

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. IPR2026-00506
U.S. Patent No. 7,924,156

DECLARATION OF DR. SAYFE KIAEI

TABLE OF CONTENTS

I.	INTRODUCTION	5
II.	EXPERIENCE AND QUALIFICATIONS.....	6
III.	MATERIALS CONSIDERED	10
IV.	LEGAL STANDARDS	12
	A. Anticipation	12
	B. Obviousness.....	13
	C. Claim Construction.....	14
V.	OVERVIEW OF THE '156 PATENT	15
	A. Subject Matter of the '156 Patent.....	15
	B. Prosecution History of the '156 Patent	17
	C. RFID Communication Devices	20
VI.	LEVEL OF ORDINARY SKILL IN THE ART	23
VII.	CLAIM CONSTRUCTION	24
VIII.	SUMMARY OF PRIOR ART.....	28
	A. <i>Waters</i> (EX1024).....	28
	B. <i>Dua</i> (EX1023)	30
	C. <i>Pont</i> (EX1026)	31
	D. <i>Selker</i> (EX1027).....	34
IX.	SUMMARY OF PRIOR ART GROUNDS	36
X.	GROUND 1A: <i>WATERS</i> RENDERS OBVIOUS CLAIMS 1–33 AND 51–60	36
	A. Independent Claim 1	37
	B. Independent Claim 11	47
	C. Independent Claim 14	48
	D. Independent Claim 20	50

E.	Independent Claim 29	53
F.	Independent Claim 51	54
G.	Independent Claim 53	54
H.	Independent Claim 54	55
I.	Independent Claim 57	55
J.	Independent Claim 60	56
K.	Dependent Claims	57
XI.	GROUND 1B: <i>WATERS</i> WITH <i>PONT</i> RENDERS OBVIOUS CLAIMS 1–33 AND 51–60.....	62
A.	Motivation to Combine	63
B.	“State Memory” Claims: 1, 4, 6–7, 11, 14, 20, 23–24, 29, 51–54, 57, 60	69
C.	Claims 2–3, 5, 8–10, 12–13, 15–19, 21–22, 25–28, 30–33, 55–56, 58–59	69
XII.	GROUND 1C: <i>WATERS</i> WITH <i>SELKER</i> RENDERS OBVIOUS CLAIMS 39–43	70
A.	Motivation to Combine	70
B.	Independent Claim 39	73
C.	Dependent Claims	75
XIII.	GROUND 2A: <i>DUA</i> RENDERS OBVIOUS CLAIMS 1–10, 14–38 AND 44–59	76
A.	Independent Claim 1	76
B.	Independent Claim 14	87
C.	Independent Claim 20	88
D.	Independent Claim 29	93
E.	Independent Claim 34	94
F.	Independent Claim 44	96
G.	Independent Claim 51	98
H.	Independent Claim 53	98

I.	Independent Claim 54	99
J.	Independent Claim 57	100
K.	Dependent Claims	101
XIV.	GROUND 2B: <i>DUA</i> WITH <i>PONT</i> RENDERS OBVIOUS CLAIMS 1–10, 14–38 AND 44–59.....	107
A.	Motivation to Combine	108
B.	“State Memory” Claims: 1, 4, 6–7, 14, 20, 23–24, 29, 34, 44, 47, 51– 54, 57	110
C.	Claims 2–3, 5, 8–10, 15–19, 21–22, 25–28, 30–33, 35–38, 45–46, 48– 50, 55–56, 58–59.....	111
XV.	GROUND 2C: <i>DUA</i> WITH <i>SELKER</i> RENDERS OBVIOUS CLAIMS 39– 43	112
A.	Motivation to Combine	112
B.	Independent Claim 39	115
C.	Dependent Claims	116
XVI.	CONCLUSION.....	117

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 1–60 of U.S. Patent No. 7,924,156 (the “’156 Patent”), entitled “Electronically Switchable RFID Tags,” by named inventor Steven M. Colby. I understand that the ’156 Patent is assigned to SureCell Transactions LLC (the “Patent Owner”). I have been asked to provide technical review, analysis, insights, and opinions regarding the ’156 Patent 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 ’156 Patent (the “Petition”). This declaration is a statement of my opinions on issues related to the unpatentability of claims 1–60 of the ’156 Patent.

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. theses were 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 Instruments (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 theses, 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 '156 Patent at issue here and have been an expert in the relevant field since before the claimed priority date of the '156 Patent. I am familiar with how a person of ordinary skill in the art ("POSITA") would have understood and used the terminology found in the '156 Patent before and at the time of its 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 '156 Patent (EX1001) and its prosecution history (EX1007). I have reviewed and am familiar with the specification of the '156 Patent. I have reviewed and am familiar with the prosecution history of the '156 Patent.

19. In preparing this declaration, I have also reviewed and am familiar with the following prior art used in the Petition 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	U.S. Patent No. 7,924,156
EX1002-1006	RESERVED
EX1007	Prosecution History of U.S. Patent No. 7,924,156
EX1008-1014	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 Osaifu-Keitai - CNBC Interview</i> , https://www.eurotechnology.com/2014/09/18/applepay-vs-osaifu-keitai-cnbc/ (Sept. 18, 2014)
EX1018	IEEE Spectrum, <i>Here Comes The Wallet Phone</i> , https://spectrum.ieee.org/here-comes-the-wallet-phone (Nov. 1, 2005)
EX1019	Declaration of Sylvia D. Hall-Ellis, Ph.D. in support of authenticity and public availability of documents for <i>inter partes</i> review of U.S. Patent No. 7,924,156
EX1020	<i>SureCell Transactions LLC v. Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.</i> , No. 2:26-cv-00106, Dkt. 9 (E.D. Tex. Feb. 26, 2026) (“Amended Complaint”)
EX1021	SureCell’s Infringement Contentions, <i>SureCell Transactions LLC v. Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.</i> , No. 2:26-cv-00106 (E.D. Tex. Feb. 26, 2026)
EX1022	Claim Construction Order, <i>Mynette Techs., Inc. and Steven M. Colby v. The United States and Unisys Corp.</i> , No. 16-1647 (COFC Aug. 17, 2018)
EX1023	U.S. Patent Publication No. 2006/0165060 (“Dua”), published July 27, 2006 (filed Jan. 21, 2005)

