloses digital receipts containing “the transaction amount, date/time of the transaction, merchant name, [and] payment method used.” *Id.*, [0430]. Thus, the wallet application stores transaction logs including details such as date, time, merchant, location, credential, and amount. *Id.*, [0489], [0430] (“The wallet application is capable of receiving digital receipts from merchants. Digital receipts are electronic equivalents of paper receipts. They work as the payer's record of a payment transaction that has taken place during a proximity, personal, or remote transaction using the wallet application. Similar to a paper receipt, they contain information such as the transaction amount, date/time of the transaction, merchant name, payment method used, and sometimes details of what was purchased. The receipt functionality makes it possible to have a record of the payment before a physical receipt can be delivered, or in cases where a physical receipt is not used at all.”).

127. To the extent that *Dua* does not explicitly recite “the circuit is configured to store transaction logs,” in my opinion, it would have been obvious to a POSITA that the circuit would store transaction logs. I understand that during prosecution of the ’949 Patent, Applicant expressly admitted that “implementation of a circuit to store transaction logs would be well understood by one of ordinary skill in the art.” *See supra* § V.B.1.

128. Therefore, in my opinion, a POSITA would have understood that *Dua* anticipates, or otherwise renders obvious, Claim 19.

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

129. *Dua* discloses every element of Claim 1. *See supra* § IX.B.i ('949 Patent Claim 1). As discussed above, *Dua* discloses that its circuitry includes a fingerprint scanner (biometric sensor), which authenticates a user. *See supra* §IX.B.ii ('949 Patent Claims 7 and 8). As further discussed above, the electronic switch enables RFID communication depending on whether a user is authenticated. *See supra* §IX.B.i.1[b] ('949 Patent Claim 1). Therefore, in my opinion, a POSITA would have understood that the electronic switch is responsive to the fingerprint scanner (biometric sensor).

130. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 20.

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

131. *Dua* discloses every element of Claim 1. *See supra* § IX.B.i ('949 Patent Claim 1). *Dua* discloses Claim 21, because as discussed above, *Dua* discloses a key pad (input) for entry of a PIN, and that RFID communication via the inductive coupling is responsive to the PIN. *See supra* §IX.B.ii ('949 Patent Claim 10).

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

132. *Dua* discloses every element of Claim 1. *See supra* § IX.B.i ('949 Patent Claim 1). *Dua* explains that “wireless device 200...is capable of wirelessly connecting to the Internet using network protocols such as...802.11a, 802.11b, [and] 802.11g.” EX1023, [0041] (“wireless device **200** is preferably a device that is capable of wirelessly connecting to the Internet using network protocols such as GSM/GPRS, CDMA2000, W-CDMA, EDGE, HDR, 1xRTT, UMTS, IMT-2000, 802.11a, 802.11b, 802.11g, or BLUETOOTH or other relevant protocols developed hereinafter.”), [0318], [0323], [0423]. Each of these is a WiFi protocol. Thus, *Dua*’s device is configured to communicate via WiFi.

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

134. Therefore, in my opinion, a POSITA would have understood that *Dua* renders obvious Claim 22.

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

135. *Dua* discloses every element of Claim 1. *See supra* § IX.B.i ('949 Patent Claim 1). As discussed, *Dua*'s device includes an inductive coupling. *See supra* §IX.B.i.1[a] ('949 Patent Claim 1). *Dua*'s device is also capable of RFID communication, and is therefore an RFID device. *Id.*

136. Therefore, in my opinion, a POSITA would have understood that *Dua* renders obvious Claim 23.

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

137. *Dua* discloses every element of Claim 1. *See supra* § IX.B.i ('949 Patent Claim 1). As discussed above, *Dua* discloses (1) PIN and biometric authentication mechanisms, which include an electronic switch, and (2) a wallet button (mechanical switch). *See supra* §§IX.B.i.1[b] ('949 Patent Claim 1), IX.B.ii ('949 Patent Claim 13). As further discussed above, both the electronic switch and the wallet button (mechanical switch) are configured to approve a financial transaction. *Id.*

138. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 26.

Claim 27: The system of claim 1, wherein the cellular phone is configured to purchase goods by placing the circuit within the reading range of a wireless point of sale device and

communicating a financial account number to the wireless point of sale device using the induction coupling responsive to the states of the circuit.

139. *Dua* discloses every element of Claim 1. *See supra* § IX.B.i ('949 Patent Claim 1). As discussed above, *Dua* discloses placing the wireless device (and the circuitry contained therein) within the reading range of a reader connected to a point-of-sale terminal to facilitate a transaction. *See supra* §IX.B.ii ('949 Patent Claims 14 and 15). *Dua* provides that an exemplary transaction includes “a grocery store POS purchase.” EX1023, [0352]. As further discussed above, *Dua* discloses that such a financial transaction is facilitated by communicating a financial account number to the reader via the inductive coupling responsive to the states of the circuit. *See supra* §§IX.B.i.1[b]-1[c] ('949 Patent Claim 1), IX.B.ii ('949 Patent Claims 5 and 9).

140. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 27.

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

141. *Dua* discloses every element of Claim 1. *See supra* § IX.B.i ('949 Patent Claim 1). As discussed above, *Dua* discloses an electronic switch responsive to fingerprint (biometric) authentication. *See supra* §§IX.B.i.1[b] ('949 Patent Claim 1), IX.B.ii ('949 Patent Claims 8 and 20). In my opinion, a POSITA would have

understood that, to enable the described fingerprint authentication, it would have been necessary, or at least obvious, to store the user's true fingerprint (biometric) data in device memory for comparison to the fingerprint (biometric) data received from the fingerprint scanner during a subsequent authentication attempt by the user. EX1023, [0041], [0366].

142. Therefore, in my opinion, a POSITA would have understood that *Dua* anticipates or otherwise renders obvious Claim 28.

iii. Independent Claim 29

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

143. In my opinion, a POSITA would have understood that *Dua* anticipates, or otherwise renders obvious, 29[pre], because as discussed above, its cellular telephone communicates wirelessly via RFID (using an inductive coupling) and WiFi. *See supra* §§IX.B.i.1[a] ('949 Patent Claim 1), IX.B.ii ('949 Patent Claim 22).

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

144. In my opinion, a POSITA would have understood that *Dua* discloses 29[a], because as discussed above, its device circuitry includes an inductive coupling, and facilitates RFID payments (financial transactions communicated via the inductive coupling). *See supra* §§IX.B.i.1[b]-1[c] ('949 Patent Claim 1), IX.B.ii

(’949 Patent Claim 5).

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

145. In my opinion, a POSITA would have understood that *Dua* discloses 29[b], because as discussed above, its device circuitry facilitates RFID payments (financial transactions) responsive to a fingerprint scanner (biometric sensor). *See supra* §IX.B.ii (’949 Patent Claim 8).

146. Therefore, in my opinion, a POSITA would have understood that *Dua* anticipates, or otherwise renders obvious, independent Claim 29.

iv.Independent Claim 30

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

147. 30[pre] is identical to 29[pre]. Therefore, in my opinion, a POSITA would have understood that *Dua* anticipates, or otherwise renders obvious, 30[pre] for the reasons discussed above. *See supra* §IX.B.iii.29[pre] (’949 Patent Claim 29).

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

148. 30[a] is identical to 29[a]. Therefore, in my opinion, a POSITA would have understood that *Dua* anticipates, or otherwise renders obvious, 30[a] for the reasons discussed above. *See supra* §IX.B.iii.29[a] (’949 Patent Claim 29).

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

149. *Dua* discloses 30[b], because as discussed above, its device circuitry facilitates RFID payments (financial transaction) responsive to a PIN entered by a user. *See supra* §IX.B.ii ('949 Patent Claim 10).

150. Therefore, in my opinion, *Dua* anticipates, or otherwise renders obvious, independent Claim 30.

C. GROUND 3: *Dua* in View of *Woike* Renders Obvious Claims 24 and 25

i. Motivation to Combine

151. In my opinion, a POSITA would have understood that *Dua* and *Woike* are both directed to electronic systems for conducting financial transactions using portable electronic devices. *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 (“The invention allows for automated cashless payments with a cell phone.”).

152. In my opinion, 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. In my opinion, a POSITA would have recognized that 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.

153. In my opinion, 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. The combination would involve implementing *Woike*’s contactless payments with *Dua*’s mobile device and wallet application, which, in my opinion, a POSITA would have understood to be a straightforward software implementation.

ii. Claims 24 and 25

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

154. *Dua*’s wireless device anticipates and/or renders obvious the limitations

of Claim 1, from which Claim 24 depends, for the reasons discussed above. *See supra* § IX.B.i ('949 Patent Claim 1).

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

156. *Woike* explains that the SIM card requires a PIN code, which prevents misuse of its payment methods. EX1025, p. 2, ll. 24-26 (“Because 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.”). In my opinion, it would have been obvious to a POSITA that the PIN code included in the SIM described by *Woike* is used to authenticate a user prior to facilitating the described financial transactions. Therefore, in my opinion, a POSITA would have understood that the PIN code is an account identifier, because through the authentication process, the PIN would be used to identify an account as belonging (or not belonging) to a user. When implementing the methods of *Woike* using the mobile device of *Dua*, the PIN code included in the SIM described by *Woike* can be used to authenticate a user for accessing the wallet

application.

157. Therefore, in my opinion, a POSITA would have understood that *Dua-Woike* renders obvious Claim 24.

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

158. Because in my opinion, a POSITA would have understood that *Woike*'s SIM card, which requires a PIN code, is configured to store a password for the reasons discussed above in §IX.C.ii ('949 Patent Claim 24), the combination of *Dua* in view of *Woike* renders obvious Claim 25. EX1025, p. 2, ll. 24-26.

D. GROUND 4: *Waters* in View of *Dua* Renders Obvious Claims 1-30

i. Motivation to Combine

159. In my opinion, a POSITA would have understood that *Waters* and *Dua* are both directed to mobile payment systems using wireless communication technology. *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 ("The mobile terminal (1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The 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 or obtain entry to a building (for example).”). *Dua* discloses a comprehensive mobile wallet application with RFID capabilities. *See supra* § VI.A; EX1023, [0011], [0336], [0383]. In my opinion, a POSITA would have understood that both references address the goal of improving data security in RFID applications. EX1023, [0382]–[0383]; EX1024, [0049]–[0050] (“The near field tag 41 may be selectively enabled and disabled in order to reduce the opportunity to obtain information from the near field tag 41 by an unauthorised reader.”), [0051]. In my opinion, a POSITA would have understood that 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.

160. In my opinion, a POSITA would have understood that both *Waters* and *Dua* address the problem of enabling secure financial transactions using mobile devices. *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] (“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.”). *Dua* provides detailed implementation of a wallet application with credential management and RFID communication. EX1023, [0295]–[0305], [0334]–[0347].

161. In my opinion, 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. Specifically, *Dua*'s detailed disclosures regarding credential storage, user authentication, and RFID communication, in my opinion, would have provided a POSITA with sufficient implementation details for *Waters*'s mobile payment system to make it commercially useful.

162. In my opinion, 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. The combination would involve using *Dua*'s wallet application implementation within *Waters*'s mobile transaction framework.

ii. Independent Claim 1

1[pre]: An electronic communication system comprising:

163. *Waters* discloses a mobile terminal (electronic communication system) including a near field or RFID tag, wherein the mobile terminal is operable to facilitate financial transactions. EX1024, Abstract ("use the near field tag (41) to make a payment"), [0045] ("use their RF tag to make payments"). *Waters* further explains that "[t]he mobile terminal 1 may be a handheld mobile telephone." *Id.*, [0020].

164. Therefore, in my opinion, a POSITA would have understood that

Waters in view of *Dua* discloses 1[pre].²

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

165. *Waters* explains that its device is a “[m]obile terminal...registered with [a] GSM/GPRS or UMTS (3G) mobile or cellular telecommunications network.” EX1024, [0020]. In my opinion, a POSITA would have understood that *Waters*’s device is a cellular telephone.

166. *Waters* further explains that its device “includes a near field or RFID tag **41**. The near field tag **41** operates in the unregulated RF band of 13.56 MHz in this embodiment although other frequencies could be used.” *Id.*, [0034]. *Waters*’s device carries out wireless RFID communication via an “inbuilt inductive antenna” configured to “exchange information with a tag reader when the two are brought in close proximity.” EX1024, [0035] (“The near field tag **41** may operate in accordance with ISO-IEC 14443 and ISO-IEC 15693 standards. The tag **41** includes an inbuilt inductive antenna that allows the card to exchange information with a tag reader when the two are brought into close proximity, as described above. The reader may emit an RF signal to supply power to the tag to communicate with it if the tag is ‘passive.’ If the tag is ‘active’ it will have a power supply and its operation is

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

independently of the reader. The near field tag **41** may transmit selected information, such as an ID number (GU ID).”). *Waters* further explains its “near field tag 41 may operate in accordance with ISO-IEC 14443 and ISO-IEC 15693 standards.” *Id.* To the extent that the inductive antenna of *Waters* does not explicitly disclose an inductive coupling, in my opinion, a POSITA would have understood that an inductive coupling naturally flows or is a natural result of the disclosure of *Waters* that teaches a “near field tag” including an “inbuilt inductive antenna” operating “in accordance with ISO-IEC 14443 and ISO-IEC 15693 standards.”

167. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* discloses 1[a].

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

168. Similar to *Dua*, *Waters* discloses the use of PIN or biometric authentication to implement RFID communication logic responsive to a PIN or biometric sensor. EX1024, [0052] (“the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader”). In my opinion, a POSITA would have understood that the PIN and biometric authentication mechanisms necessarily include an electronic switch that, in response to PIN or biometric entry, makes or breaks an electrical connection in the processing or control circuitry that executes the wallet application and controls

the embedded RF interface (*i.e.*, the circuit). In my opinion, a POSITA would have understood that the electronic switch, in response to PIN or biometric entry, makes or breaks an electrical connection in the circuit, causing an electronic signal to change the operative state of the circuit (*e.g.*, from disabled to enabled, from PIN-less to authenticated).

169. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious 1[b].

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

170. In my opinion, a POSITA would have understood that the near field tag 41 and its associated control circuitry (as identified in §IX.D.ii.1[b] ('949 Patent Claim 1)) is configured to communicate responsive to its own state, because that circuit has an enabled state in which the tag “is then able to communicate with readers” and a disabled state in which “a reader is not able to obtain any information from the near field tag 41, even when brought into close proximity thereto.” EX1024, [0037] (“According to an important feature of this embodiment, the near field tag **41** is selectively enabled or disabled for communication with the reader under control of the SIM **15**, by means of communication link **43**. By means of the link **43**, the SIM can enable or disable the near field tag **41** by, for example, rendering its antenna inoperative. 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 (within a range

that, in normal circumstances, near field communication would be possible).”), [0042]. In my opinion, a POSITA would have also understood that the near field tag 41 and its associated control circuitry (as identified in §IX.D.ii.1[b] (’949 Patent Claim 1)), that executes the wallet application of *Dua*, is configured to communicate responsive to its own state, because that circuit can transmit only PIN-less credentials in a PIN-less state and PIN-protected credentials in an authenticated state. The circuit enters the authenticated states when the electronic switch is activated by correct PIN or biometric entry. *Id.*, [0051]–[0052] (“The following arrangements are useful if the near field tag 41 is to be enabled and disabled for fairly long periods of time: (1) Personal identification number (PIN) entry—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. The user’s PIN may be stored in a secure location in the mobile terminal 1 or in the SIM 15. When the user enters their PIN using the keypad 37, the entered PIN is compared with the stored PIN. If the PINs match, the SIM transmits a message, via link 43, to the near field tag 41 to activate the near field tag. (2) Biometric data entry—the mobile terminal 1 may incorporate a fingerprint reader 45. The fingerprint reader 45 scans the fingerprint of the user when the user’s finger is placed on the reader 45 and compares it to the user’s fingerprint stored in the memory of the mobile terminal 1 or the SIM 15. If the fingerprints are determined to match, the message is sent from the SIM 15, via link 43, to the RF tag 41. As an

alternative to a fingerprint, other biometric data could be used—for example, voice recognition (using the mobile terminal's built-in microphone and a voice recognition algorithm within the mobile terminal **1** or SIM card **15**) or retinal scanning (using the mobile terminal's built-in camera)").