EX1024	U.S. Patent Publication No. 2009/0215385 (“ <i>Waters</i> ”), published August 27, 2009 (PCT filed Feb. 15, 2005)
EX1025	RESERVED
EX1026	Pont, <i>Embedded C</i> (2002)
EX1027	U.S. Patent Publication No. 2003/0132301 (“ <i>Selker</i> ”), published July 17, 2003
EX1028	U.S. Army, <i>Engineering Design Handbook: Timing Systems and Components</i> (Dec. 31, 1975)
EX1029	Finkenzeller, <i>RFID Handbook</i> , 2d ed. (2003)
EX1030	Koslowski, <i>Global Migration Perspectives</i> (Oct. 2004)
EX1031-1033	RESERVED
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 also 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

27. 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 ’156 PATENT

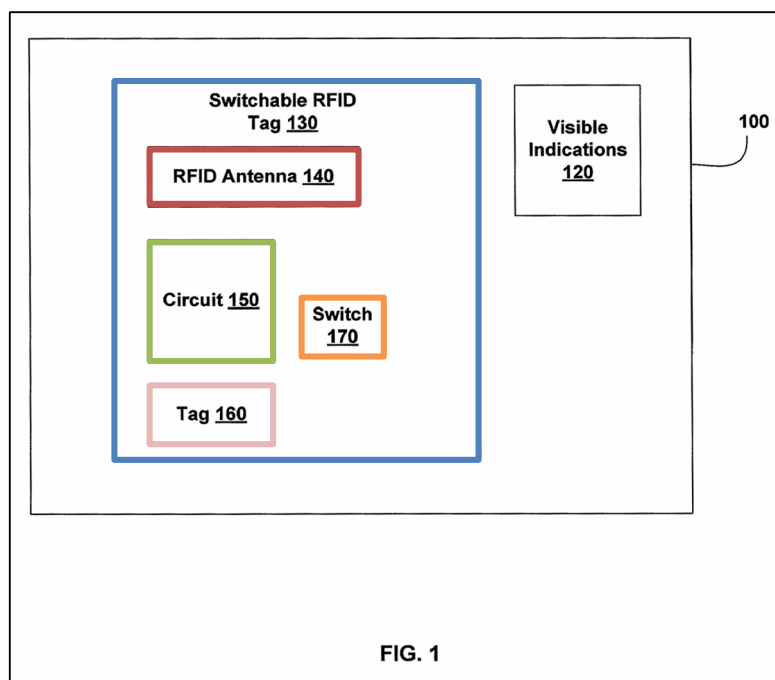
28. I have reviewed the ’156 Patent, which is entitled “Electronically Switchable RFID Tags.” EX1001 at Cover. I understand that the ’156 Patent was filed on July 19, 2006 and issued on April 12, 2011. *Id.* For purposes of this declaration, I have been asked to assume that the ’156 Patent has a priority date of May 6, 2005 based on a provisional application filed on that date.

29. 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 the time of the alleged invention of the ’156 Patent.

A. Subject Matter of the ’156 Patent

30. The ’156 Patent is directed to a “switchable” RFID tag 130, which includes an RFID antenna 140, circuit 150, switch 170, and tag 160. EX1001 at FIG.

1.



EX1001, FIG. 1.¹

31. Thus, the switch is operable to select a state of the tag, which can be an OFF state, in which transmission is disabled, or one of several ON states, each of which transmits different information via RFID communication. *Id.*, 20:50–59. More specifically, the specification provides that the switch is operable by a user to “repeatedly turn on and off the function (e.g., de[t]ectability or readability) of Tag 160.” *Id.*, 7:63–64. The “function (e.g., de[t]ectability or readability)” corresponds to an ON/OFF state of the tag. *Id.*, 19:30–33. In an OFF state, the tag will not emit RFID signals, and in an ON state, the tag will emit RFID signals. *Id.*, 7:23–35. The tag can also have multiple ON states, which are distinguished by the contents of data

¹ Unless otherwise noted, all colored/highlighted text/annotations in figures and emphasis in quotes are added.

encoded in the emitted RFID signal. *Id.*, 21:41–49. In one example provided by the specification, the tag can transmit a name, when in a first ON state, and can transmit a name and medical information, when in a second ON state. *Id.*

32. The circuit and RFID antenna facilitate RFID communication. The circuit facilitates on-tag communication by transmitting signals between the tag and the antenna. *Id.*, 3:43–50. The antenna receives power and data from an RFID reader, and transmits data, as controlled by the tag. *Id.*

B. Prosecution History of the '156 Patent

33. The '156 Patent was filed on July 19, 2006 (Application No. 11/458,620), originally with 34 claims, directed to an RFID tag and methods of operating the same. EX1001 at Cover; EX1007 at 232–237. It claims priority to a provisional application filed on May 6, 2005 (Application No. 60/678,428). EX1001 at Cover.

34. On March 30, 2009, the Examiner issued a first Non-Final Office Action, in which pending claims 1, 3–6, 8, 20–21, 25–27, and 29 were rejected under pre-AIA 35 U.S.C. §103(a) as unpatentable over U.S. Patent No. 7,246,754 (“Siuta”), and pending claims 10–12, 14, 18–19, 22, and 24 were rejected under pre-AIA 35 U.S.C. §103(a) as unpatentable over Siuta in view of U.S. Patent Publication No. 2004/0145453 (“Tuttle”). EX1007, at 157–63. Pending claims 2, 9, 13, 15–17, 23, and 28 were objected to as being dependent upon a rejected base claim, but were

indicated as otherwise being allowable if rewritten in independent form. *Id.*, at 163.

35. On July 20, 2009, Applicant submitted a Response to Non-Final Office Action, together with minor amendments to correct mislabeled claim numbers. *Id.*, 124–48. In the Response, Applicant traversed each of the Examiner’s rejections. In particular, Applicant argued that Siuta failed to render obvious pending independent claim 1, because Siuta’s disclosure of performing a read/write operation only upon successful authentication did not teach providing a second RF signal to the antenna. *Id.*, at 133. Additionally, Applicant argued that the Examiner failed to provide a proper motivation to add a memory to Siuta’s device. *Id.*, at 134. Regarding independent claims 10 and 20, Applicant similarly argued that the Examiner failed to provide a proper motivation to add a memory to Siuta’s device. *Id.*, at 137, 140. Regarding independent claim 10, Applicant also argued that the Examiner improperly combined the mechanical switch of Tuttle with Siuta’s device, because “[t]he addition of the teachings of Tuttle to those of Siuta would change Siuta from a key based authentication system to a mechanical switch based system. Specifically, the principle of operation would be changed from a key based authentication to a mechanical switch....Further, in the teachings of Siuta the authentication process is used to merely control a read or write operation NOT to disable [the] device entirely. (If the device were disabled entirely it wouldn’t be possible to make another authorization attempt.) In contrast, the mechanical switch of Tuttle appears to

completely disable the operation of the communications circuitry....Adding the mechanical switch of Tuttle would again change the principle of operation of Siuta because the entire communications ability would be shut down instead of merely read and write operations.” *Id.*, at 141.

36. On December 14, 2009, the Examiner issued a second Non-Final Office Action, in which pending claims 1, 3–5, 7–8, 20–21, 25–27, and 29 were again rejected under pre-AIA 35 U.S.C. §103(a) as unpatentable over Siuta, and pending claims 10–12, 14, 18–19, and 22 were again rejected under pre-AIA §103(a) as unpatentable over Siuta in view of Tuttle. *Id.*, at 102. Claims 2, 6, 9, 13, 15–17, 22–23, and 28 were objected to as being dependent upon a rejected base claim, but were otherwise indicated as being allowable if rewritten in independent form. *Id.*, at 108. Claims 30–34 were indicated as allowable, because according to the Examiner, “no prior arts have been found to fairly teach and suggest reading a state from a state memory, the state memory being configured to alternatively store an OFF state, a first ON state and a second ON state and sending a responsive signal being a response to the first signal, if the state is the first ON or the second ON state.” *Id.*

37. On March 15, 2010, Applicant submitted a Response to Non-Final Office Action, together with amendments cancelling pending claims 1, 10, and 20; amending claims 2–8, 11–19, and 21–29 to incorporate limitations that were indicated by the Examiner as being allowable; and adding new claims 35–57. *Id.*, at

77–94. Applicant did not include traversal arguments. *Id.*

38. On June 24, 2010, the Examiner issued a third Non-Final Office Action, in which pending claims 30–31 were rejected under pre-AIA 35 U.S.C. §103(a) as unpatentable over U.S. Patent Publication No. 2007/0075140 (“Guez”) in view of U.S. Patent No. 6,282,407 (“Vega”). *Id.*, at 64–65. Claims 32–34 were objected to as being dependent upon rejected base claims, but were otherwise indicated as being allowable if rewritten in independent form. *Id.*, at 66. Claims 2–9, 11–19, 21–29, and 35–57 were indicated as being allowable. *Id.*, 65.

39. On September 21, 2010, Applicant submitted a Response to Non-Final Office Action, together with amendments cancelling claim 30, amending claim 31 to depend from claim 32, rewriting claims 32–34 in independent form, and adding new claims 58–64. *Id.*, at 39–56. Applicant did not include traversal arguments. *Id.*

40. On December 16, 2010, the Examiner issued a Notice of Allowance, indicating that pending claims 2–9, 11–19, 21–29, and 31–64 were allowed. EX1007 at 9–12. No reasons for allowance were provided. *Id.*

C. RFID Communication Devices

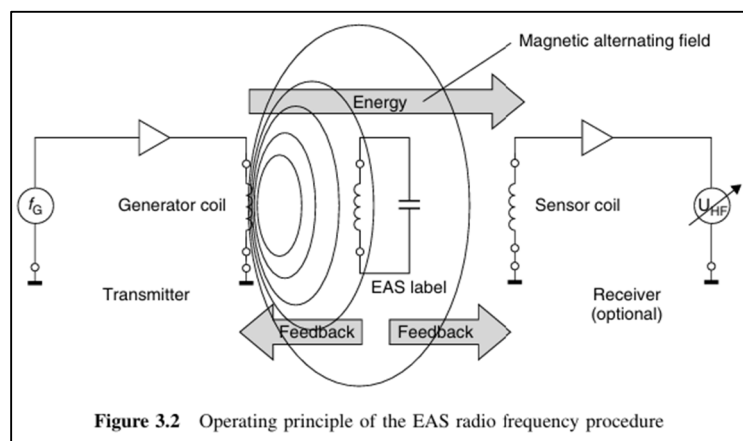
41. Based on my experience in the industry, I am familiar with the design of RFID communication devices of the type relevant to the ’156 Patent.

i. RFID

42. 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.*

43. 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.

44. 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.*

45. 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

46. 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.

47. 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.*

48. 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.*

49. 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

50. I am informed and understand that a 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.

51. In my opinion, a POSITA at the time of the alleged invention of the '156 Patent 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 '156 Patent, I had this level of skill. Around the time of the alleged invention, 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 the '156 Patent.

VII. CLAIM CONSTRUCTION

52. I understand that "claim construction" is the process of determining a patent claim'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.

53. I have been informed that the ’156 Patent 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	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
Response	Plain and ordinary meaning
Responsive	Plain and ordinary meaning
ON/OFF state	A switchable status that includes an OFF state and at least one ON state. An OFF state is one in which data cannot be