171. As discussed above, it would have been obvious to a POSITA that such communication would occur via an inductive coupling. *See supra* § IX.D.ii.1[a] ('949 Patent Claim 1).

172. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* discloses 1[c].

173. Therefore, in my opinion, *Waters* in view of *Dua* renders obvious independent Claim 1.

iii. Dependent Claims 2–28

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

174. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 1. *See supra* § IX.D.ii ('949 Patent Claim 1). As discussed above, it is my understanding that this limitation is recited in the alternative (using the word “or”), and it is therefore disclosed if at least one of the recited elements is met. *Waters* discloses that its device circuitry has at least memory and a power supply. EX1024,

[0035]–[0036] (“If the tag is “active” it will have a power supply and its operation is independently of the reader.”), [0051] (“The user's PIN may be stored in a secure location in the mobile terminal **1** or in the SIM **15**.”).

175. Further, to the extent that *Waters* and *Dua* do not expressly disclose a switchable RFID tag, input logic, processing logic, a return signal generator, switch logic, a switch state monitor, encryption logic, or one or more antenna, in my opinion, it would have been obvious to a POSITA to implement each of these components in the device of *Waters* in view of *Dua*, as these are necessary to enable the RFID payment functionality described above. *See supra* §§IX.D.i–ii (’949 Patent Claim 1).

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

176. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 2. *See supra* § IX.D.iii (’949 Patent Claim 2). As discussed above with respect to Grounds 1–2, *Dua*’s wallet application is configured such that when such a stored value credential “is waved in front of a reader at the turnstile, the electronic balance is automatically debited from the onboard chip” and “an over-the-air reload tool” can be programmed into the wallet application. EX1023, [0290], [0293]. As further discussed above, when applied to the device of *Waters*, in my opinion, a POSITA would have understood that debiting and reloading an electronic balance on the device similarly requires that the balance be stored in the device’s memory.

See supra §IX.B.ii ('949 Patent Claim 3).

177. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 3.

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

178. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 2. *See supra* § IX.D.iii ('949 Patent Claim 2). Similar to *Dua*, *Waters* discloses that its device includes a “keypad” (a type of user interface). EX1024, [0034], [0051]. As discussed above with respect to Grounds 1–2, *Dua* discloses that its wallet application is configured to receive a financial account number inputted by a user via a keypad. *See supra* § IX.B.ii ('949 Patent Claim 4). Therefore, in my opinion, a POSITA would have understood that when implemented in *Waters*’s device, the wallet application would receive a financial account number inputted by a user via *Waters*’s keypad (user interface).

179. As further discussed above, *Dua*’s wallet application controls the device to store a financial account number in memory. *See supra* §IX.B.ii ('949 Patent Claim 4). In my opinion, when implemented in *Waters*’s device, a POSITA would have understood that the financial account number would be stored in memory.

180. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 4.

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

181. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 1. *See supra* § IX.D.ii ('949 Patent Claim 1). As discussed above with respect to 1[c], in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious that the circuit is configured to control communication via the inductive coupling, responsive to the states of the circuit. *See supra* §IX.D.ii.1[c] ('949 Patent Claim 1).

182. Further, in my opinion, a POSITA would have understood that *Waters* and *Dua* both teach that such communication can facilitate a financial transaction. For example, *Waters* provides that the communication can be used to “make a payment.” EX1024, Abstract, [0043] (“OTA messages would be sent at the beginning and the end of the school lunch time so that the near field tag **41** could only be used to make a payment during the appropriate time.”). Similarly, *Dua* discloses that its circuitry can control a device to “transmit payment...information to a reader using the short-range transmission capability of the wireless device (e.g., RF).” EX1023, [0315] (“During 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).”).

183. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 5.

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

184. In my opinion, a POSITA would have understood that the mobile terminal of *Waters* incorporating the wallet application of *Dua* renders obvious Claim 6 for the same reasons discussed above in Grounds 1–2. *See supra* § IX.B.ii (’949 Patent Claim 6).

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

185. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 5. *See supra* § IX.D.iii (’949 Patent Claim 5). Similar to *Dua*, *Waters* discloses that its PIN and biometric authentication mechanisms include a keypad (used to capture a user’s PIN) and a fingerprint reader (used to capture a user’s fingerprint), respectively. EX1024, [0034], [0051] (“(1) Personal identification number (PIN) entry—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**. ... (2) Biometric data entry—the mobile terminal **1** may incorporate a fingerprint reader **45**. The fingerprint reader **45** scans the fingerprint of the user when the user's finger is placed

on the reader **45** and compares it to the user's fingerprint stored in the memory of the mobile terminal **1** or the SIM **15**.”). In my opinion, a POSITA would have understood *Waters*’s key pad and fingerprint scanner are user interfaces for the PIN and biometric authentication mechanisms, respectively, because they interface with the user to capture data (PIN or fingerprint) to enable these mechanisms.

186. Additionally, as explained above, the *Waters* in view of *Dua* device includes an electronic switch that enables transmission of certain credentials, responsive to the PIN or biometric authentication mechanisms. §§IX.D.ii.1[b]–1[c] (’949 Patent Claim 1), IX.D.iii (’949 Patent Claim 6). As discussed above, when the user is successfully authenticated using PIN or biometric authentication (via the key pad and fingerprint reader user interfaces), RFID communication of payment credentials is enabled (a financial transaction is approved) via the electronic switch. *Id.*

187. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 7.

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

188. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 5. *See supra* § IX.D.iii (’949 Patent Claim 5). In my opinion, a POSITA would have understood that *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]. In my opinion, 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. *Dua* also discloses making its wallet application functionality and transmission of financial credentials responsive to a fingerprint sensor. *See supra* §IX.B.ii (’949 Patent Claim 8). *Dua* explains that the wallet application “is specifically designed to store several types of electronic credentials,” including “Payment Methods” such as “[c]redit, debit/ATM, stored value, electronic check, and RFID payment methods.” EX1023, [0334], [0336]. The “credential record” contains “Account number” among other account-specific information. *Id.*, [0297], [0302]–[0304]. *Dua* further states that “[e]lectronic credentials issued to a user and stored in the wallet application can be

used” in a proximity transaction, where “the wireless device can transmit payment, identification, or other confidential information to a reader using the short-range transmission capability of the wireless device (e.g. RF).” *Id.*, [0313]–[0315].

189. As identified in § IX.D.ii, the “circuit” is the processing and control circuitry that executes the wallet application of *Dua* and controls the embedded RF interface. In my opinion, a POSITA would have understood that the circuitry is configured to facilitate the financial transaction and to communicate financial account information based on the functionality of the wallet application it executes. Thus, by making the wallet application functionality and transmission of financial credentials responsive to a fingerprint sensor, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 8.

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

190. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 5. *See supra* § IX.D.iii (’949 Patent Claim 5). In my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 9, because as discussed above with reference to Grounds 1–2, *Dua*’s wallet application (which, in the *Waters* in view of *Dua* combination, is implemented in *Waters*’s device) controls the device circuitry to communicate financial account information, including an “Account number,” via the inductive coupling to facilitate the financial

transaction. EX1023, [0297], [0302] (“Account number”), [0303] (“Expiration date of credential”), [0304] (“Special security information related to credential (e.g. CVV/CVC/CVV2/CVC2, etc)”), [0383]; *See supra* §IX.B.ii (’949 Patent Claim 9).

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

191. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 5. *See supra* § IX.D.iii (’949 Patent Claim 5).

192. As discussed above, the *Waters* in view of *Dua* device includes a keypad (input) for entry of a PIN, which is required to enable a financial transaction. *See supra* § IX.D.iii (’949 Patent Claim 7).

193. As further discussed above, when RFID transmission is enabled, the circuit can communicate financial account information via the inductive coupling to facilitate the financial transaction. *See supra* §IX.D.iii (’949 Patent Claim 5).

194. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 10.

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

195. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 5. *See supra* § IX.D.iii (’949 Patent Claim 5). *Waters* discloses that the

SIM stores “authentication information” in memory (key memory), which is used as an encryption key during an authentication process. EX1024, [0023] (“Each of the mobile terminals **1,11** and **13** is provided with a respective smart card or subscriber identity module (SIM) **15**. During the manufacturing process of each SIM, authentication information is stored thereon under the control of the mobile telecommunications network **3**. The mobile telecommunications network **3** itself stores details of each of the SIMs issued under its control. In operation of the mobile telecommunications network **3**, a terminal **1, 11, 13** is authenticated (for example, when the user activates the terminal in the network with a view to making or receiving calls) by the network sending a challenge to the terminal **1,11,13** incorporating a SIM **15**, in response to which the SIM **15** calculates a reply (dependent on the predetermined information held on the SIM—typically an authentication algorithm and a unique key K_i) and transmits it back to the mobile telecommunications network **3**. The mobile telecommunications network **3** includes an authentication processor **17** which generates the challenge and which receives the reply from the terminal **1,11,13**. Using information pre-stored concerning the content of the relevant SIM **15**, the authentication processor calculates the expected value of the reply from the mobile terminal **1,11,13**. If the reply received matches the expected calculated reply, the SIM **15** and the associated mobile terminal are considered to be authenticated.”). For example, *Waters* provides that a

telecommunications network can send a challenge to the SIM. *Id.* Then, the SIM “calculates a reply” “dependent on” the authentication information. *Id.* A processor connected to the telecommunications network then “calculates the expected value of the reply” and compares it to the reply sent by the SIM. *Id.* If these match, then the SIM is authenticated. *Id.*

196. In my opinion, a POSITA would have understood that the process described above would require the SIM to “calculate” the reply by encrypting the challenge message using the authentication information. Thus, in my opinion, a POSITA would have understood that the authentication information is an encryption key.

197. *Waters* further discloses that the RFID functionality (which, as discussed above, is carried out via an inductive coupling) can be enabled or disabled, depending on whether the SIM is authenticated by this process (*i.e.*, responsive to the authentication information). EX1024, [0036], [0046]-[0047] (“Typically, when the mobile terminal **1** is powered up within the coverage area of the mobile telecommunications network **3**, the authentication process between the SIM **15** and the authentication processor **17** of the network **3** occurs automatically. When this authentication has been completed, a message is sent to the near field tag **41**, via the link **43**, to enable operation of the tag. When the SIM **15** is no longer authenticated (for example, when the mobile terminal **1** is powered down), a further message is

sent from the SIM **15** to the near field tag **41**, via the link **43**, to deactivate the near field tag **41**.”); *See supra* §IX.D.ii.1[b] (’949 Patent Claim 1). Therefore, in my opinion, a POSITA would have understood that RFID transactions are facilitated by successful authentication using the authentication information.

198. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 11.

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

199. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 5. *See supra* § IX.D.iii (’949 Patent Claim 5). In my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 12, because as discussed above, its device includes a key memory configured to store authentication information (key), which is required to enable RFID communication (change the states of the circuit) to facilitate a financial transaction, which is made via the inductive coupling. *See supra* §§IX.D.ii.1[a]–[c] (’949 Patent Claim 1), IX.D.iii (’949 Patent Claim 11).

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

200. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 5. *See supra* § IX.D.iii (’949 Patent Claim 5). Similar to *Dua*, *Waters*

discloses that its device can include a “pressure sensor...[that] acts as a switch” to enable RFID communication. EX1024, [0053] (“(2) Pressure sensor—a pressure sensor on the casing of mobile terminal 1 acts as a switch. The RF tag 41 is only enabled when the user physically presses the pressure sensor. Therefore, when the mobile terminal is in a case or the user’s pocket, the pressure sensor is disabled. The pressure sensor may itself be deactivated by the user, for example, when a function of the mobile terminal 1 is selected such that the keypad 37 is inoperative.”), [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]. In my opinion, a POSITA would have understood that the pressure sensor is 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]; *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.”).

201. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 13.

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

202. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 5. *See supra* § IX.D.iii ('949 Patent Claim 5). *Waters* states that its device can “exchange information with a tag reader when the two are brought into close proximity.” EX1024, [0035]. Such an information exchange can be used to “make a payment” at a reader. *Id.*, Abstract; *see also id.*, [0041]–[0043] (“In the second example, a user wishes to use the near field tag **41** of the mobile terminal **1** to pay for travel by public transport (for example on the London Underground), where entry barriers are equipped with a suitable near field tag reader.”), [0045] (“ For example, a school child's parent may set the times during which the school child is able to use their RF tag to make payments, in the example given above relating to paying for a school lunch.”).

203. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 14.

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

204. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 14. *See supra* § IX.D.iii ('949 Patent Claim 14). In my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 15 for the same reasons discussed above, with respect to Claim 14, because in my opinion it would have been obvious to a POSITA that *Waters*'s reader would be located within a point of sale, to reduce complexity and cost. *See supra* § IX.D.iii ('949 Patent Claim

14).

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

205. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 1. *See supra* § IX.D.iii ('949 Patent Claim 1). In my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 16, because as discussed above, *Dua*'s wallet application (which, in the *Waters* in view of *Dua* combination, is implemented in *Waters*'s device) controls the device circuitry to operate in an authenticated state (first ON state) and a PIN-less state (second ON state), responsive to the electronic switch. *See supra* §IX.B.ii ('949 Patent Claim 16).

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

206. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 16. *See supra* § IX.D.iii ('949 Patent Claim 16). In my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 17, because as discussed above, *Dua*'s wallet application (which, in the *Waters* in view of *Dua* combination, is implemented in *Waters*'s device) controls the device circuitry to facilitate a financial transaction in the authenticated state (first ON state) but not in the PIN-less state (second ON state). *See supra* §§IX.B.ii ('949 Patent

Claims 16 and 17).

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

207. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 1. *See supra* § IX.D.ii ('949 Patent Claim 1). In my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 18, because as discussed above in Grounds 1–2, in my opinion, a POSITA would have understood that, to enable implementation of the software-based logic described above, it would have been necessary, or at least obvious, for the processing and control circuitry to store its states in memory (state memory). *See supra* §IX.B.ii ('949 Patent Claim 18).

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

208. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 1. *See supra* § IX.D.ii ('949 Patent Claim 1). In my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 19, because as discussed above with respect to Grounds 1–2, *Dua*'s wallet application (which, in *Waters* in view of *Dua*, is implemented in *Waters*'s device) controls the device circuit to store transaction logs. *See supra* §§III.B (during prosecution, Applicant expressly admitted that “implementation of a circuit to store transaction logs would be well understood by one of ordinary skill in the art”), IX.B.ii ('949

Patent Claim 19).

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

209. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 1. *See supra* § IX.D.ii ('949 Patent Claim 1). As discussed above, the *Waters* in view of *Dua* circuitry includes a fingerprint reader (biometric sensor), which authenticates a user. *See supra* §§IX.D.iii ('949 Patent Claims 7 and 8). As further discussed above, the electronic switch enables RFID communication depending on whether a user is authenticated. *See supra* §IX.D.ii.1[b] ('949 Patent Claim 1). Therefore, in my opinion, a POSITA would have understood that the electronic switch is responsive to the fingerprint scanner (biometric sensor).

210. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 20.

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

211. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 1. *See supra* § IX.D.ii ('949 Patent Claim 1). In my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 21, because as discussed above, its device includes a keypad (input) for entry of a PIN, and RFID communication via the inductive coupling is responsive to the PIN. *See*

supra §IX.D.iii ('949 Patent Claim 10).

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

212. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 1. *See supra* § IX.D.ii ('949 Patent Claim 1). *Waters* explains that its device can communicate “with a network...via a UMA ‘access point.’” EX1024, [0024] (“For example, the terminal may communicate with the network via the fixed telephone network (PSTN), via a UMA ‘access point’ and/or via the Internet.”). Unlicensed Mobile Access (“UMA”) is a telecommunications standard that enables mobile phones to route data over unlicensed IP-based networks, including WiFi networks. To the extent *Waters* does not expressly describe a separate WiFi antenna, in my opinion, providing one would have been necessary, or at least obvious to a POSITA, in order to implement the UMA connectivity *Waters* describes. Further, in my opinion, a POSITA would have understood that such a WiFi antenna would be tuned to 2.4 GHz or 5 GHz, both of which are different frequencies than the 13.56 MHz frequency used for *Waters*’s RFID communication described above. EX1024, [0034].

213. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 22.

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

214. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 1. *See supra* § IX.D.ii ('949 Patent Claim 1).