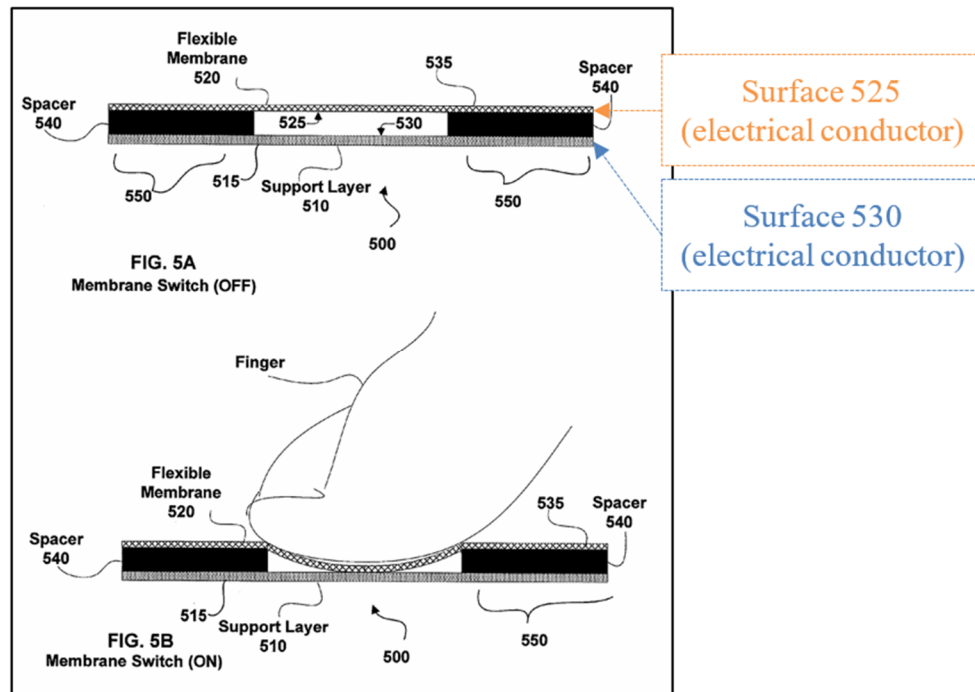
	transmitted from a RFID tag; an ON state is one in which data can be transmitted from a RFID tag
Switch	A control device that makes or breaks an electrical connection in a circuit
Switch logic	Circuitry and set or sets of logic instructions directing the operation of a RFID tag
Passport	A passport booklet

EX1022, at 15, 20, 41.

54. 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 '156 Patent claims is based on these claim constructions.

55. 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 specification of the '156 Patent describes switch 170, 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.” EX1001, 8:10–14, 20:49–53. 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. Further, as described in the specification, the mechanical switch can be “activated by applying pressure to an

outside surface of Switchable RFID Device 100.” *Id.*, 8:18–21. The mechanical switch can also be “configured to be moved between the on position and the off position, for example using a finger.” *Id.*, 9:17–28. Further, Figures 5A–B (reproduced below) illustrate a “membrane switch,” which is a type of mechanical switch. *Id.*, 8:10–14. In this example, the switch is illustrated as making or breaking an electrical connection between surfaces 525 and 530, which are both electrical conductors, responsive to a user pressing flexible membrane 520. 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.



EX1001, FIGs. 5A–B.

VIII. SUMMARY OF PRIOR ART

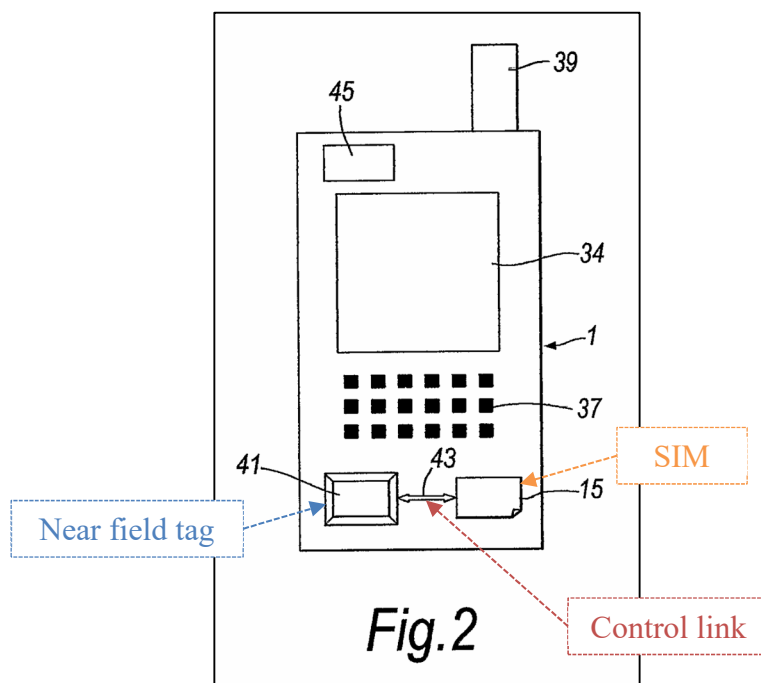
A. *Waters* (EX1024)

56. 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 ’156 Patent by over a year.

57. *Waters* relates to an RFID-enabled cellphone having a SIM 15 which includes² 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

² 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].

sensors, heat sensors, skin resistance sensors, and inertial sensors to authenticate a user and enable RFID communication. *Id.*, [0051]–[0053].



Id., FIG. 2.

58. 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.*

59. *Waters* is in the same field of endeavor as the ’156 Patent—RFID-enabled communication devices—and in my opinion, *Waters* provides an alternative

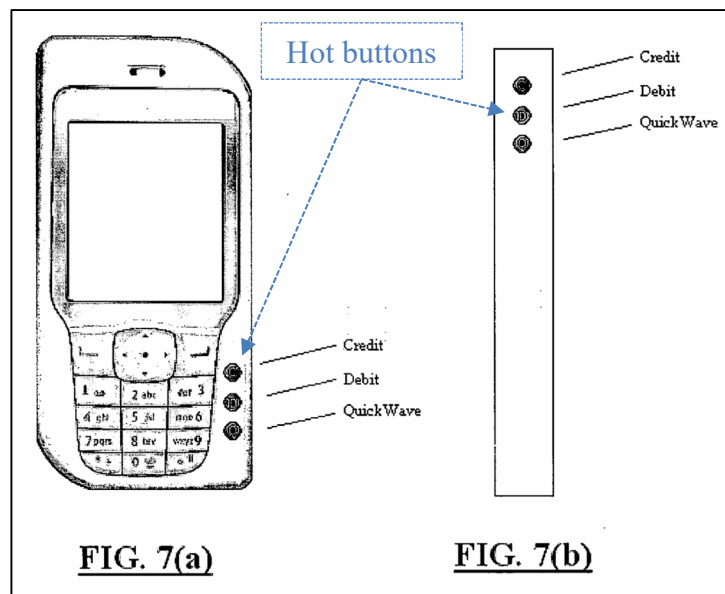
design that would have been available to a POSITA at the time of invention.

B. *Dua* (EX1023)

60. 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 ’156 Patent by over a year.

61. 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.

62. *Dua* is in the same field of endeavor as the '156 Patent—RFID-enabled communication devices—and in my opinion, *Dua* provides an alternative design that would have been available to a POSITA at the time of invention.

C. *Pont* (EX1026)

63. Michael *Pont*, *Embedded C* (2002) (“*Pont*”) is a textbook, which was

published in 2002. EX1026, at iv; EX1019, at 24. Thus, *Pont* predates the '156 Patent by over a year.

64. *Pont* relates to techniques for programming embedded processors using the C programming language. *Id.*, xi. *Pont* discloses that such processors are suitable for a variety of applications, including in mobile phones. *Id.*, xi, 2. *Pont* provides useful guidance for a programmer seeking to program an embedded processor to control an output based on a peripheral input, which is similar to the use cases of *Waters* and *Dua*, wherein the device must control an RFID interface (output) based on a pressure sensor, keypad, button, etc. (input). *Id.*, ch. 4. To do so, *Pont* teaches that a processor can be programmed to poll an input pin, assign the input value to an input state variable, perform logic using the input state variable, and set an output state variable based on the logic. *Id.*, 71–74.

```
/*-----*/
Switch_read.C (v1.00)
-----

A simple 'switch input' program for the 8051.
- Reads (and debounces) switch input on Pin1^0
- If switch is pressed, changes Port 3 output
/*-----*/

#include <Reg52.h>

// Connect switch to this pin
sbit Switch_pin = P1^0;

// Display switch status on this port
#define Output_port P3
```

Logic based on
input state variable

Assigning input state variable

Polling input pin

```
// Return values from Switch_Get_Input()
#define SWITCH_NOT_PRESSED (bit) 0
#define SWITCH_PRESSED (bit) 1

// Function prototypes
void SWITCH_Init(void);
bit SWITCH_Get_Input(const unsigned char DEBOUNCE_PERIOD);
void DISPLAY_SWITCH_STATUS_Init(void);
void DISPLAY_SWITCH_STATUS_Update(const bit);
void DELAY_LOOP_Wait(const unsigned int DELAY_MS);

/* ----- */
void main(void)
{
    bit Sw_state;

    // Init functions
    SWITCH_Init();
    DISPLAY_SWITCH_STATUS_Init();

    while(1)
    {
        Sw_state = SWITCH_Get_Input(30);
        DISPLAY_SWITCH_STATUS_Update(Sw_state);
    }
}

/* ----- */
void SWITCH_Init()
{
    Initialisation function for the switch library.
}

/* ----- */
void SWITCH_Get_Input()
{
    Switch_pin = 1; // Use this pin for input
}

/* ----- */
SWITCH_Get_Input()
{
    Reads and debounces a mechanical switch as follows:

```

```
1. If switch is not pressed, return SWITCH_NOT_PRESSED.
2. If switch is pressed, wait for DEBOUNCE_PERIOD (in ms),
   then:
   a. If switch is still pressed, return SWITCH_PRESSED.
   b. If switch is not pressed, return SWITCH_NOT_PRESSED.
See Switch_Wait.H for details of return values.
/* ----- */
bit SWITCH_Get_Input(const unsigned char DEBOUNCE_PERIOD)
{
    bit Return_value = SWITCH_NOT_PRESSED;

    if (Switch_pin == 0)
    {
        // Switch is pressed

        // Debounce - just wait...
        DELAY_LOOP_Wait(DEBOUNCE_PERIOD);

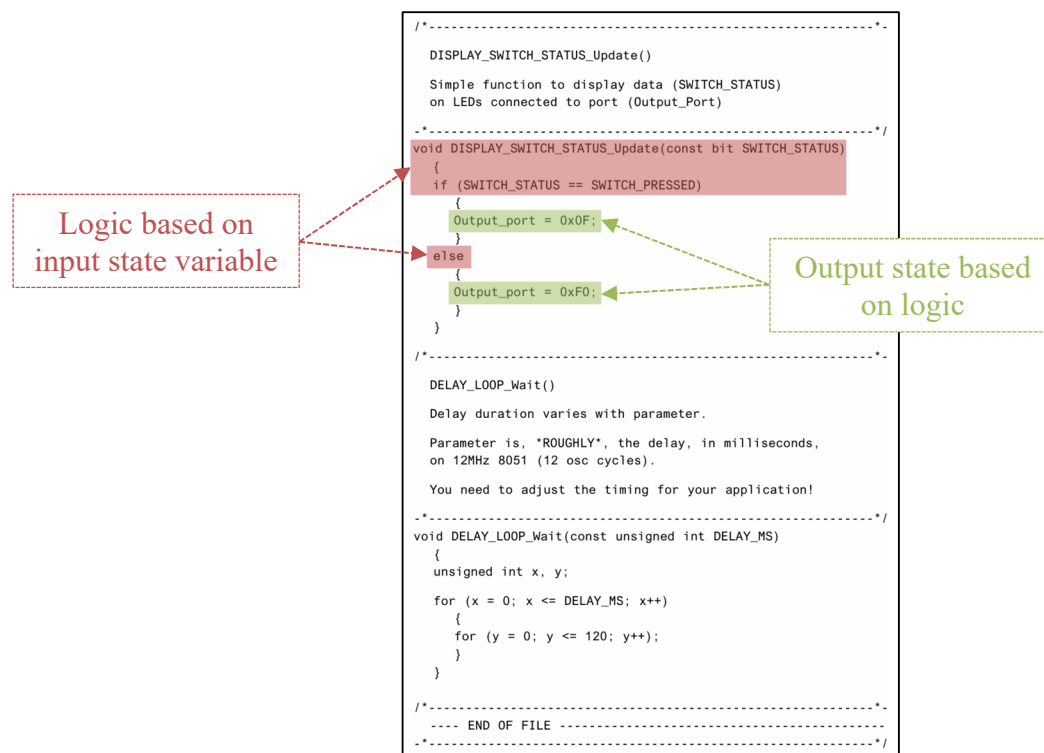
        // Check switch again
        if (Switch_pin == 0)
        {
            Return_value = SWITCH_PRESSED;
        }
    }

    // Now return switch value
    return Return_value;
}

/* ----- */
DISPLAY_SWITCH_STATUS_Init()
{
    Initialization function for the DISPLAY_SWITCH_STATUS library.
}

/* ----- */
void DISPLAY_SWITCH_STATUS_Init(void)
{
    Output_port = 0xF0;
}

```



EX1026, 71–74.