215. As discussed above, the *Waters* in view of *Dua* device includes an inductive coupling. *See supra* §IX.D.ii.1[a] ('949 Patent Claim 1). The *Waters* in view of *Dua* device is also capable of RFID communication, and, in my opinion, a POSITA would have understood that is therefore an RFID device. *Id.*

216. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 23.

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

217. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 1. *See supra* § IX.D.ii ('949 Patent Claim 1).

218. *Waters* explains that its device includes a “subscriber identity module (SIM) 15.” EX1024, [0023]. A SIM card is a component that is inserted into a device, such as a cellular telephone.

219. *Waters* explains that the SIM can store “authentication information,” which can be used to authenticate whether “a particular user...has a particular pre-paid account with a network.” EX1024, [0023], [0026] (“Nevertheless, such a user

cannot make use of the network until the network has authenticated the user's SIM—that is, has confirmed that such user is a particular user who has a particular pre-paid account with a network.”); *see also supra* §IX.D.iii ('949 Patent Claim 11). In my opinion, a POSITA would have understood the authentication information to be an account identifier, because it can be used to identify a user's account. *Waters* further explains that the RFID functionality (which, as discussed above, is carried out via an inductive coupling) can be enabled or disabled, depending on whether the SIM is successfully authenticated using the authentication information (account identifier). EX1024, [0036] (“In order to improve the security of the near field tag, in the present embodiment it is proposed to use the SIM **15** of mobile terminal **1** to control to some extent the operation of the near field tag **41**. The authentication process of a SIM **15** with a mobile telecommunications network, using the network's authentication processor **17** is considered to be highly secure. In this embodiment, this authentication of the SIM **15** is used to protect data held by the memory of the near field tag **41** from unauthorised access.”), [0046]-[0047]; *See supra* §IX.D.ii.1[b] ('949 Patent Claim 1).

220. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 24.

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

221. *Waters* in view of *Dua* discloses and/or renders obvious every element

of Claim 24. *See supra* § IX.D.iii ('949 Patent Claim 24). *Waters* discloses that the “The user's PIN may be stored in a secure location in the mobile terminal **1** or in the SIM **15**.” EX1024, [0051], [0060]. As discussed above, the PIN is used as a password to enable RFID communication. *Id.*; *See supra* §IX.D.iii ('949 Patent Claim 7).

222. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 25.

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

223. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 1. *See supra* § IX.D.ii ('949 Patent Claim 1). As discussed above, the *Waters* in view of *Dua* device includes (1) PIN and biometric authentication mechanisms, which include an electronic switch, and (2) a pressure sensor (mechanical switch). *See supra* §§IX.D.ii.1[b] ('949 Patent Claim 1), IX.D.iii ('949 Patent Claim 13). As further discussed above, both the electronic switch and the pressure sensor (mechanical switch) are configured to approve a financial transaction. *Id.*

224. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 26.

Claim 27: The system of claim 1, wherein the cellular phone is configured to purchase goods by placing the circuit within

the reading range of a wireless point of sale device and communicating a financial account number to the wireless point of sale device using the induction coupling responsive to the states of the circuit.

225. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 1. *See supra* § IX.D.ii ('949 Patent Claim 1). As discussed above, *Waters* discloses placing the wireless device (and the circuitry contained therein) within the reading range of a reader connected to a point-of-sale terminal to facilitate a transaction. *See supra* §IX.D.iii ('949 Patent Claims 14 and 15). *Waters* provides that “[a] similar arrangement could be used, for example, to enable a school child to pay for their lunch using the near field tag **41**.” EX1024, [0043]. As further discussed above, a financial transaction is facilitated by communicating a financial account number to the reader via the inductive coupling responsive to the states of the circuit. *See supra* §§IX.D.ii.1[b]-1[c] ('949 Patent Claim 1), IX.D.iii ('949 Patent Claims 5 and 9).

226. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 27.

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

227. *Waters* in view of *Dua* discloses and/or renders obvious every element of Claim 1. *See supra* § IX.D.ii ('949 Patent Claim 1). As discussed above, *Waters*

discloses an electronic switch responsive to fingerprint (biometric) authentication. *See supra* §§IX.D.ii.1[b] ('949 Patent Claim 1), IX.D.iii ('949 Patent Claims 8 and 20). In one example, a “fingerprint reader 45 scans the fingerprint of the user when the user’s finger is placed on the reader 45 and compares it to the user’s fingerprint stored in the memory of the mobile terminal 1 or the SIM 15.” EX1024, [0051]. If the captured fingerprint matches the stored fingerprint, then RFID communication is enabled. *Id.*

228. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 28.

iv. Independent Claim 29

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

229. *Waters* in view of *Dua* renders obvious 29[pre], because as discussed above, its cellular telephone communicates wirelessly via RFID (using an inductive coupling) and WiFi. *See supra* §§IX.D.ii.1[a] ('949 Patent Claim 1), IX.D.iii ('949 Patent Claim 22).

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

230. *Waters* in view of *Dua* renders obvious 29[a], because as discussed above, its device circuitry includes an inductive coupling, and facilitates RFID

payments (financial transactions communicated via the inductive coupling). *See supra* §IX.D.ii.1[b]-1[c] ('949 Patent Claim 1), IX.D.iii ('949 Patent Claim 5).

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

231. *Waters* in view of *Dua* renders obvious 29[b], because as discussed above, its device circuitry facilitates RFID payments (financial transactions) responsive to a fingerprint scanner (biometric sensor). *See supra* §IX.D.iii ('949 Patent Claim 8).

Therefore, *Waters* in view of *Dua* renders obvious independent Claim 29.

v. Independent Claim 30

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

232. 30[pre] is identical to 29[pre]. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious 30[pre] for the reasons discussed above. *See supra* §IX.D.iv.29[pre] ('949 Patent Claim 29).

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

233. 30[a] is identical to 29[a]. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious 30[a] for the reasons discussed above. *See supra* §IX.D.iv.29[a] ('949 Patent Claim 29).

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

234. *Waters* in view of *Dua* renders obvious 30[b], because as discussed above, its device circuitry facilitates RFID payments (financial transaction) responsive to a PIN entered by a user. *See supra* §IX.D.iii ('949 Patent Claim 10).

235. Therefore, *Waters* in view of *Dua* renders obvious independent Claim 30.

X. THE '734 PATENT

A. SUMMARY OF PRIOR ART GROUNDS

Ground	Claims	Basis	Prior Art
1	1–10, 13–21, 23–28, 30	Anticipation	<i>Dua</i>
2	1–10, 13–21, 23–28, 30	Obviousness	<i>Dua</i>
3	11, 12, 22, 29	Obviousness	<i>Dua</i> with <i>Woike</i>
4	1–30	Obviousness	<i>Dua</i> with <i>Waters</i>

B. GROUNDS 1-2: *Dua*

236. *Dua* anticipates and/or renders obvious claims 1–10, 13–21, 23–28, and 30.

i. Independent Claim 1

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

237. 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] (“During 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). 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.”). Therefore, in my opinion, a POSITA would have understood that *Dua* discloses 1[Pre].

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

238. *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] (emphasis added).

239. *Dua*’s wireless device (cellular phone) can be placed within reading range of a wireless POS device. 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. In my opinion, 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. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Limitation 1[a].

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

240. *See supra* § IX.B.i.1[a] (’949 Patent Claim 1).

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

241. *See supra* § IX.B.i.1[b] (’949 Patent Claim 1).

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

242. *See supra* § IX.B.i.1[b] (’949 Patent Claim 1).

1[e]: activating the electronic switch within the cellular telephone to change the state of the circuit; and

243. *Dua* discloses Limitation 1[e] for the reasons discussed above in § IX.B.i.1[c] (’949 Patent Claim 1). Specifically, in my opinion, a POSITA would have understood that the PIN and biometric authentication mechanisms taught by *Dua* necessarily disclose an electronic switch that, in response to a correct PIN or 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). In my opinion, a POSITA would have further

understood 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). Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Limitation 1[e].

1[f]: 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 financial account information using the inductive coupling.

244. *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 supra* §§ X.B.i.1[Pre] ('734 Patent Claim 1), 1[b]-1[d]. As discussed above, while *Dua* does not expressly use the phrase “inductive coupling,” inductive coupling naturally flows from or is the natural result of the disclosure of *Dua* teaching such RFID communication, in particular because of *Dua*’s disclosure of NFC technology. *See supra* § X.B.i.1[b] ('734 Patent Claim 1).

245. *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. §§ IX.B.i.1[c], 1[e] (’949 Patent Claim 1). For example, in my opinion, a POSITA would have understood that 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. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Limitation 1[f].

246. Therefore, in my opinion, a POSITA would have understood that *Dua* anticipates or renders obvious independent Claim 1.

ii. Dependent Claims 2-10, 13, 14

2[Pre]: The method of claim 1,

247. *See supra* § X.B.i (’734 Patent Claim 1).

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

248. *See supra* § IX.B.ii (’949 Patent Claim 16).

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

249. *See supra* § IX.B.ii (’949 Patent Claim 18).

3[Pre]: The method of claim 1,

250. *See supra* § X.B.i ('734 Patent Claim 1).

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

251. *See supra* § IX.B.ii ('949 Patent Claim 16).

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

252. *Dua* describes various categories of information that can be contained in its wallet application, including “Personal Information—Name, billing address, shipping address, home phone number, business phone number, fax number, social security number, and date of birth. Electronic business cards could also be stored.” EX1023, [0343]. *Dua* discloses that the circuit identified in § IX.B.i has a first ON state (*i.e.*, the PIN-less state) and a second ON state (*i.e.*, the authenticated state), as discussed in § IX.B.ii ('734 Patent Limitation 2[a]). A user can “designate specific credentials in their wallet as requiring advance PIN-entry and others to function without the prior input of the wallet PIN.” *Id.*, [0368]. In the first ON state, the circuit transmits only “a credential that has a ‘reader key’ and is approved for PIN-less transactions” (*e.g.*, less-sensitive personal information). *Id.*, [0383]; *see also id.*, [0369]-[0370]. Once the electronic switch is activated by correct biometric entry and the circuit enters the second ON state, the circuit can transmit the PIN-less credentials, plus PIN-protected credentials (*e.g.*, payment and other sensitive

personal information) to carry out a credit card or debit card transaction. *Id.*, [0393] (“Pressing buttons 1 or 2 could in addition to transmitting a payment method, also transfer a PIN-less credential that has a ‘reader key’ associated with it—provided that the reader sent the key in its initial communication with the wireless device.”). Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Limitation 3[b].

253. In my opinion, a POSITA would have understood that *Dua* anticipates or renders obvious Claim 3.

Claim 4: The method of claim 1, wherein the circuit is configured to store transaction logs.

254. *See supra* § IX.B.ii (’949 Patent Claim 19).

Claim 5: The method of claim 1, wherein the electronic switch is configured for a user to select between a plurality of financial accounts for the financial transaction.

255. *See supra* § IX.B.ii (’949 Patent Claim 6).

Claim 6: The method of claim 1, wherein the electronic switch is configured to enter a personal identification number or a password.

256. *Dua* discloses every element of Claim 1. *See supra* § X.B.i (’734 Patent Claim 1). *Dua* describes that “[t]he default security setting in the wallet application is that PIN-entry is required before the wallet application can be ‘opened’ and any credentials transmitted to an external device.” EX1023, [0366]. *Dua* further discloses that a user “may be required to input a PIN and click ‘OK’ to enable RF

communication for a 30 second window” or to “input his PIN, click ‘OK’ to initiate PIN verification, and upon positive confirmation be prompted to hold down either button 1 or 2 while placing the device in close proximity to a reader.” *Id.*, [0395].

257. In my opinion, a POSITA would have understood that this PIN-based authentication mechanism necessarily discloses the same electronic switch identified in § IX.B.i.1[c] ('949 Patent Claim 1), which, in response to correct PIN entry, makes or breaks an electrical connection in the processing and control circuitry that executes the wallet application and controls the embedded RF interface (*i.e.*, the circuit). In my opinion, a POSITA would further understand that the electronic switch, in response to PIN entry, makes or breaks an electrical connection in the circuit (*i.e.*, enters the PIN), causing an electronic signal to change the operative state of the circuit. *See also* § IX.B.i.1[c] ('949 Patent Claim 1).

258. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 6.

Claim 7: The method of claim 1, wherein the circuit is configured to communicate an account number via the inductive coupling to facilitate the financial transaction.

259. *See supra* § IX.B.ii ('949 Patent Claim 9).

Claim 8: The method of claim 1, wherein the cellular telephone includes a key memory configured to store an encryption key used to facilitate the financial transaction.

260. *See supra* § IX.B.ii ('949 Patent Claim 11).

Claim 9: The method of claim 1, wherein the cellular telephone includes a key memory configured to store a key required to change the state of the circuit to facilitate the financial transaction via the inductive coupling.

261. *See supra* § IX.B.ii ('949 Patent Claim 12).

Claim 10: The method of claim 1, wherein the cellular telephone includes an antenna configured to communicate using WiFi, the antenna being configured to operate at a different radio frequency than the inductive coupling.

262. *Dua* discloses every element of Claim 1. *See supra* § X.B.i ('734 Patent Claim 1). *Dua* provides that “wireless device 200...is capable of wirelessly connecting to the Internet using network protocols such as...802.11a, 802.11b, [and] 802.11g.” EX1023, [0041] (“wireless device **200** is preferably a device that is capable of wirelessly connecting to the Internet using network protocols such as GSM/GPRS, CDMA2000, W-CDMA, EDGE, HDR, 1xRTT, UMTS, IMT-2000, 802.11a, 802.11b, 802.11g, or BLUETOOTH or other relevant protocols developed hereinafter.”), [0318], [0323], [0423]. Each of these is a WiFi protocol. Therefore, in my opinion, a POSITA would have understood that *Dua*’s device is configured to communicate via WiFi.

263. In my opinion, a POSITA would have understood that to the extent *Dua* does not expressly describe a separate WiFi antenna, providing one would have been obvious, and indeed necessary, to implement *Dua*’s 802.11 (WiFi) functionality. Further, in my opinion, a POSITA would have understood that such a WiFi antenna

would be tuned to 2.4 GHz or 5 GHz, both of which are different frequencies than the 13.56 MHz frequency used for *Dua*'s RFID communication described above.

264. Therefore, in my opinion, a POSITA would have understood that *Dua* renders obvious Claim 10.

Claim 13: The method of claim 1, wherein the circuit includes both the electronic switch and a mechanical switch configured to approve the financial transaction.

265. *See supra* § IX.B.ii ('949 Patent Claim 26).

Claim 14: The method of claim 1, wherein activating the electronic switch is responsive to data stored in memory of the cellular telephone and the data stored in memory includes biometric data.

266. *Dua* discloses every element of Claim 1. *See supra* § X.B.i ('734 Patent Claim 1). *Dua* discloses "activating the electronic switch within the cellular telephone to change the state of the circuit, activation of the electronic switch being responsive to a biometric sensor included in the cellular telephone." *See supra* § IX.B.i.1[e] ('949 Patent Claim 1). In my opinion, a POSITA would have understood that, to enable implementation of the software-based logic described above (authentication using biometric verification via a fingerprint scanner), it would have been necessary, or at least obvious, for the circuit to store the user's biometric data in memory for comparison to the biometric data entered, and that activation of the electronic switch is therefore responsive to that stored biometric data. EX1023, [0366]. Therefore, in my opinion, a POSITA would have understood that *Dua*

discloses Claim 14.

iii.Independent Claim 15

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

267. *See supra* § X.B.i.1[Pre] ('734 Patent Claim 1).

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

268. *See supra* § X.B.i.1[a] ('734 Patent Claim 1).

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

269. *See supra* § IX.B.i.1[a] ('949 Patent Claim 1).

15[c]: 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;

270. *See supra* § IX.B.i.1[b] ('949 Patent Claim 1).

15[d]: activating the electronic switch within the cellular telephone to change the state of the circuit; and

271. *See supra* § X.B.i.1[e] ('734 Patent Claim 1).

15[e]: 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 financial account information using the inductive coupling,

272. *See supra* § X.B.i.1[f] ('734 Patent Claim 1).

15[f]: wherein the cellular telephone is configured for a user to enter a personal identification number (PIN), communication of the financial account information via the inductive coupling being responsive to the personal identification number.