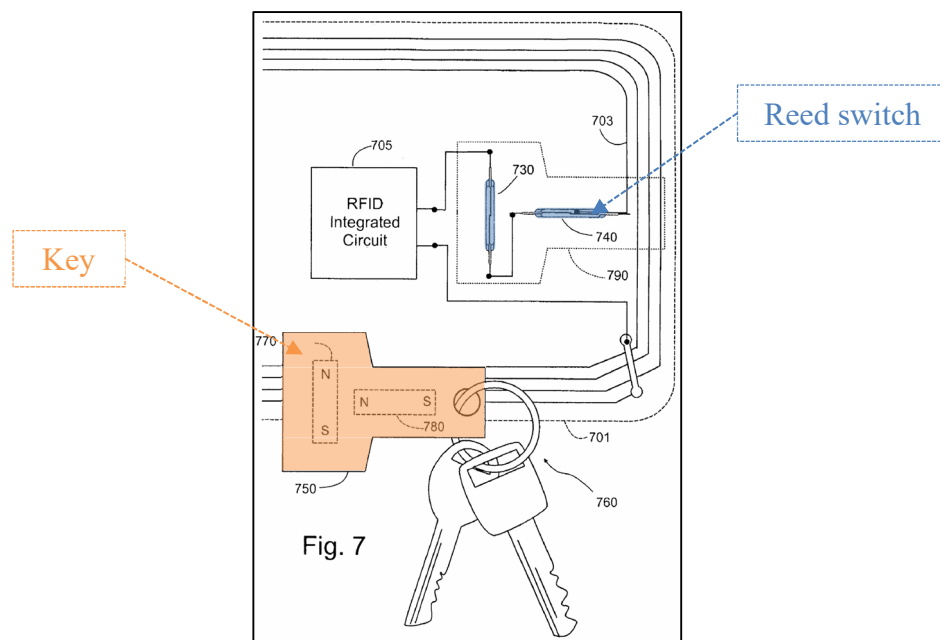
65. *Pont* is in the same field of endeavor as the '156 Patent—communication devices—and in my opinion, *Pont* provides an alternative design that would have been available to a POSITA at the time of invention.

D. *Selker* (EX1027)

66. U.S. Patent Publication No. 2003/0132301 ("*Selker*") was filed on December 31, 2002, and published on July 17, 2003. EX1027, at Cover. Thus, *Selker* predates the '156 Patent by over a year.

67. *Selker* relates to an RFID-enabled smart card, on which various types of security measures can be implemented. *Id.*, Abstract. In one embodiment, *Selker* discloses a reed switch and key mechanism, which is operable to close a circuit

between an RFID integrated circuit (control circuitry) and an RFID antenna, when the **key** is brought in close proximity to the **reed switches**. *Id.*, [0004], [0027], [0031], FIG. 7.



Id., FIG. 7.

68. More specifically, the on-card structure comprises two perpendicularly-arranged reed switches connected in series. EX1027, [0027], FIG. 7. The off-card key includes two perpendicularly-arranged magnets, corresponding to each reed switch. *Id.* When the key is brought in close proximity to the card, and aligned with the reed switches, the reed switches close, and the circuit is completed. *Id.* Thus, only a person in possession of a matching key can close the circuit and enable RFID signal transmission. *Id.*

69. According to *Selker*, this technique can also be applied using “different

keys, or different placements of a single key...to selectively close only certain on-card switches to provide the needed connections.” *Id.*, [0031].

70. *Selker* is in the same field of endeavor as the ’156 Patent—RFID-enabled communication devices—and in my opinion, *Selker* provides an alternative design that would have been available to a POSITA at the time of invention.

IX. SUMMARY OF PRIOR ART GROUNDS

Ground	Claims	Basis	Prior Art
1A	1–33, 51–60	Obviousness	<i>Waters</i>
1B	1–33, 51–60	Obviousness	<i>Waters</i> with <i>Pont</i>
1C	39–43	Obviousness	<i>Waters</i> with <i>Selker</i>
2A	1–10, 14–38, 44–59	Obviousness	<i>Dua</i>
2B	1–10, 14–38, 44–59	Obviousness	<i>Dua</i> with <i>Pont</i>
2C	39–43	Obviousness	<i>Dua</i> with <i>Selker</i>

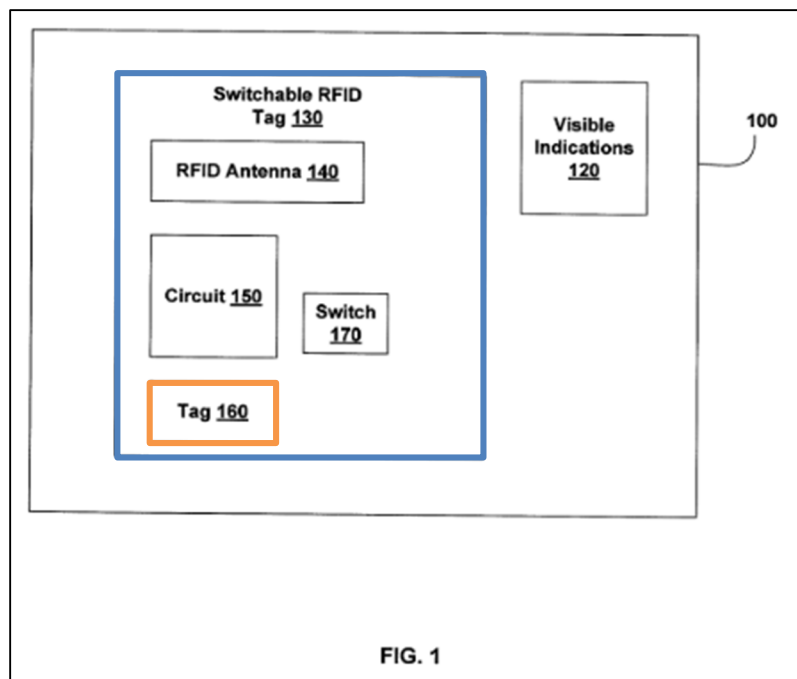
X. GROUND 1A: *WATERS* RENDERS OBVIOUS CLAIMS 1–33 AND 51–60

71. *Waters* renders obvious claims 1–33 and 51–60.

A. Independent Claim 1

i. 1[pre]

72. The '156 Patent uses the term “RFID tag” to encompass a Radio Frequency Identification Device, which includes a “tag” that facilitates RFID communication. See EX1001, FIG. 1 (below).



73. *Waters* likewise discloses SIM 15, which includes two substructures: near field tag 41 and control link 43. EX1024, [0037], [0057]. For example, *Waters* explicitly discloses that “the mechanism for activating/deactivating the tag,” which corresponds to control link 43, “may be incorporated directly into...SIM 15 itself.” *Id.* Similarly, *Waters* discloses that “the tag 41 or part of the tag 41 may be incorporated into the SIM 15.” *Id.* Near field tag 41 provides RFID communication functionality and SIM 15 controls tag 41 through control link 43. EX1024, [0035]–

[0037].

74. Therefore, in my opinion, *Waters*'s SIM 15 corresponds to the claimed RFID tag, because it is a Radio Frequency Identification Device and includes a "tag" that facilitates RFID communication.

75. Therefore, in my opinion, *Waters* discloses limitation 1[pre].

ii. 1[a]

76. *Waters* discloses "an antenna configured to receive data in a first RF signal, to receive energy from the first RF signal, and to transmit data in a second RF signal, the transmission of the second RF signal being powered by the energy received from the first RF signal."

77. Tag 41 includes an "inbuilt inductive antenna" (antenna), which is able to receive data and power from a signal emitted by an RFID reader (first RF signal) and "exchange information" with the RFID reader when in "close proximity," including financial transaction data (second RF signal). *Id.*, [0035]; Abstract. Specifically, *Waters* discloses that the "inbuilt inductive antenna...allows the card to exchange information with a tag reader when the two are brought into close proximity," and that "[t]he reader may emit an RF signal to supply power to the tag to communicate with it if the tag is 'passive.'" *Id.* *Waters* likewise describes using "the near field tag (41) to make a payment." *Id.*, Abstract, [0043]. Tag 41 may be "passive," such that transmission of the financial transaction data (second RF signal)

is powered by the energy received from the signal emitted by the RFID reader (first RF signal). *Id.*, [0035]. Such passive RFID technologies were well-known in the art.

78. Therefore, in my opinion, *Waters* discloses limitation 1[a].

iii. 1[b]

79. *Waters* renders obvious “integrated circuitry including an input configured to receive data from the antenna and to receive power resulting from the energy received from the antenna.”

80. *Waters*’s device circuitry receives both data and power. For example, *Waters* discloses that its circuitry receives RFID data from a tag reader via the inductive antenna. *Id.*, [0035] (“tag 41 includes an inbuilt inductive antenna that allows the card to exchange information with a tag reader”). Additionally, the device can be “passive,” such that its circuitry additionally receives power from the RFID signal emitted by the tag reader. *Id.*, [0035] (“The reader may emit an RF signal to supply power to the tag to communicate with it if the tag is ‘passive’”); Abstract.

81. In my opinion, a POSITA would have understood that an input to receive and analyze data and power necessarily flows or is a natural result of such RFID functionality. Without such an input, *Waters*’s circuitry would not be capable of receiving power or data from the antenna, or any other source, as described throughout its specification. *Id.*, [0035] (the circuitry receives data and power from the antenna), [0051] (the circuitry also receives data from a keypad).

82. To the extent that *Waters* does not explicitly describe an integrated circuit, it does discuss in depth the functionality underlying this element. In particular, as noted above, *Waters* describes passive RFID circuitry, powered by a reader's RF signal. In my opinion, a POSITA would understand that such RFID circuitry would contain integrated circuitry coupled to the antenna, to obtain data and operating power. Further, such integrated circuits were commonly used in mobile phone and RFID applications to provide communications and control functionality, with increased efficiency and decreased cost, compared to other methods. EX1029, 292–293; EX1026, 4. Thus, in my opinion, it would also have been obvious to a POSITA that the functionality described above would be implemented as integrated circuitry.

83. Thus, in my opinion, and as described above, *Waters* discloses or otherwise renders obvious that the device circuitry includes an inductive antenna that exchanges information with a reader, that the reader supplies data and power to the device circuitry, and that the device circuitry transmits selected information to the reader.

84. Therefore, in my opinion, *Waters* renders obvious limitation 1[b].

iv. 1[c]

85. *Waters* discloses “integrated circuitry including...an output configured to provide the second RF signal to the antenna for transmission.”

86. Similar to the above, tag 41 (including SIM 15, which *Waters* explains provides “control...to the operation of” tag 41) controls the inductive antenna to “exchange information” (send/receive data) with a “tag reader when the two are brought into close proximity.” EX1024, [0035]. *Waters* discloses, for example, that “[t]he near field tag 41 may transmit selected information, such as an ID number (GU ID).” *Id.* That functionality includes an output that provides financial transaction data to the antenna. *Id.*, Abstract (disclosing that “near field tag (41) may...be read by a reader” and that the near field tag may be used “to make a payment”), [0045] (“the school child is able to use their RF tag to make payments”). The financial transaction data corresponds to a second RF signal because it is an RFID (RF) signal that is transmitted from the device’s antenna to the reader. For instance, *Waters* describes using “the near field tag (41) to make a payment,” and permitting users to “use their RF tag to make payments.” *Id.*, Abstract (disclosing that “near field tag (41) may...be read by a reader” and that the near field tag may be used “to make a payment”), [0045] (“the school child is able to use their RF tag to make payments”).

87. Therefore, in my opinion, *Waters* discloses limitation 1[c].

v. 1[d]

88. *Waters* renders obvious “integrated circuitry including...a state memory configured to store an ON/OFF state including two or more ON states of

the RFID tag.”