273. *Dua* describes that “[t]he default security setting in the wallet application is that PIN-entry is required before the wallet application can be ‘opened’ and any credentials transmitted to an external device.” EX1023, [0366]. *Dua* further discloses that a user “may be required to input a PIN and click ‘OK’ to enable RF communication for a 30 second window” or to “input his PIN, click ‘OK’ to initiate PIN verification, and upon positive confirmation be prompted to hold down either button 1 or 2 while placing the device in close proximity to a reader.” *Id.*, [0395].

274. In my opinion, a POSITA would have understood that this PIN-based authentication mechanism necessarily discloses the same electronic switch identified in § IX.B.i.1[c] (’949 Patent Claim 1), which, in response to correct PIN entry, makes or breaks an electrical connection in the processing and control circuitry that executes the wallet application and controls the embedded RF interface (*i.e.*, the circuit). In my opinion, a POSITA would have further understood that the electronic switch, in response to PIN entry, makes or breaks an electrical connection in the circuit, causing an electronic signal to change the operative state of the circuit (*e.g.*, from disabled to enabled; from PIN-less to authenticated). *See also* § IX.B.i.1[c] (’949 Patent Claim 1). In my opinion, a POSITA would have understood

that because the state of the circuit is responsive to the PIN, and the communication of the financial information via the inductive coupling is responsive to the state of the circuit (*See supra* § IX.B.i.1[d] ('949 Patent Claim 1)), *Dua* discloses Limitation 15[f].

275. In my opinion, a POSITA would have understood that *Dua* anticipates or renders obvious independent Claim 15.

iv. Dependent Claims 16-21

16[Pre]: The method of claim 15,

276. *See supra* § X.B.iii ('734 Patent Claim 15).

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

277. *See supra* § IX.B.ii ('949 Patent Claim 16).

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

278. *See supra* § IX.B.ii ('949 Patent Claim 18).

17[Pre]: The method of claim 15,

279. *See supra* § X.B.iii ('734 Patent Claim 15).

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

280. *See supra* § IX.B.ii ('949 Patent Claim 16).

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

281. *See supra* § X.B.ii ('734 Patent Limitation 3[b]).

Claim 18: The method of claim 15, wherein the electronic switch is configured for a user to select between a plurality of financial accounts for the financial transaction.

282. *See supra* § IX.B.ii ('949 Patent Claim 6).

Claim 19: The method of claim 15, wherein the circuit is configured to communicate an account number via the inductive coupling to facilitate the financial transaction.

283. *See supra* § IX.B.ii ('949 Patent Claim 9).

Claim 20: The method of claim 15, wherein the cellular telephone includes a key memory configured to store a key required to change the state of the circuit to facilitate the financial transaction via the inductive coupling.

284. *See supra* § IX.B.ii ('949 Patent Claim 12).

Claim 21: The method of claim 15, wherein activating the electronic switch is responsive to data stored in memory of the cellular telephone and the data stored in memory includes biometric data.

285. *Dua* discloses every limitation of Claim 15. *See supra* § X.B.iii ('734 Patent Claim 15). As discussed above, in my opinion, a POSITA would have understood that *Dua* discloses the use of PIN-based (§ X.B.iii.15[f]) and biometric-based (§ X.B.ii ('734 Patent Claim 14)) authentication mechanisms to facilitate financial transactions. *Dua* also describes a dual-authentication scheme using both PIN and biometric authentication mechanisms.

286. *Dua* describes that, separate from wallet application authentication, “[c]ertain credential issuers such as financial institutions may require that users

validate their identity during a transaction by providing a PIN that was established with or set by the financial institution.” EX1023, [0397]. *Dua* further describes: “credential issuers may issue a credential to a wireless device, require the wallet PIN with every transaction, but also prompt the user for an issuer PIN (or PIN set with the issuer) on the POS terminal during each transaction. The POS terminal may know to prompt for a PIN based on a card BIN number for example.” *Id.*, [0402]. Since *Dua*’s mobile device is configured for PIN-entry (*see* EX1023, [0366]), in my opinion, it would have been obvious to a POSITA that this dual-authentication scheme (*i.e.*, biometric entry to open the wallet application followed by issuer PIN entry to facilitate the transaction) could be executed by utilizing the fingerprint sensor and the PIN-entry functionalities of the mobile device itself.

287. In my opinion, a POSITA would have understood that *Dua* anticipates or renders obvious Claim 21.

v.Independent Claim 23

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

288. *See supra* § X.B.i.1[Pre] (’734 Patent Claim 1).

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

289. *See supra* § X.B.i.1[a] (’734 Patent Claim 1).

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

290. *See supra* § IX.B.i.1[a] ('949 Patent Claim 1).

23[c]: 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;

291. *See supra* § IX.B.i.1[b] ('949 Patent Claim 1).

23[d]: activating the electronic switch within the cellular telephone to change the state of the circuit; and

292. *See supra* § X.B.i.1[e] ('734 Patent Claim 1).

23[e]: 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 financial account information using the inductive coupling,

293. *See supra* § X.B.i.1[f] ('734 Patent Claim 1).

23[f]: wherein the cellular telephone includes a user interface configured to enter a financial account number and includes memory configured to store the financial account number for use in the financial transaction.

294. *Dua* states that the wallet application may request the user to enter “such information as the user’s account number with the issuer.” EX1023, [0444]. *Dua* further provides that “[t]he wallet application is specifically designed to store several types of electronic credentials.” *Id.*, [0334]. These credentials are stored in memory. *Id.*, [0381]. *Dua* further provides that the credential record contains an “Account number” that is transmitted via the RFID interface. EX1023, [0297], [0302]-[0304], [0383]. Therefore, in my opinion, a POSITA would have understood

that *Dua* discloses Limitation 23[f].

295. In my opinion, a POSITA would have understood that *Dua* anticipates or renders obvious independent Claim 23.

vi. Dependent Claims 24-28, 30

24[Pre]: The method of claim 23,

296. *See supra* § X.B.v.

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

297. *See supra* § IX.B.ii ('949 Patent Claim 16).

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

298. *See supra* § IX.B.ii ('949 Patent Claim 18).

25[Pre]: The method of claim 23,

299. *See supra* § X.B.v.

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

300. *See supra* § IX.B.ii ('949 Patent Claim 16).

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

301. *See supra* § X.B.ii ('734 Patent Limitation 3[b]).

Claim 26: The method of claim 23, wherein the electronic switch is configured for a user to select between a plurality of financial accounts for the financial transaction.

302. *See supra* § IX.B.ii ('949 Patent Claim 6).

Claim 27: The method of claim 23, wherein the circuit is configured to communicate an account number via the inductive coupling to facilitate the financial transaction.

303. *See supra* § IX.B.ii ('949 Patent Claim 9).

Claim 28: The method of claim 23, wherein the cellular telephone includes a key memory configured to store a key required to change the state of the circuit to facilitate the financial transaction via the inductive coupling.

304. *See supra* § IX.B.ii ('949 Patent Claim 12).

Claim 30: The method of claim 23, wherein communicating the financial account information is responsive to biometric data stored in memory of the cellular telephone.

305. *See supra* § X.B.ii ('734 Patent Claim 14).

C. GROUND 3: *Dua* in View of *Woike* Renders Obvious Claims 11, 12, 22, AND 29

i. Motivation to Combine

306. The motivation to combine *Dua* and *Woike* is the same as discussed above. *See supra* § IX.C.i.

ii. Claim Analysis

11[Pre]: The method of claim 1,

307. *See supra* § X.B.i ('734 Patent Claim 1).

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

308. *Woike* explains that “[b]ecause current cell phones can only be used with a SIM card (Subscriber Identity Module card), which usually has a PIN code,

prevention of misuse of this payment method requires no additional precautions.” EX1025, p. 2, ll. 24-26. In my opinion, a POSITA would have understood that a SIM card including a PIN code (*i.e.*, an electronic key) is a separate component that is inserted into a device such as a cellular telephone. In my opinion, a POSITA would have understood that thus, *Dua* in view of *Woike* renders obvious Limitation 11[a].

11[b]: the electronic key including a financial account identifier and a signal communicated via the inductive coupling to facilitate the financial transaction being responsive to the financial account identifier.

309. *Woike* explains that the SIM card requires a PIN code, which prevents misuse of its payment methods. EX1025, p. 2, ll. 24-26. In my opinion, it would have been obvious to a POSITA that the PIN code included in the SIM described by *Woike* is used to authenticate a user prior to facilitating the described financial transactions. In my opinion, a POSITA would have understood that the PIN code is a financial account identifier, because through the authentication process, the PIN would be used to identify an account as belonging (or not belonging) to a user. In my opinion, a POSITA would have understood that when implementing the methods of *Woike* using the mobile device of *Dua*, the PIN code included in the SIM described by *Woike* can be used to authenticate a user for accessing the wallet application.

310. Therefore, in my opinion *Dua* in view of *Woike* anticipates or renders obvious Claim 11.

12[Pre]: The method of claim 1,

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

12[b]: the electronic key including an account identifier and the communication via the inductive coupling being responsive to the account identifier,

12[c]: the electronic key being configured to store a password or personal identification number.

311. *See supra* § X.C.ii (Limitations 11[Pre]-[b]).

22[Pre]: The method of claim 15,

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

22[b]: the electronic key including an account identifier,

22[c]: the electronic key being configured to store the personal identification number.

312. *See supra* § X.C.ii (Claims 11-12).

29[Pre]: The method of claim 23,

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

29[b]: the electronic key including an account identifier and the communication via the inductive coupling being responsive to the account identifier,

29[c]: the electronic key being configured to store a password or personal identification number.

313. *See supra* § X.C.ii (Claims 11-12).

D. GROUND 4: *Waters* in View of *Dua* Renders Obvious Claims 1-30

i. Motivation to Combine

314. The motivation to combine *Waters* and *Dua* is the same as discussed above. *See supra* § IX.D.i.

ii. Independent Claim 1

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

315. 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”). Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious 1[Pre].³

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

316. *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

³ *Dua* also discloses each limitation of Claims 1-10, 13-21, 23-28, and 30 for the reasons discussed above in Grounds 1-2. *See supra* § X.B.

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]. In my opinion, a POSITA would have understood that the tag reader disclosed in *Waters* corresponds to “a wireless point of sale device” as recited in Claim 1. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Limitation 1[a].

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

317. *See supra* § IX.D.ii.1[a] (’949 Patent Claim 1).

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

318. *See supra* § IX.D.ii.1[b] (’949 Patent Claim 1).

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

319. *See supra* § IX.D.ii.1[b] (’949 Patent Claim 1).

1[e]: activating the electronic switch within the cellular telephone to change the state of the circuit; and

320. *Waters* discloses Limitation 1[e] for the reasons discussed above in § IX.D.ii.1[c] (’949 Patent Claim 1). Specifically, in my opinion, a POSITA would have understood that the PIN and biometric authentication mechanisms taught by *Waters* necessarily disclose an electronic switch that, in response to a correct PIN or 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. In my opinion, a POSITA would have further understood 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). Therefore, in my opinion, a POSITA would have understood that *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 state of the circuit to facilitate the financial transaction, the communication of the financial account information using the inductive coupling.

321. *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 supra* §§ X.D.ii.1[Pre], 1[b]-1[d] ('734 Patent Claim 1).

322. In my opinion, 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. *Dua* also discloses this limitation. *See supra* § X.B.i.1[f] ('734 Patent Claim 1). *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]. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Limitation 1[f].

323. In my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious independent Claim 1.

iii. Dependent Claims 2-14

2[Pre]: The method of claim 1,

324. *See supra* § X.D.ii (’734 Patent Claim 1).

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

325. *See supra* § IX.D.iii (’949 Patent Claim 16).

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

326. *See supra* § IX.D.iii (’949 Patent Claim 18).

3[Pre]: The method of claim 1,

327. *See supra* § X.D.ii ('734 Patent Claim 1).

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

328. *See supra* § IX.D.iii ('949 Patent Claim 16).

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

329. *Waters* in view of *Dua* renders obvious Limitation 3[b] for the reasons discussed above. *See supra* § X.B.ii ('734 Patent Limitation 3[b]).

330. In my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 3.

Claim 4: The method of claim 1, wherein the circuit is configured to store transaction logs.

331. *See supra* § IX.D.iii ('949 Patent Claim 19).

Claim 5: The method of claim 1, wherein the electronic switch is configured for a user to select between a plurality of financial accounts for the financial transaction.

332. *See supra* § IX.D.iii ('949 Patent Claim 6).

Claim 6: The method of claim 1, wherein the electronic switch is configured to enter a personal identification number or a password.

333. *Waters* in view of *Dua* renders obvious Claim 6 for the same reasons discussed above in Grounds 1-2. *See supra* § X.B.ii ('734 Patent Claim 6); *see also supra* § IX.D.ii.1[c] ('949 Patent Claim 1).

Claim 7: The method of claim 1, wherein the circuit is configured to communicate an account number via the inductive coupling to facilitate the financial transaction.

334. *See supra* § IX.D.iii ('949 Patent Claim 9).

Claim 8: The method of claim 1, wherein the cellular telephone includes a key memory configured to store an encryption key used to facilitate the financial transaction.

335. *See supra* § IX.D.iii ('949 Patent Claim 11).

Claim 9: The method of claim 1, wherein the cellular telephone includes a key memory configured to store a key required to change the state of the circuit to facilitate the financial transaction via the inductive coupling.

336. *See supra* § IX.D.iii ('949 Patent Claim 12).

Claim 10: The method of claim 1, wherein the cellular telephone includes an antenna configured to communicate using WiFi, the antenna being configured to operate at a different radio frequency than the inductive coupling.

337. *Waters* in view of *Dua* renders obvious every element of Claim 1. *See supra* § X.D.ii ('734 Patent Claim 1). *Waters* discloses that its device can communicate “with a network...via a UMA ‘access point.’” EX1024, [0024]. In my opinion, a POSITA would have understood that Unlicensed Mobile Access (“UMA”) is a telecommunications standard that enables mobile phones to route data over unlicensed IP-based networks, including WiFi networks. In my opinion, a POSITA would have understood that to the extent *Waters* does not expressly describe a separate WiFi antenna, providing one would have been necessary, or at least obvious, in order to implement the UMA connectivity *Waters* describes.

Further, in my opinion, a POSITA would have understood that such a WiFi antenna would be tuned to 2.4 GHz or 5 GHz, both of which are different frequencies than the 13.56 MHz frequency used for *Waters*'s RFID communication described above. EX1024, [0034].

338. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 10.

11[Pre]: The method of claim 1,

339. *See supra* § X.D.ii ('734 Patent Claim 1).

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

340. *Waters* explains that its device includes a “subscriber identity module (SIM) 15.” EX1024, [0023]. In my opinion, a POSITA would have understood that a SIM card is a component that is inserted into a device, such as a cellular telephone.

341. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Limitation 11[a].

11[b]: the electronic key including a financial account identifier and a signal communicated via the inductive coupling to facilitate the financial transaction being responsive to the financial account identifier.

342. *Waters* explains that the SIM can store “authentication information,” which can be used to authenticate whether “a particular user...has a particular pre-paid account with a network.” EX1024, [0023], [0026] (“Nevertheless, such a user cannot make use of the network until the network has authenticated the user's SIM—

that is, has confirmed that such user is a particular user who has a particular pre-paid account with a network.”); *see also supra* § IX.D.iii (’949 Patent Claim 8). Therefore, in my opinion, a POSITA would have understood that the authentication information is a financial account identifier, because it can be used to identify a user’s account. *Waters* further discloses that the RFID functionality (which, as discussed above, is carried out via an inductive coupling) can be enabled or disabled, depending on whether the SIM is successfully authenticated using the authentication information (account identifier). EX1024, [0036] (“In order to improve the security of the near field tag, in the present embodiment it is proposed to use the SIM **15** of mobile terminal **1** to control to some extent the operation of the near field tag **41**. The authentication process of a SIM **15** with a mobile telecommunications network, using the network’s authentication processor **17** is considered to be highly secure. In this embodiment, this authentication of the SIM **15** is used to protect data held by the memory of the near field tag **41** from unauthorised access.”), [0046]-[0047] (“Typically, when the mobile terminal **1** is powered up within the coverage area of the mobile telecommunications network **3**, the authentication process between the SIM **15** and the authentication processor **17** of the network **3** occurs automatically. When this authentication has been completed, a message is sent to the near field tag **41**, via the link **43**, to enable operation of the tag. When the SIM **15** is no longer authenticated (for example, when the mobile terminal **1** is powered down), a further

message is sent from the SIM **15** to the near field tag **41**, via the link **43**, to deactivate the near field tag **41**.”); *See supra* § IX.D.ii.1[b] (’949 Patent Claim 1).

343. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Limitation 11[b].

344. In my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 11.

12[Pre]: The method of claim 1,

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

12[b]: the electronic key including an account identifier and the communication via the inductive coupling being responsive to the account identifier,

12[c]: the electronic key being configured to store a password or personal identification number.

345. *Dua* discloses Limitations 12[Pre]-[c] for the reasons discussed above in § X.D.ii (Limitations 11[Pre]-[b]).

Claim 13: The method of claim 1, wherein the circuit includes both the electronic switch and a mechanical switch configured to approve the financial transaction.

346. *See supra* § IX.D.iii (’949 Patent Claim 26).

Claim 14: The method of claim 1, wherein activating the electronic switch is responsive to data stored in memory of the cellular telephone and the data stored in memory includes biometric data.

347. *Waters* in view of *Dua* renders obvious every element of Claim 1. *See*

supra § X.D.ii ('734 Patent Claim 1). *Waters* in view of *Dua* also renders obvious that the electronic switch is responsive to a biometric sensor. *See supra* §§ IX.D.ii.1[c]-[e] ('949 Patent Claim 1). *Waters* further states that “[t]he pressure sensor may be combined with the fingerprint scanner **45**. The combined sensor detects, not only that pressure is applied, but also that an authorised person is pressing the sensor.” EX1024, [0053]. *Waters* also explains that the fingerprint reader “scans the fingerprint of the user when the user’s finger is placed on the reader **45** and compares it to the user’s fingerprint stored in the memory of the mobile terminal **1** or the SIM **15**.” *Id.*, [0051]; *see also id.*, [0068], FIG. 5 (“[t]he print is ideally compared to a previously taken print stored in the memory **130** of the smart card **100**”). Thus, *Waters* in view of *Dua* renders obvious Claim 14.

iv. Independent Claim 15

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

348. *See supra* § X.D.ii.1[Pre] ('734 Patent Claim 1).

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

349. *See supra* § X.D.ii.1[a] ('734 Patent Claim 1).

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

350. *See supra* § IX.D.ii.1[a] ('949 Patent Claim 1).

15[c]: 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;

351. *See supra* § IX.D.ii.1[b] ('949 Patent Claim 1).

15[d]: activating the electronic switch within the cellular telephone to change the state of the circuit; and

352. *See supra* § X.D.ii.1[e] ('734 Patent Claim 1).

15[e]: 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 financial account information using the inductive coupling,

353. *See supra* § X.D.ii.1[f] ('734 Patent Claim 1).

15[f]: wherein the cellular telephone is configured for a user to enter a personal identification number (PIN), communication of the financial account information via the inductive coupling being responsive to the personal identification number.

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

355. In my opinion, a POSITA would have understood that this PIN-based

authentication mechanism necessarily discloses the same an electronic switch identified in §§ IX.D.ii.1[c] ('949 Patent Claim 1), which, in response to a correct PIN entry, makes or breaks an electrical connection in the processing and control circuitry that executes the wallet application and controls the embedded RF interface (*i.e.*, the circuit). In my opinion, a POSITA would have further understood that the making or breaking of that electrical connection changes the state of the circuit from the PIN-less state, in which only PIN-less credentials can be transmitted, to the authenticated state, in which PIN protected credentials can be transmitted. §§ IX.D.ii.1[c]-[e] ('949 Patent Claim 1). Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Limitation 15[f].

v. Dependent Claims 16-22

16[Pre]: The method of claim 15,

356. *See supra* § X.D.iv.

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

357. *See supra* § IX.D.iii ('949 Patent Claim 16).

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

358. *See supra* § X.D.iii ('734 Patent Claim 18).

17[Pre]: The method of claim 15,

359. *See supra* § X.D.iv.

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

360. *See supra* § IX.D.iii ('949 Patent Claim 16).

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

361. *See supra* § X.D.iii (Limitation 3[b]).

Claim 18: The method of claim 15, wherein the electronic switch is configured for a user to select between a plurality of financial accounts for the financial transaction.

362. *See supra* § IX.D.iii ('949 Patent Claim 6).

Claim 19: The method of claim 15, wherein the circuit is configured to communicate an account number via the inductive coupling to facilitate the financial transaction.

363. *See supra* § IX.D.iii ('949 Patent Claim 9).

Claim 20: The method of claim 15, wherein the cellular telephone includes a key memory configured to store a key required to change the state of the circuit to facilitate the financial transaction via the inductive coupling.

364. *See supra* § IX.D.iii ('949 Patent Claim 12).

Claim 21: The method of claim 15, wherein activating the electronic switch is responsive to data stored in memory of the cellular telephone and the data stored in memory includes biometric data.

365. *Waters* in view of *Dua* discloses every limitation of Claim 15. *See supra* § X.D.iv ('734 Patent Claim 15). As discussed above in §§ X.D.ii.1[c]-[e] ('734 Patent Claim 1), *Waters* in view of *Dua* renders obvious the use of a biometric

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

366. In my opinion, a POSITA would have understood that along with strict biometric authentication, both references also teach dual-authentication schemes. *Waters* explains that its activation arrangements can be used in any combination and “may work in series,” such that the tag is enabled only after more than one arrangement has been satisfied. EX1024, [0056]. *Dua* likewise describes a dual-authentication scheme using biometric entry and an issuer PIN, which in my opinion it would have been obvious to a POSITA to implement fully on its mobile device running its wallet application. *See supra* § X.B.iv (’734 Patent Claim 21).

367. *Waters* describes dual-authentication using both a biometric sensor and PIN-entry in series, which is consistent with *Dua*’s biometric/issuer PIN scheme. EX1024, [0056]. It would also have been obvious to a POSITA to implement the same dual-authentication scheme discussed in § X.B.iv (’734 Patent Claim 21) in

the device of *Waters* incorporating the wallet application of *Dua*. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 21.

22[Pre]: The method of claim 15,

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

22[b]: the electronic key including an account identifier,

22[c]: the electronic key being configured to store the personal identification number.

368. *See supra* § X.D.iii (Claims 11-12).

vi. Independent Claim 23

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

369. *See supra* § X.D.ii.1[Pre] ('734 Patent Claim 1).

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

370. *See supra* § X.D.ii.1[a] ('734 Patent Claim 1).

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

371. *See supra* § IX.D.ii.1[a] ('949 Patent Claim 1).

23[c]: 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;

372. *See supra* § IX.D.ii.1[b] ('949 Patent Claim 1).

23[d]: activating the electronic switch within the cellular telephone to change the state of the circuit; and

373. *See supra* § X.D.ii.1[e] ('734 Patent Claim 1).

23[e]: 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 financial account information using the inductive coupling,

374. *See supra* § X.D.ii.1[f] ('734 Patent Claim 1).

23[f]: wherein the cellular telephone includes a user interface configured to enter a financial account number and includes memory configured to store the financial account number for use in the financial transaction.

375. *Waters* discloses that its device includes a “keypad” (a type of user interface). EX1024, [0034], [0051]. As discussed above with respect to Grounds 1–2, *Dua* discloses that its wallet application is configured to receive a financial account number inputted by a user via a keypad. *See supra* § X.B.ii ('734 Patent Claim 4). In my opinion, a POSITA would have understood that when implemented in *Waters*’s device, the wallet application would receive a financial account number inputted by a user via *Waters*’s keypad (user interface).

376. As further discussed above, *Dua*’s wallet application controls the device to store a financial account number in memory. *See supra* § X.B.ii ('734 Patent Claim 4). Therefore, in my opinion, when implemented in *Waters*’s device, a POSITA would have understood that the financial account number would be stored in memory.

377. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* discloses Limitation 23[f].

378. In my opinion, a POSITA would have understood that *Waters* in view of *Dua* anticipates or renders obvious independent Claim 23.

vii. Dependent Claims 24-30

24[Pre]: The method of claim 23,

379. *See supra* § X.D.vi.

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

380. *See supra* § IX.D.iii ('949 Patent Claim 16).

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

381. *See supra* § X.D.iii ('734 Patent Claim 18).

25[Pre]: The method of claim 23,

382. *See supra* § X.D.vi.

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

383. *See supra* § IX.D.iii ('949 Patent Claim 16).

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

384. *See supra* § X.D.iii (Limitation 3[b]).

Claim 26: The method of claim 23, wherein the electronic switch is configured for a user to select between a plurality of financial accounts for the financial transaction.

385. *See supra* § IX.D.iii ('949 Patent Claim 6).

Claim 27: The method of claim 23, wherein the circuit is configured to communicate an account number via the inductive coupling to facilitate the financial transaction.

386. *See supra* § IX.D.iii ('949 Patent Claim 9).

Claim 28: The method of claim 23, wherein the cellular telephone includes a key memory configured to store a key required to change the state of the circuit to facilitate the financial transaction via the inductive coupling.

387. *See supra* § IX.D.iii ('949 Patent Claim 12).

29[Pre]: The method of claim 23,

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

29[b]: the electronic key including an account identifier and the communication via the inductive coupling being responsive to the account identifier,

29[c]: the electronic key being configured to store a password or personal identification number.

388. *See supra* § X.D.iii (Claims 11-12).

Claim 30: The method of claim 23, wherein communicating the financial account information is responsive to biometric data stored in memory of the cellular telephone.

389. *See supra* § X.D.iii ('734 Patent Claim 14).

XI. THE '741 PATENT

A. SUMMARY OF PRIOR ART GROUNDS

Ground	Claims	Basis	Prior Art
1	1–13, 15–28, 30	Anticipation	<i>Dua</i>
2	1–13, 15–28, 30	Obviousness	<i>Dua</i>
3	9, 14, 29, 30	Obviousness	<i>Dua</i> with <i>Woike</i>
4	1–30	Obviousness	<i>Dua</i> with <i>Waters</i>

B. GROUNDS 1-2: *Dua*

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

i. Independent Claim 1

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

391. *See supra* § X.B.i.1[Pre]-[a] ('734 Patent Claim 1).

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

392. *See supra* § X.B.i.1[a] ('734 Patent Claim 1).

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

393. *See supra* § IX.B.i.1[b] ('949 Patent Claim 1).

394. To the extent that “RF antenna” means an antenna for RF communications different from the RFID antenna, in my opinion, a POSITA would have understood that *Dua* also anticipates or renders obvious this limitation. For

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

395. Therefore, in my opinion, a POSITA would have understood that *Dua* anticipates, or at least renders obvious, Limitation 1[b].

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

396. *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]. In my opinion, a POSITA would have understood that the wireless device running the wallet application that enables communication with the embedded RF interface necessarily includes processing and control circuitry (*i.e.*, a circuit) that executes the wallet application and controls the embedded RF interface or smart card.

397. *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”).

398. In my opinion, a POSITA would have understood that the PIN and biometric authentication mechanisms necessarily include an electronic switch that, in response to PIN or biometric entry, makes or breaks an electrical connection in the processing or control circuitry that executes the wallet application and controls the embedded RF interface (*i.e.*, the circuit). In my opinion, a POSITA would have further understood that the electronic switch, in response to PIN or biometric entry, makes or breaks an electrical connection in the circuit, causing an electronic signal to change the operative state of the circuit (*e.g.*, from disabled to enabled; from PIN-less to authenticated). EX1023, [0367] (describing PIN-less state—“A user can at their own discretion, choose to designate certain credentials within the wallet application to be used without requiring entry of the wallet application PIN.

Registered credentials that can be designated by the user as not requiring entry of a wallet PIN are those that have a ‘reader key’ associated with them. Credentials with a ‘reader key’ associated with them will be flagged as such in the wallet application to help a user identify them.”), [0395] (describing disabled/enabled states—“Pressing buttons **1** or **2**, may prompt the user to input a PIN before RF communication can be enabled. As such, a user may be required to input a PIN and click ‘OK’ to enable RF communication for a 30 second window. Alternatively, the user may be required to input his PIN, click ‘OK’ to initiate PIN verification, and upon positive confirmation be prompted to hold down either button **1** or **2** while placing the device in close proximity to a reader.”), [0397] (describing authenticated state—“Certain credential issuers such as financial institutions may require that users validate their identity during a transaction by providing a PIN that was established with or set by the financial institution.”), [0414] (“While the above description calls for the use of over-the-air PIN verification, it should be noted that biometrics could also be used in lieu of PINs, while still falling within the scope of the present invention. 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.”). Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Limitation 1[c].

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

399. *See supra* § IX.B.i.1[b] ('949 Patent Claim 1).

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

400. *Dua* discloses Limitation 1[e] for the reasons discussed above in § XI.A.i.1[c]. Specifically, in my opinion, a POSITA would have understood 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). A POSITA would have further understood that the electronic switch, in response to PIN or biometric entry, makes or breaks an electrical connection in the circuit, causing an electronic signal to change the operative state of the circuit (*e.g.*, from disabled to enabled; from PIN-less to authenticated). Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Limitation 1[e].

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

401. *Dua* discloses communication by the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate a financial transaction using inductive coupling or an RF antenna. *See supra* §§ XI.B.i.1[Pre],

1[b]-1[d] ('741 Patent Claim 1).

402. *Dua* explains that the wallet application “is specifically designed to store several types of electronic credentials,” including “Payment Methods” such as “[c]redit, debit/ATM, stored value, electronic check, and RFID payment methods.” EX1023, [0334], [0336]. The “credential record” contains “Account number” among other account-specific information. *Id.*, [0297], [0302]-[0304]. *Dua* further states that “[e]lectronic credentials issued to a user and stored in the wallet application can be used” in a proximity transaction, where “the wireless device can transmit payment, identification, or other confidential information to a reader using the short-range transmission capability of the wireless device (e.g. RF).” *Id.*, [0313]-[0315]. *Dua* also describes “peer-to-peer” transactions with connectivity “made via 802.11 a/b/g, Bluetooth, or other RF protocols” and that “remote transaction[s] using a wireless device can be conducted over the Internet with a browser on the wireless device.” *Id.*, [0318], [0323]; *see also id.*, [0423] (describing web-based transactions). In these cases, communication of financial account information is responsive to the state of the circuit as explained above. §§ XI.B.i.1[c], 1[e] ('741 Patent Claim 1). Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Limitation 1[f].

403. Therefore, in my opinion, a POSITA would have understood that *Dua* anticipates or renders obvious independent Claim 1.

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

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

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

404. *Dua* discloses every element of Claim 1. *See supra* § XI.B.i ('741 Patent Claim 1). *Dua*'s wallet is "the core" of the platform and "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," including performance of financial transactions. EX1023 [0309], [0315] ("During 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). 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."). 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].

405. As identified in § IX.B.i.1[b] ('949 Patent Claim 1), *Dua*'s "circuit" is the processing and control circuitry that executes the wallet application and controls the embedded RF interface or smart card. In my opinion, a POSITA would have understood that the circuitry is configured to facilitate the financial transaction and to communicate financial account information based on the functionality of the wallet application it executes. Thus, by making the wallet application functionality and transmission of financial credentials responsive to a fingerprint sensor, in my opinion, a POSITA would have understood that *Dua* discloses Claims 2 and 4.

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

406. *Dua* discloses every element of Claim 1. *See supra* § XI.B.i ('741 Patent Claim 1). As noted above, *Dua* discloses that a biometric sensor can be used to enable financial transactions. *See supra* §§ XI.B.i.1[e] ('741 Patent Claim 1), XI.B.ii ('741 Patent Claim 2). *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.”).

407. As identified in § IX.B.i ('949 Patent Claim 1), *Dua*'s “circuit” is the processing and control circuitry that executes the wallet application and controls the embedded RF interface or smart card. In my opinion, a POSITA would have understood that the circuitry is configured to approve the financial transaction based on the functionality of the wallet application it executes. Thus, by making the wallet application's user authentication and financial transaction approval responsive to a fingerprint sensor, in my opinion, a POSITA would have understood that *Dua* discloses Claim 3.

5[Pre]: The method of claim 1,

408. *See supra* § XI.B.i ('741 Patent Claim 1).

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

409. *See supra* § IX.B.ii ('949 Patent Claim 16).

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

410. *See supra* § IX.B.ii ('949 Patent Claim 18).

6[Pre]: The method of claim 1,

411. *See supra* § XI.B.i ('741 Patent Claim 1).

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

412. *See supra* § IX.B.ii ('949 Patent Claim 16).

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

413. *See supra* § X.B.ii ('734 Patent Limitation 3[b]).

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

414. *See supra* § IX.B.ii ('949 Patent Claim 19).

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

415. *Dua* discloses every element of Claim 1. *See supra* § XI.B.i ('741 Patent Claim 1). *Dua*'s wallet application can store multiple payment credentials, including "[c]redit, debit/ATM, stored value, electronic check, and RFID payment methods." EX1023, [0336]. *Dua* further explains that "[o]nce the user completes making his selection(s) in the 'Credential Selector', the wallet application is ready to transmit the credential(s) via its RFID interface." *Id.*, [0378]. As identified in § IX.B.i.1[b] ('949 Patent Claim 1), *Dua*'s circuit is the processing and control circuitry that executes the wallet application and controls the embedded RF interface or smart card. In my opinion, a POSITA would have understood that the circuit is configured for a user to select between a plurality of financial accounts for the financial transaction based on the functionality of the wallet application it executes. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 8.

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

416. *Dua* discloses every element of Claim 1. *See supra* § XI.B.i ('741 Patent Claim 1). *Dua* states that “[o]ne advantage of establishing peer-to-peer connectivity with a POS terminal is that it allows for a bi-directional exchange of data where a user may be prompted on his wireless device for various types of preferences, questions, or other data input in sequence.” EX1023, [0319]. In my opinion, a POSITA would have understood that these broad categories of data that the user may be prompted to enter during a financial transaction clearly can include the amount of the financial transaction. Alternatively, in my opinion, it would be obvious to a POSITA that one of the data a user could enter on a wireless phone keypad is a transaction amount. For example, *Dua* explains that an “an over-the-air reload tool” associated with a stored value credential can be programmed into the wallet application. EX1023, [0293]. In my opinion, it would have been obvious to a POSITA that to reload a stored value account, a user would be prompted to enter the amount of the reload (*i.e.*, the transaction). In my opinion, a POSITA would have understood that *Dua* anticipates, or at least renders obvious, Claim 9.

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

417. *See supra* § IX.B.ii ('949 Patent Claim 9).

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

418. *See supra* § IX.B.ii ('949 Patent Claim 4).

12[Pre]: The method of claim 1,

419. *See supra* § XI.B.i ('741 Patent Claim 1).

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

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

420. As discussed above in § XI.B.i ('741 Patent Claim 1), *Dua* discloses the use of a biometric authentication mechanism to facilitate a financial transaction. *Dua* also describes that, separate from wallet application authentication, “[c]ertain credential issuers such as financial institutions may require that users validate their identity during a transaction by providing a PIN that was established with or set by the financial institution.” EX1023, [0397]. *Dua* further describes: “credential issuers may issue a credential to a wireless device, require the wallet PIN with every transaction, but also prompt the user for an issuer PIN (or PIN set with the issuer) on the POS terminal during each transaction. The POS terminal may know to prompt

for a PIN based on a card BIN number for example.” *Id.*, [0402]. Since *Dua*’s mobile device is configured for PIN-entry (*see* EX1023, [0366]), in my opinion, it would have been obvious to a POSITA that this dual-authentication scheme (*i.e.*, biometric entry to open the wallet application followed by issuer PIN entry to facilitate the transaction) could be executed by utilizing the fingerprint sensor and the PIN-entry functionalities of the mobile device itself.

421. Therefore, in my opinion *Dua* anticipates or renders obvious Claim 12.

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

422. *See supra* § IX.B.ii (’949 Patent Claim 12).

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

423. *Dua* discloses every element of Claim 1. *See supra* § XI.B.i (’741 Patent Claim 1). *Dua* discloses that the circuit is configured to communicate financial account information including the account number via the inductive coupling or RF antenna to facilitate the financial transaction. *See supra* §§ XI.B.i.1[f] (’741 Patent Claim 1); XI.B.ii (’741 Patent Claim 11). Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 15.

Claim 16: The method of claim 1, wherein activating the electronic switch is responsive to data stored in memory of

the cellular telephone and the data stored in the memory includes biometric data.

424. *See supra* § X.B.ii ('734 Patent Claim 14).

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

425. *See supra* § IX.B.ii ('949 Patent Claim 9).

18[Pre]: The method of claim 1,

426. *See supra* § XI.B.i ('741 Patent Claim 1).

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

427. *See supra* § IX.B.ii ('949 Patent Claim 4).

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

428. *See supra* § XI.B.ii ('741 Patent Claim 8).

18[c]: presenting a user interface to the user, the user interface being configured to allow the user to select a specific member of the plurality of financial accounts of the user for the financial transaction;

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

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

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

431. Therefore, in my opinion, a POSITA would have understood that *Dua* anticipates or renders obvious Claim 18.

iii.Independent Claim 19

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

432. *See supra* § X.B.i.1[Pre]-[a] (’734 Patent Claim 1).

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

433. *See supra* § X.B.i.1[a] (’734 Patent Claim 1).

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

434. *See supra* § XI.B.i.1[b] (’741 Patent Claim 1).

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

435. *See supra* § XI.B.i.1[c] (’741 Patent Claim 1).

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

436. *See supra* § IX.B.i.1[b] ('949 Patent Claim 1).

437. Limitations 19[c]-[d] are substantively identical to Limitations 1[c]-[d] except that Limitations 19[c]-[d] require that “the RF antenna” (rather than “communication by the cellular telephone” as recited in Limitations 1[c]-[d]) is “responsive to the state of the circuit.” As discussed above in § XI.B.i.1[b] ('741 Patent Claim 1), “communication by the cellular telephone” in *Dua* occurs using an RF antenna. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses limitations 19[c]-[d] for the reasons discussed above in § XI.B.i.1[c]-1[d] ('741 Patent Claim 1).

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

438. *Dua* describes that “[t]he default security setting in the wallet application is that PIN-entry is required before the wallet application can be ‘opened’ and any credentials transmitted to an external device.” EX1023, [0366]. *Dua* further discloses that a user “may be required to input a PIN and click ‘OK’ to enable RF communication for a 30 second window” or to “input his PIN, click ‘OK’ to initiate PIN verification, and upon positive confirmation be prompted to hold down either button 1 or 2 while placing the device in close proximity to a reader.” *Id.*, [0395].

439. In my opinion, a POSITA would have understood that this PIN-based authentication mechanism necessarily discloses the same electronic switch identified in § XI.B.i.1[c] ('741 Patent Claim 1), which, in response to correct PIN entry, makes or breaks an electrical connection in the processing and control circuitry that executes the wallet application and controls the embedded RF interface (*i.e.*, the circuit). In my opinion, a POSITA would have further understood that the electronic switch, in response to PIN or biometric entry, makes or breaks an electrical connection in the circuit, causing an electronic signal to change the operative state of the circuit (*e.g.*, from disabled to enabled, from PIN-less to authenticated). *See also* § XI.B.i.1[c] ('741 Patent Claim 1). Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Limitation 19[e].

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

440. *See supra* § XI.B.i.1[f] ('741 Patent Claim 1).

441. Therefore, in my opinion, a POSITA would have understood that *Dua* anticipates or renders obvious independent Claim 19.

iv. Dependent Claims 20-28, 30

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

442. *Dua* discloses every element of Claim 19. *See supra* § XI.B.iii ('741 Patent Claim 19). As discussed above in § XI.B.ii ('741 Patent Limitation 12[b]), *Dua* renders obvious a dual-authentication scheme using both PIN-entry (*e.g.*, as recited in Claim 19) and a biometric sensor (*e.g.*, as recited in Claim 20). In my opinion, a POSITA would have understood that *Dua*'s wallet button corresponds to a mechanical switch. Additionally, *Dua* explains that after the user presses the wallet button, the wallet application "prompts the user for his Wallet PIN. . . . if the user wants to open the wallet application to select credentials or make changes to settings, the user can simply enter his wallet PIN when prompted." EX1023, [0384]. As discussed throughout *Dua*, the petitions, and this declaration, "wireless devices with embedded biometric technologies could use a fingerprint in lieu of a PIN code to authenticate a user to the wallet application." *Id.*, [0366]. In my opinion, a POSITA would have understood that by describing a wallet button (*i.e.*, a mechanical switch) that opens the wallet application, the wallet application prompting the user for authentication (*e.g.*, utilizing the biometric sensor), and subsequent entry of an issuer PIN (*See supra* § XI.B.ii ('741 Patent Limitation 12[b])), *Dua* discloses Claim 20.

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

443. *See supra* § XI.B.ii ('741 Patent Claim 3).

Claim 22: The method of claim 19, wherein the cellular telephone includes a user interface configured for a user to

enter a financial account number for use in the financial transaction.

444. *See supra* § IX.B.ii ('949 Patent Claim 4).

23[Pre]: The method of claim 22,

445. *See supra* § XI.B.iv ('741 Patent Claim 22).

23[a]: wherein the cellular telephone includes memory configured to store the financial account number, wherein the circuit is configured for the user to select between a plurality of financial accounts for the financial transaction;

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

446. *Dua* discloses Limitations 23[a]-[b] for the reasons discussed above in § XI.B.ii ('741 Patent Claims 8 and 11).

447. Therefore, in my opinion, a POSITA would have understood that *Dua* anticipates or renders obvious Claim 23.

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

448. *See supra* § XI.B.ii ('741 Patent Claim 8).

25[Pre]: The method of claim 19,

449. *See supra* § XI.B.iii ('741 Patent Claim 19).

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

450. *See supra* § IX.B.ii ('949 Patent Claim 16).

451. To the extent that "RF antenna" here refers to an antenna for RF

communications via a cellular network, in my opinion, a POSITA would have understood that *Dua* discloses this limitation. In this context of RF communications via a cellular network, in my opinion, a POSITA would have understood that the circuit is in a first ON state when the mobile telephone is powered on (*i.e.*, the mobile telephone has service and can communicate with the cellular network). In my opinion, a POSITA would have further understood that circuit is in a second ON state when the RF interface is enabled to communicate with a reader. In my opinion, a POSITA would have understood that thus, *Dua* discloses Limitation 25[a].

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

452. *See supra* § X.B.ii ('734 Patent Limitation 3[b]).

453. To the extent that “RF antenna” refers to an antenna for RF communications via a cellular network, in my opinion, a POSITA would have understood that *Dua* discloses this limitation. In my opinion, a POSITA would have understood that in the first ON state (*i.e.*, mobile telephone is powered on), the circuit of the mobile terminal can communicate personal information using the cellular network. In my opinion, a POSITA would have further understood that in the second ON state (*i.e.*, RF interface is enabled), the circuit can communicate different amounts of personal information (*i.e.*, authentication-protected sensitive payment and personal information). In my opinion, a POSITA would have understood that

thus, *Dua* renders obvious Limitation 25[b].

454. Therefore, *Dua* anticipates or renders obvious Claim 25.

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

455. *See supra* § IX.B.ii ('949 Patent Claim 19).

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

456. *See supra* § IX.B.ii ('949 Patent Claim 9).

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

457. *Dua* discloses every element of Claim 19. *See supra* § XI.B.iii ('741 Patent Claim 19). *Dua* discloses PIN-based authentication with the password stored in memory. *See supra* § XI.B.ii ('741 Patent Claim 12). *Dua* describes that “[t]he default security setting in the wallet application is that PIN-entry is required before the wallet application can be ‘opened’ and any credentials transmitted to an external device.” EX1023, [0366]. *Dua* further describes that “PINs can be any length, and be comprised of any combination of upper or lower case letters, numbers, and special characters as provided for by the wireless device itself.” *Id.* In my opinion, a POSITA would have understood such a PIN used to open and enable the wallet application can correspond to a password. In my opinion, a POSITA would have further understood that, to enable implementation of the software-based logic

described above (authentication using PIN-based verification), it would have been necessary, or at least obvious, to store the entered PIN (*i.e.*, a password) in memory, such that the device can verify whether it matches the correct PIN. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 28.

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

458. *See supra* § XI.B.ii ('741 Patent Claim 9).

C. GROUND 3: *Dua* in View of *Woike* Renders Obvious Claims 9, 14, 29, AND 30

i. Motivation to Combine

459. *See supra* § IX.C.i.

ii. Claim Analysis

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

460. *Dua* discloses every element of Claim 1. *See supra* § XI.B.i ('741 Patent Claim 1). *Dua* anticipates, or at least renders obvious, that the user can enter transaction amounts. *See supra* § XI.B.ii ('741 Patent Claim 9). Additionally, *Woike* explains that a payment can be made by “quickly entering the identification number for the receiver of the payment, ***and the payment amount***, in the cell phone, and sending this data to the authorization computer.” EX1025, p. 2, ll. 17-19. In my opinion, a POSITA would have understood that thus, *Dua* in view of *Woike* renders

obvious Claim 9.

14[Pre]: The method of claim 1,

461. *See supra* § XI.B.i ('741 Patent Claim 1).

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

462. *See supra* § X.C.ii (Limitation 11[a]).

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

463. *See supra* § X.C.ii (Limitation 11[b]).

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

464. *See supra* § X.C.ii (Limitation 11[b]).

465. Therefore, in my opinion, *Dua* in view of *Woike* renders obvious Claim 14.

29[Pre]: The method of claim 19,

466. *See supra* § XI.B.iii ('741 Patent Claim 19).

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

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

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

467. *See supra* § X.C.ii (Limitations 11[a]-[b]).

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

468. *Dua* discloses every element of Claim 19. *See supra* § XI.B.iii (’741 Patent Claim 19). “[T]he cellular telephone is configured for a user to enter an amount of the financial transaction” is also rendered obvious, by *Dua* in view of *Woike*. *See supra* § IX.C.ii (’949 Patent Claim 9). Thus, in my opinion, a POSITA would have understood that *Dua* in view of *Woike* renders obvious Claim 30.

D. GROUND 4: *Waters* in View of *Dua* Renders Obvious Claims 1-30

i. Motivation to Combine

469. *See supra* § IX.D.i.

ii. Independent Claim 1

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

470. *See supra* § X.D.ii.1[Pre]-[a] (’734 Patent Claim 1).⁴

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

471. *See supra* § X.D.ii.1[a] (’734 Patent Claim 1).

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

472. *See supra* § IX.D.ii.1[b] (’949 Patent Claim 1).

⁴ *Dua* also anticipates and/or renders obvious each limitation of Claims 1–30 for the reasons discussed above in Grounds 1–2. *See supra* § XI.B.

473. To the extent that “RF antenna” means an antenna for RF communications separate from the RFID antenna, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* also anticipates or renders obvious this limitation. For example, *Waters* provides “an antenna **39** for communicating wirelessly with the mobile communications network **3**.” EX1024, [0034]. *Dua* describes “peer-to-peer” transactions with connectivity “made via 802.11a/b/g, Bluetooth, or other RF protocols.” EX1023, [0318]. *Dua* further explains that “wireless device 200 is preferably a device that is capable of wirelessly connecting to the Internet using network protocols such as GSM/GPRS, CDMA2000, W-CDMA, EDGE, HDR, 1xRTT, UMTS, IMT-2000, 802.11a, 802.11b, 802.11g, or BLUETOOTH or other relevant protocols developed hereinafter.” *Id.*, [0041]. A POSITA would have understood that these include RF protocols that can operate over a cellular network. *See supra* § IX.B.i.1[b] (’949 Patent Claim 1). Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Limitation 1[b].

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

474. *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 supra* § XI.B.i.1[c] (’741 Patent Claim 1). In my opinion, a POSITA would have understood 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. *See supra* § XI.B.i.1[c] (’741 Patent Claim 1)

475. *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]. In my opinion, 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 supra* §§ XI.B.i.1[c]-[d] ('741 Patent Claim 1), XI.B.ii ('741 Patent Limitation 5[a]) controlled by these PIN and/or biometric authentication mechanism.

476. In my opinion, a POSITA would have understood that these PIN and biometric authentication mechanisms necessarily include an electronic switch that, in response to PIN or biometric entry, makes or breaks an electrical connection in the processing or control circuitry that executes the wallet application of *Dua* (*i.e.*, the circuit) and controls the embedded RF interface (*i.e.*, automatic deauthorizing after use). In my opinion, a POSITA would have further understood that the electronic switch, in response to PIN or biometric entry, makes or breaks an electrical connection in the circuit, causing an electronic signal to change the operative state of the circuit (*e.g.*, from disabled to enabled; from PIN-less to authenticated). EX1023, [0367] (describing PIN-less state—"A user can at their own discretion, choose to designate certain credentials within the wallet application to be used without requiring entry of the wallet application PIN. Registered credentials that can be designated by the user as not requiring entry of a wallet PIN are those that have a 'reader key' associated with them. Credentials with a 'reader key' associated with them will be flagged as such in the wallet application to help a user identify them."), [0395] (describing disabled/enabled states—"Pressing buttons 1 or 2, may prompt the user to input a PIN before RF communication can be enabled. As

such, a user may be required to input a PIN and click ‘OK’ to enable RF communication for a 30 second window. Alternatively, the user may be required to input his PIN, click ‘OK’ to initiate PIN verification, and upon positive confirmation be prompted to hold down either button **1** or **2** while placing the device in close proximity to a reader.”), [0397] (describing authenticated state—“Certain credential issuers such as financial institutions may require that users validate their identity during a transaction by providing a PIN that was established with or set by the financial institution.”), [0414] (“While the above description calls for the use of over-the-air PIN verification, it should be noted that biometrics could also be used in lieu of PINs, while still falling within the scope of the present invention. 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.”). Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Limitation 1[c].

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

477. *See supra* § IX.D.ii.1[b] (’949 Patent Claim 1).

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

478. *Waters* in view of *Dua* renders obvious Limitation 1[e] for the same

reasons discussed above in § XI.D.ii ('741 Patent Claim 1).1[c]. Specifically, in my opinion, 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. In my opinion, a POSITA would have further understood that the making or breaking of an electrical connection in the processing and control circuitry by the electronic switch changes the state of the circuit (e.g., from disabled to enabled; from PIN-less to authenticated). Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* discloses Limitation 1[e].

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

479. *Waters* in view of *Dua* renders obvious communication by the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate a financial transaction using inductive coupling or an RF antenna. See *supra* §§ XI.D.ii ('741 Patent Claim 1).1[Pre], 1[b]-1[d].

480. In my opinion, 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. *Dua* separately discloses this limitation. *See supra* § XI.D.ii ('741 Patent Claim 1).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]. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* discloses Limitation 1[f].

481. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious independent Claim 1.

iii. Dependent Claims 2-18

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

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

482. *Waters* in view of *Dua* renders obvious every element of Claim 1. *See supra* § XI.D.ii ('741 Patent Claim 1). *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]. In my opinion, 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. *Dua* also discloses making its wallet application functionality and transmission of financial credentials responsive to a fingerprint sensor. § XI.B.ii ('741 Patent Claims 2 and 4). *Dua* explains that the wallet application “is specifically designed to store several types of electronic credentials,” including “Payment Methods” such as “[c]redit,

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

483. As identified in § XI.D.ii (’741 Patent Claim 1), the “circuit” is the processing and control circuitry that executes the wallet application of *Dua* and controls the embedded RF interface. In my opinion, a POSITA would have understood that the circuitry is configured to facilitate the financial transaction and to communicate financial account information based on the functionality of the wallet application it executes. Thus, by making the wallet application functionality and transmission of financial credentials responsive to a fingerprint sensor, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claims 2 and 4.

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

484. *Waters* in view of *Dua* renders obvious every element of Claim 1. *See supra* § XI.D.ii (’741 Patent Claim 1). As noted above, *Waters* in view of *Dua*

anticipates or renders obvious that a biometric sensor can be used to enable financial transactions. §§ XI.D.ii ('741 Patent Claim 1).1[e], XI.D.iii ('741 Patent Claim 2). *Waters* states that “the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal **1** into proximity to the reader. After successful reading of the RF tag **41**, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered.” EX1024, [0052]. *Waters* explains that in the disabled state, “a reader is not able to obtain any information from the near field tag 41” but when enabled, the tag “is then able to communicate with readers to allow use of” financial services. *Id.*, [0037], [0042]. This biometric authentication scheme is also disclosed by *Dua*, where the fingerprint sensor is used to “authenticate a user to the wallet application,” and the processing and control circuitry executing that wallet application approves the transaction. *See supra* § XI.B.ii ('741 Patent Claim 3).

485. As identified in § XI.D.ii ('741 Patent Claim 1), the “circuit” is the processing and control circuitry that executes the wallet application of *Dua* and controls the embedded RF interface. In my opinion, a POSITA would have understood that the circuitry is configured to approve the financial transaction responsive to the biometric sensor based on the functionality of the wallet application it executes. Thus, by making the wallet application’s user authentication and financial transaction approval responsive to a fingerprint sensor, in my opinion,

a POSITA would have understood that the combination of *Waters* in view of *Dua* renders obvious Claim 3.

5[Pre]: The method of claim 1,

486. *See supra* § XI.D.ii ('741 Patent Claim 1).

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

487. *See supra* § IX.D.iii ('949 Patent Claim 16).

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

488. *See supra* § IX.D.iii ('949 Patent Claim 18).

6[Pre]: The method of claim 1,

489. *See supra* § XI.D.ii ('741 Patent Claim 1).

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

490. *See supra* § IX.D.iii ('949 Patent Claim 16).

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

491. *See supra* § X.D.iii (Limitation 3[b]).

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

492. *See supra* § IX.D.iii ('949 Patent Claim 19).

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

493. The mobile terminal of *Waters* incorporating the wallet application of *Dua* renders obvious Claim 8 for the same reasons discussed above in Grounds 1-2. *See supra* § XI.B.ii ('741 Patent Claim 8). Specifically, the processing and control circuitry that executes the wallet application (*i.e.*, the circuit) provides a “Credential Selector” for the user to select from multiple payment credentials once the user is authenticated by the biometric sensor of *Waters*. EX1023, [0371], [0378]. In my opinion, a POSITA would have understood that the circuitry is configured for a user to select between a plurality of financial accounts for the financial transaction based on the functionality of the wallet application it executes. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious claim 8.

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

494. *See supra* § XI.B.ii ('741 Patent Claim 9).

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

495. *See supra* § XI.B.ii ('741 Patent Claim 10).

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

to store the financial account number for use in the financial transaction.

496. *See supra* § XI.B.ii ('741 Patent Claim 11).

12[Pre]: The method of claim 1,

497. *See supra* § XI.D.ii ('741 Patent Claim 1).

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

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

498. As discussed above in § XI.D.ii ('741 Patent Claim 1).1[e], *Waters* in view of *Dua* renders obvious the use of a biometric authentication mechanism to facilitate a financial transaction. *Waters* describes that “the keypad **37** of the mobile terminal **1** is used to enter a PIN (or other secret password) to enable the near field tag **41**. . . . If the PINs match, the SIM transmits a message, via link **43**, to the near field tag **41** to activate the near field tag.” EX1024, [0051]. *Dua* also describes that, separate from wallet application authentication, “[c]ertain credential issuers such as financial institutions may require that users validate their identity during a transaction by providing a PIN that was established with or set by the financial institution.” EX1023, [0397].

499. In my opinion, a POSITA would have understood that along with strict biometric authentication, both references also teach dual-authentication schemes.

Waters explains that its activation arrangements can be used in any combination and “may work in series,” such that the tag is enabled only after more than one arrangement has been satisfied. EX1024, [0056]. *Dua* likewise describes a dual-authentication scheme using biometric entry and an issuer PIN, which, in my opinion, it would have been obvious to a POSITA to implement fully on its mobile device running its wallet application. See XI.B.ii (’741 Patent Limitations 12[a]-[b]).

500. *Waters* describes dual-authentication using both a biometric sensor and PIN-entry in series, which is consistent with *Dua*’s biometric/issuer PIN scheme. EX1024, [0056]. In my opinion, it would also have been obvious to a POSITA to implement the same dual-authentication scheme discussed in § XI.B.ii (’741 Patent Limitations 12[a]-[b]) in the device of *Waters* incorporating the wallet application of *Dua*. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* discloses Limitations 12[a]-[b].

501. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 12.

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

502. See *supra* § IX.D.iii (’949 Patent Claim 12).

14[Pre]: The method of claim 1,

503. See *supra* § XI.D.ii (’741 Patent Claim 1).

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

504. *See supra* § X.D.iii (Limitation 11[a]).

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

505. *Waters* explains that “[t]he user’s PIN may be stored in a secure location in the mobile terminal **1** or in the SIM **15**.” EX1024, [0051]. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* discloses Limitation 14[b].

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

506. *See supra* § X.D.iii (Limitation 11[b]).

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

507. *See supra* § XI.B.ii (’741 Patent Claim 15).

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

508. *See supra* § X.D.iii (’734 Patent Claim 14).

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

509. *See supra* § IX.D.iii ('949 Patent Claim 9).

18[Pre]: The method of claim 1,

510. *See supra* § XI.D.i.

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

511. *See supra* § IX.D.iii ('949 Patent Claim 4).

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

512. *See supra* § XI.D.iii ('741 Patent Claim 8).

18[c]: presenting a user interface to the user, the user interface being configured to allow the user to select a specific member of the plurality of financial accounts of the user for the financial transaction;

513. *See supra* § XI.B.ii ('741 Patent Limitation 18[c]).

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

514. *See supra* § XI.B.ii ('741 Patent Limitation 18[d]).

515. Therefore, in my opinion *Waters* in view of *Dua* renders obvious Claim 18.

iv.Independent Claim 19

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

516. *See supra* § X.D.ii.1[Pre]-[a] ('734 Patent Claim 1).

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

517. *See supra* § X.D.ii.1[a] ('734 Patent Claim 1).

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

518. *See supra* § XI.D.ii.1[b] ('741 Patent Claim 1).

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

519. *See supra* § XI.D.ii.1[c] ('741 Patent Claim 1).

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

520. Limitations 19[c]-[d] are substantively identical to Limitations 1[c]-[d] except that Limitations 19[c]-[d] require that “the RF antenna” (rather than “communication by the cellular telephone” as recited in Limitations 1[c]-[d]) is “responsive to the state of the circuit.” As discussed above in § XI.D.ii ('741 Patent Claim 1).1[b], “communication by the cellular telephone” in the *Waters-Dua* combination occurs using an RF antenna. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* discloses limitations 19[c]-[d] for the reasons discussed above in § XI.D.ii.1[c]-[d] ('741 Patent Claim 1).

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

521. *Waters* describes that “the keypad 37 of the mobile terminal 1 is used

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

522. In my opinion, a POSITA would have understood that this PIN-based authentication mechanism necessarily discloses the same electronic switch identified in §§ XI.D.ii.1[c] (’741 Patent Claim 1), which, in response to a correct PIN entry, makes or breaks an electrical connection in the processing and control circuitry that executes the wallet application and controls the embedded RF interface (*i.e.*, the circuit). In my opinion, a POSITA would have further understood that the making or breaking of that electrical connection changes the state of the circuit from the PIN-less state, in which only PIN-less credentials can be transmitted, to the authenticated state, in which PIN protected credentials can be transmitted. § XI.D.ii.1[e] (’741 Patent Claim 1). Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Limitation 19[e].

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

523. *See supra* § XI.D.ii.1[f] ('741 Patent Claim 1).

524. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious independent Claim 19.

v. Dependent Claims 20-30

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

525. *Waters* in view of *Dua* renders obvious every element of Claim 19. *See supra* § XI.D.iv ('741 Patent Claim 19). As discussed above in § XI.D.iii ('741 Patent Limitation 12[b]), *Waters* in view of *Dua* renders obvious a dual-authentication scheme using both PIN-entry (*e.g.*, as recited in Claim 19) and a biometric sensor (*e.g.*, as recited in Claim 20). *Waters* further describes that its “pressure sensor may be combined with the fingerprint scanner **45**. The combined sensor detects, not only that pressure is applied, but also that an authorised person is pressing the sensor.” EX1024, [0053]. *Waters* further explains that its activation arrangements can be used in any combination (*e.g.*, PIN entry and biometric entry). *Id.*, [0056]. *Waters* describes that “the arrangements may work in series—for example, the near field tag **41** would be enabled if the light sensor was activated and the correct PIN was subsequently entered.” *Id.* In my opinion, a POSITA would have understood that thus, because *Waters* describes an activation scheme responsive to both a pressure sensor (*i.e.*, a mechanical switch) and a fingerprint scanner (*i.e.*, a

biometric sensor), and *Dua* describes subsequent entry of an issuer PIN (*See supra* § XI.D.iii ('741 Patent Limitation 12[b])), *Waters* in view of *Dua* renders obvious Claim 20.

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

526. *See supra* § XI.D.iii ('741 Patent Claim 3).

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

527. *See supra* § IX.D.iii ('949 Patent Claim 4).

23[Pre]: The method of claim 22,

528. *See supra* § XI.D.v ('741 Patent Claim 22).

23[a]: wherein the cellular telephone includes memory configured to store the financial account number, wherein the circuit is configured for the user to select between a plurality of financial accounts for the financial transaction;

529. *See supra* § XI.B.iv ('741 Patent Limitations 23[a]-[b]).

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

530. *See supra* § XI.D.iii ('741 Patent Claim 8).

531. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 23.

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

532. *See supra* § XI.D.iii ('741 Patent Claim 8).

25[Pre]: The method of claim 19,

533. *See supra* § XI.D.iv ('741 Patent Claim 19).

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

534. *See supra* § IX.D.iii ('949 Patent Claim 16).

535. In my opinion, a POSITA would have understood that to the extent that “RF antenna” refers to an antenna for RF communications via a cellular network, *Waters* in view of *Dua* renders obvious this limitation. In this context of RF communications via a cellular network, in my opinion, a POSITA would have understood that the circuit of the mobile terminal of *Waters* incorporating the wallet application of *Dua* (*i.e.*, the processing and control circuitry executing the wallet application and controlling the embedded RF interface) is in a first ON state when the mobile terminal is powered on (*i.e.*, the mobile terminal has service and can communicate with the cellular network). In my opinion, a POSITA would have further understood that circuit is in a second ON state when the near field tag **41** is enabled to communicate with a reader. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Limitation 25[a].

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

536. *See supra* § X.D.iii (Limitation 3[b]).

537. In my opinion, a POSITA would have understood that to the extent that “RF antenna” refers to an antenna for RF communications via a cellular network, *Waters* in view of *Dua* renders obvious this limitation. In my opinion, a POSITA would have understood that in the first ON state (*i.e.*, mobile terminal is powered on), the circuit of the mobile terminal can communicate personal information using the cellular network. In my opinion, a POSITA would have further understood that in the second ON state (*i.e.*, the near field tag **41** is enabled), the circuit of the mobile terminal can communicate different amounts of personal information (*i.e.*, authentication-protected sensitive payment and personal information). Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Limitation 25[b].

538. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 25.

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

539. *See supra* § IX.D.iii (’949 Patent Claim 19).

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

540. *See supra* § IX.D.iii ('949 Patent Claim 9).

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

541. *Waters* in view of *Dua* renders obvious every element of Claim 19. *See supra* § XI.D.iv ('741 Patent Claim 19). *Dua* also discloses Claim 28. *See supra* § XI.B.iv ('741 Patent Claim 28). *Waters* also states that “[t]he user's PIN may be stored in a secure location in the mobile terminal 1 or in the SIM 15.” EX1024, [0051]. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 28.

29[Pre]: The method of claim 19,

542. *See supra* § XI.D.iv ('741 Patent Claim 19).

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

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

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

543. *See supra* § XI.D.iii ('741 Patent Limitations 14[a]-[c]).

544. Therefore, in my opinion *Waters* in view of *Dua* renders obvious Claim 29.

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

545. *See supra* § XI.B.iv ('741 Patent Claim 30).

XII. THE '612 PATENT

A. SUMMARY OF PRIOR ART GROUNDS

Ground	Claims	Basis	Prior Art
1	1–5	Anticipation	<i>Dua</i>
2	1–5	Obviousness	<i>Dua</i>
3	1–5	Obviousness	<i>Dua with Waters</i>

B. GROUNDS 1-2: *Dua*

546. *Dua* anticipates and/or renders obvious claims 1-5.

i. Independent Claim 1

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

547. *See supra* § X.B.i.1[Pre] ('734 Patent Claim 1).

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

548. *See supra* § X.B.i.1[a] ('734 Patent Claim 1).

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

549. *See supra* § IX.B.i.1[a] ('949 Patent Claim 1).

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

550. *See supra* § IX.B.i.1[b] ('949 Patent Claim 1).

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

551. *See supra* § IX.B.i.1[b] ('949 Patent Claim 1).

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

552. *See supra* §§ X.B.i.1[e] ('734 Patent Claim 1), XI.B.i.1[e] ('741 Patent Claim 1).

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.

553. *See supra* § X.B.i.1[f] ('734 Patent Claim 1).

554. Further, in my opinion, a POSITA would have understood that RFID communication using inductive coupling necessarily requires an “inductive antenna.”

555. Therefore, in my opinion, *Dua* anticipates or renders obvious independent Claim 1.

ii. Dependent Claims 2-5

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

556. *Dua* discloses every element of Claim 1. *See supra* § XII.B.i ('612

Patent Claim 1). *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]. In my opinion, 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. Thus, in my opinion, a POSITA would have understood that *Dua* discloses 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.

557. *See supra* § XI.B.ii (’741 Patent Claims 2 and 4).

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

558. *See supra* § XI.B.ii (’741 Patent Claim 3).

C. GROUND 3: *Waters* in View of *Dua* Renders Obvious Claims 1-5

i. Motivation to Combine

559. *See supra* § IX.D.i.

ii. Independent Claim 1

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

560. *See supra* § X.D.ii.1[Pre] ('734 Patent Claim 1).⁵

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

561. *See supra* § X.D.ii.1[a] ('734 Patent Claim 1).

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

562. *See supra* § IX.D.ii.1[a] ('949 Patent Claim 1).

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

563. *See supra* § IX.D.ii.1[b] ('949 Patent Claim 1).

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

564. *See supra* § IX.D.ii.1[b] ('949 Patent Claim 1).

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

565. *See supra* §§ X.D.ii.1[e] ('734 Patent Claim 1), XI.D.ii.1[e] ('741 Patent Claim 1).

⁵ *Dua* also anticipates and/or renders obvious each limitation of Claims 1–5 for the reasons discussed above in Grounds 1–2. *See supra* §XIII.B.

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.

566. *See supra* § X.D.ii.1[f] ('734 Patent Claim 1).

567. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious independent Claim 1.

iii. Dependent Claims 2-5

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

568. *Waters* in view of *Dua* renders obvious every element of Claim 1. *See supra* § XII.C.ii ('612 Patent Claim 1). *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. Thus, in my opinion, a POSITA would have understood that *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.

569. *See supra* § XI.D.iii ('741 Patent Claims 2 and 4).

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

570. *See supra* § XI.D.iii ('741 Patent Claim 3).

XIII. THE '396 PATENT

A. SUMMARY OF PRIOR ART GROUNDS

Ground	Claims	Basis	Prior Art
1	1–10, 12–20	Anticipation	<i>Dua</i>
2	1–10, 12–20	Obviousness	<i>Dua</i>
3	11	Obviousness	<i>Dua</i> with <i>Woike</i>
4	1–4, 6–20	Obviousness	<i>Dua</i> with <i>Waters</i>

B. GROUNDS 1–2: *Dua* Anticipates and/or Renders Obvious Claims 1–10 and 12–20

i. Independent Claim 1

1[Pre]: A cellular telephone configured to use two or more different wireless communication modes, the cellular telephone comprising:

571. *Dua* explains that its device can be a “mobile telephone,” which, in my opinion, a POSITA would have understood to be a cellular telephone. EX1023, Abstract, [0026]. *Dua* further explains 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. 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.

572. Therefore, in my opinion, a POSITA would have understood that *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,

573. In my opinion, a POSITA would have understood 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.

574. Thus, as explained above with 1[pre], in my opinion, a POSITA would have understood that *Dua* discloses 1[a].

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;

575. *Dua*'s cellular mode operates at a different frequency than its RFID mode. *Dua* explains 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] ("wireless device **200** is preferably a device that is capable of wirelessly connecting to the Internet using network protocols such as GSM/GPRS, CDMA2000, W-CDMA, EDGE, HDR, 1xRTT, UMTS, IMT-2000, 802.11a, 802.11b, 802.11g, or BLUETOOTH or other relevant protocols developed hereinafter."). *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]. In my opinion, a POSITA would have understood that 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. EX1029, 108; EX1011, 3. Thus, the cellular mode (first wireless mode) and RFID mode (second wireless mode) use different radio frequency ranges. *See also supra* §§ XIII.B.i.1[pre]–[a] ('396 Patent

Claim 1).

576. Further, *Dua* explains 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] (“It is further preferred that wireless device **200** has processing and secure storage capabilities allowing it to host and operate a wallet application capable of receiving, storing, managing and transmitting multiple payment, identification, and other confidential information electronically.”), [0296]–[0306].

577. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses 1[b].

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

578. *See supra* § XI.B.ii (’741 Patent Claim 5).

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

579. *See supra* § XII.B.i.1[f] (’612 Patent Claim 1).

580. Therefore, in my opinion, a POSITA would have understood that *Dua* inherently anticipates, or otherwise renders obvious, 1[d].

581. Therefore, in my opinion, a POSITA would have understood that *Dua* anticipates, or otherwise renders obvious, independent Claim 1.

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

Claim 2[a]: The cellular telephone of claim 1, further comprising a mechanical switch configured to approve the financial transactions,

582. *See supra* § IX.B.ii ('949 Patent Claim 13).

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

583. *See supra* § XI.B.iv ('741 Patent Claim 20).

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

584. *Dua* discloses every element of Claim 1. *See supra* § XIII.B.i ('396 Patent Claim 1). *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].

585. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 3.

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

586. *Dua* discloses every element of Claim 1. *See supra* § XIII.B.i ('396 Patent Claim 1). *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].

587. Therefore, in my opinion, a POSITA would have understood that *Dua*

discloses Claim 4.

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

588. *Dua* discloses every element of Claim 1. *See supra* § XIII.B.i ('396 Patent Claim 1). *Dua* explains that “[c]onnectivity between the wireless device and the reader/POS terminal could be made via 802.11a/b/g [(WiFi)]...protocols.” *Id.*, [0318]. Such connectivity can include “facilitat[ing] transactions.” EX1023, [0333] (“The wallet application is designed to facilitate transactions in a proximity, personal, and remote environment using the device’s short-range or long-range transmission capability.”).

589. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 5.

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

590. *See supra* § XIII.B.ii ('396 Patent Claim 4).

Claim 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.

591. *See supra* § XIII.B.ii ('396 Patent Claim 3).

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

592. *See supra* § IX.B.ii ('949 Patent Claim 4).

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

593. *See supra* § XI.B.ii ('741 Patent Claim 8).

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

594. *Dua* discloses every element of Claim 1. *See supra* § XIII.B.i ('396 Patent Claim 1). *Dua* explains 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]. In my opinion, it would have been obvious to a POSITA that this mechanism 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 or company, as the device would require such information, in order to facilitate a transaction. EX1023, [0041] (“It is further preferred that wireless device **200** has processing and secure storage capabilities allowing it to host and operate a wallet application capable of receiving, storing, managing and transmitting multiple payment, identification, and other confidential information electronically.”).

595. Therefore, in my opinion, a POSITA would have understood that *Dua* renders obvious Claim 10.

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

596. *Dua* discloses every element of Claim 1. *See supra* § XIII.B.i ('396 Patent Claim 1). *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* explains 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].

597. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 12.

Claim 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.

598. *Dua* discloses every element of Claim 1. *See supra* § XIII.B.i ('396 Patent Claim 1). In my opinion, a POSITA would have understood that *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.*

599. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 13.

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

600. *Dua* discloses every element of Claim 1. *See supra* § XIII.B.i ('396 Patent Claim 1). *Dua* explains 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]. In my opinion, 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].

601. Therefore, in my opinion, a POSITA would have understood that *Dua* renders obvious Claim 14.

Claim 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 [sic] accounts.

602. *Dua* discloses every element of Claim 1. *See supra* § XIII.B.i (’396 Patent Claim 1). *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]. In my opinion, a POSITA would have understood that 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. *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].

603. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 15.

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

604. *See supra* §XIII.B.ii ('396 Patent Claim 14).

Claim 17: The cellular telephone of claim 1, wherein the circuits include an identity device, the identify [sic] device including a driver's license.

605. *Dua* discloses every element of Claim 1. *See supra* § XIII.B.i ('396 Patent Claim 1). *Dua* discloses that its device can store credentials including a "[d]river's license." EX1023, [0048], [0056], [0180], [0342]. In my opinion, a POSITA would have understood that *Dua*'s credentials can correspond to an "identity device," because they can be used to identify an individual person.

606. Therefore, in my opinion, a POSITA would have understood that *Dua* discloses Claim 17.

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

607. *See supra* §XIII.B.i.1[c] ('396 Patent Claim 1).

Claim 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,

608. *See supra* §§ IX.B.ii ('949 Patent Claim 16), XI.B.i.1[e] ('741 Patent Claim 1).

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

609. *See supra* § IX.B.ii ('949 Patent Claim 16).

610. *Dua* explains 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] (“Each individual will have their own risk tolerance and as such will want the flexibility to designate specific credentials in their wallet as requiring advance PIN-entry and others to function without the prior input of the wallet PIN.”). In my opinion, 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. *see* EX1023, [0336]–[0343], [0392].

611. Therefore, in my opinion, a POSITA would have understood that *Dua* renders obvious 19[b].

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

612. *See supra* §XIII.B.ii (’396 Patent Claim 3).

C. GROUND 3: *Dua* in View of *Woike* Renders Obvious Claim 11

iii. Motivation to Combine

613. *See supra* § IX.C.i.

iv. Claim 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 cellu phone to engage in the financial transactions.

614. *See supra* §§ IX.C.ii ('949 Patent Claims 24 and 25). Further, in my opinion, a POSITA would have understood *Woike*'s SIM card to be a "memory device" because it includes memory to store at least a PIN code.

615. Therefore, in my opinion, a POSITA would have understood that *Dua-Woike* renders obvious Claim 11.

D. GROUND 4: *Waters* in View of *Dua* Renders Obvious Claims 1–4, 6–20

v. Motivation to Combine

616. *See supra* § IX.D.i.

vi. Independent Claim 1

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

617. *Waters* explains that its device is a "[m]obile terminal...registered with [a] GSM/GPRS or UMTS (3G) mobile or cellular telecommunications network," which, in my opinion, a POSITA would have understood to be a cellular telephone. EX1024, [0020]. *Waters* further explains that its device additionally "includes a near field or RFID tag...[that] operates in the unregulated RF band of 13.56 MHz." *Id.*, [0034].

618. Therefore, in my opinion, a POSITA would have understood that

Waters in view of *Dua* discloses 1[pre].⁶

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

619. In my opinion, a POSITA would have understood 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.

620. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* discloses 1[a].

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;

621. 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* §XII.B.i.1[b] ('612 Patent Claim 1). Thus, the cellular mode (first wireless mode) and RFID mode (second wireless mode) use different radio frequency ranges.

622. Further, *Waters* discloses that the circuits are configured to perform

⁶ *Dua* also anticipates and/or renders obvious each limitation of Claims 1–10 and 12–20 for the reasons discussed above in Grounds 1–2. *See supra* §XIII.B.

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

623. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* discloses 1[b].

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

624. *See supra* § XI.D.iii (’741 Patent Claim 5).

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

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

626. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* discloses 1[d].

627. Therefore, *Waters* in view of *Dua* renders obvious independent Claim 1.

vii. Dependent Claims 2–4, 6–20

Claim 2[a]: The cellular telephone of claim 1, further comprising a mechanical switch configured to approve the financial transactions,

628. *See supra* § IX.D.iii (’949 Patent Claim 13).

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

629. *See supra* § XI.D.v ('741 Patent Claim 20).

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

630. *Waters* in view of *Dua* renders obvious every element of Claim 1. *See supra* § XIII.D.ii ('396 Patent Claim 1). *Waters* discloses that in the RFID mode (second wireless mode), payment information can be transmitted to a reader using RFID communication. *Id.*, [0041]–[0045].

631. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 3.

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

632. *See supra* § XIII.B.ii ('396 Patent Claim 4).

633. *Waters* in view of *Dua* renders obvious every element of Claim 1. *See supra* § XIII.D.ii ('396 Patent Claim 1). In my opinion, it would have been obvious to a POSITA that in the *Waters* in view of *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. *See supra* § XIII.D.ii.1[pre] ('396 Patent Claim 1) (the device of *Waters* is configured for cellular communication).

634. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 4.

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

635. *See supra* § XII.D.iii ('612 Patent Claim 4).

Claim 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.

636. *See supra* § XIII.D.iii ('396 Patent Claim 3).

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

637. *See supra* § IX.D.iii ('949 Patent Claim 4).

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

638. *See supra* § XI.D.iii ('741 Patent Claim 8).

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

639. *See supra*, §§ XII.B.ii ('612 Patent Claim 10).

640. *Waters* in view of *Dua* renders obvious every element of Claim 1. *See supra* § XIII.D.ii ('396 Patent Claim 1). In my opinion, it would have been obvious to a POSITA that the wallet application in the *Waters* in view of *Dua* combination would include the user interface disclosed by *Dua*, such that the wallet application can control the device to facilitate peer-to-peer payments.

641. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 10.

Claim 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 cellu phone to engage in the financial transactions.

642. *Waters* in view of *Dua* renders obvious every element of Claim 1. *See supra* § XIII.D.ii ('396 Patent Claim 1). In my opinion, a POSITA would have understood that *Waters* discloses that RFID communication can be enabled responsive to PIN authentication. EX1024, [0051] (“The following arrangements are useful if the near field tag **41** is to be enabled and disabled for fairly long periods of time: (1) Personal identification number (PIN) entry—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**. The user’s PIN may be stored in a secure location in the mobile terminal **1** or in the SIM **15**. When the user enters their PIN using the keypad **37**, the entered PIN is compared with the stored PIN. If the PINs match, the SIM transmits a message, via link **43**, to the near field tag **41** to activate the near field tag.”). 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* in view of *Dua* device. *See supra* §IX.C.ii ('949 Patent Claim 24).

643. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 11.

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

644. *Waters* in view of *Dua* renders obvious every element of Claim 1. *See supra* § XIII.D.ii ('396 Patent Claim 1). *Waters* explains that “[i]t is...known to encrypt the communication between the [RFID] tag and the reader.” EX1024, [0004]. In my opinion, it would have been obvious to a POSITA to implement encryption logic to enable such encryption of data prior to transmission.

645. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 12.

Claim 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.

646. *See supra* § XIII.B.ii ('396 Patent Claim 13).

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

647. *Waters* in view of *Dua* renders obvious every element of Claim 1. *See supra* § XIII.D.ii ('396 Patent Claim 1). 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]. In my opinion, similar to Grounds 1–2, it would have been obvious to a POSITA that the *Waters* in view of *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.

648. Therefore, in my opinion, a POSITA would have understood that *Waters* in view of *Dua* renders obvious Claim 14.

Claim 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 [sic] accounts.

649. *See supra* § XIII.B.ii (’396 Patent Claim 15).

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

650. *See supra* § XIII.D.iii (’396 Patent Claim 14).

Claim 17: The cellular telephone of claim 1, wherein the circuits include an identity device, the identify [sic] device including a driver’s license.

651. *See supra* § XIII.B.ii (’396 Patent Claim 17).

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

652. *See supra* §XIII.D.i.1[c].

Claim 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,

653. *See supra* §§ IX.D.iii ('949 Patent Claim 16), XI.B.i.1[e] ('741 Patent Claim 1).

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

654. *See supra* §§ IX.D.iii ('949 Patent Claim 16), XIII.B.ii (Limitation 19[b]).

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

655. *See supra* §XIII.D.iii ('396 Patent Claim 3).

XIV. CONCLUSION

All statements made herein of my own knowledge are true, and all statements made on information and belief are believed to be true. I further understand that willful false statements and the like are punishable by fine or imprisonment, or both under Section 1001 of Title 18 of the United States Code. I declare under penalty of perjury that the foregoing is true and correct.

Executed on Sept. 18-2026

A handwritten signature in cursive script, appearing to read "Sayfe Kiaei".

By: _____
Dr. Sayfe Kiaei