89. Tag 41 (controlled by SIM 15) may first enter a jamming state (first ON state), then transition to a transaction state (second ON state) upon successful entry of a PIN, and then transition to a deactivated state (OFF state) after being read by a reader. In the jamming state (first ON state), the “near field tag 41 and/or the mobile terminal 1 is designed to jam/disrupt the low level communications of all other RF tags within range of the jamming device,” and, “[i]nstead of following the anti-collision protocol commonly used in near field tag technology, the device attempts to create collisions and other forms of interference,” such that other RFID tags cannot nefariously communicate with a nearby RFID reader. EX1024, [0055]. In my opinion, a POSITA would understand that “the device attempts to create collisions and other forms of interference” by constantly emitting RFID signals. In my opinion, a POSITA would understand that the data encoded in such signals could be random data, or some other structured data. In any case, the transmission of a signal (jamming or otherwise) shows that data is being processed by the tag and transmitted via the antenna. Thus, the jamming state corresponds to a first ON state, because in this state, the device can (and constantly does) transmit data. *See supra* §VII (“an ON state is one in which data can be transmitted from a RFID tag”).

90. The jamming functionality is disabled when “authorized use” of the device is required. *Id.* *Waters* discloses that a PIN can be used to authorize a user

prior to a transaction. *Id.* For example, according to *Waters*, “mobile terminal (1) is operable to obtain security data from the user thereof, such as a PIN....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....” *Id.*, Abstract. *Waters* further provides 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.” *Id.*, [0051]. Thus, in my opinion, a POSITA would understand that when a PIN is successfully entered by a user, the jamming functionality can be disabled and near field tag 41 can transition from the jamming state (first ON state) to a transaction state (second ON state), in which near field tag 41 can communicate with an RFID reader to facilitate a financial transaction. *Id.*, Abstract, [0045], [0051], [0055]–[0056]. Then, near field tag 41 may automatically enter a deactivated state (OFF state), in which no RFID signals are communicated, after it has been read by an RFID reader. *Id.*, [0052]. In that state, RFID communication is disabled. *Id.*

91. Moreover, the device includes memory, and in my opinion, a POSITA would have understood that the current state (jamming, transaction enabled, or deactivated) would be stored in that memory, reflecting the current device state. *Id.*, [0036], [0051]. For example, the state could be stored in the memory of SIM 15, near field tag 41, or other on-device memory. *Id.* Alternatively, in my opinion, it would have been obvious to a POSITA to store the current state (jamming,

transaction, or deactivated) of near field tag 41 in memory (state memory), to enable implementation of the logic described above (transitioning from the jamming state to the transaction state responsive to a PIN, and transitioning from the transaction state to the deactivated state responsive to being read by an RFID reader). *Id.* That is, in my opinion, it would have been obvious to a POSITA that like any other processor, SIM 15 and near field tag 41 have memory for the operation of each state (respective state values would be assigned to the jamming, transaction, and deactivated modes), and the current value of the state would be stored in memory. The controller would read the stored state, process the applicable event or instruction, and write the resulting next state. For example, as described above, near field tag 41 determines state transitions based on (1) a PIN and (2) whether the tag has been read by an RFID reader. Both of these logical transitions require reading an input and applying logic based on its status. In my opinion, a POSITA would have understood that to implement such functionality, the control software of near field tag 41 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 as of the time of invention. *See* EX1026, 72 (storing switch state in a “Sw_state” variable), 74 (applying logic to “Sw_state” variable and storing output state in an “Output_port” variable). The value of the state variable would be stored in device 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. As *Pont* explains, “DATA memory is used to store variables and the program stack while the program is running. The DATA area will be implemented using some form of RAM.” *See id.*, 26.

92. Therefore, in my opinion, *Waters* renders obvious limitation 1[d].

vi. 1[e]

93. *Waters* discloses “integrated circuitry including...a key memory configured for storing a key for changing the ON/OFF state stored in the state memory.”

94. The PIN (key) can be stored in a “secure location” (key memory) of SIM 15 (RFID tag). EX1024, [0051], [0057]. Specifically, *Waters* discloses that “[t]he user’s PIN may be stored in a secure location in...the SIM 15,” and that “the tag 41 or part of the tag 41 may be incorporated into the SIM 15.” *Id.* As discussed above with reference to limitation 1[d], the PIN (key) is used to change the state held in state memory from a jamming state (first ON state) to a transaction state (second ON state). *See supra* §X.A.v.

95. Therefore, in my opinion, *Waters* discloses limitation 1[e].

vii. 1[f]

96. *Waters* discloses “integrated circuitry including...a switch logic configured to receive data from the input, to read the key from the key memory, to

compare the received data with the read key, and to change the ON/OFF state stored in the state memory responsive to this comparison.”

97. As discussed above, *Waters* discloses that a PIN is used to transition from the jamming state (first ON state) to the transaction state (second ON state). In particular, a PIN (data) is received from a keypad of the device. EX1024, [0051]. Then, a stored PIN (key) is read from a secure location (key memory) of SIM 15 (RFID tag) and compared with the entered PIN (data). *Id.* As *Waters* explains, “[w]hen 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.” *Id.* If the entered PIN (data) matches the stored PIN (key), SIM 15 (RFID tag) controls near field tag 41 to transition from a jamming state (first ON state) to a transaction state (second ON state). *Id.*, [0051], [0057]; *see supra* §X.A.v.

98. Therefore, in my opinion, *Waters* discloses limitation 1[f].

viii. 1[g]

99. *Waters* discloses “the switch logic being further configured to determine whether or not to provide the second RF signal to the antenna for transmission, the determination being responsive to the ON/OFF state stored in the state memory.”

100. As discussed above with reference to limitation 1[d], *Waters* discloses

logic that determines whether to provide financial transaction data (second RF signal) to the antenna for transmission, based on the current state (jamming, transaction, or deactivated) stored in state memory. *See supra* §X.A.v.

101. Therefore, in my opinion, *Waters* discloses limitation 1[g].

B. Independent Claim 11

i. 11[pre]–[g]

102. In my opinion, *Waters* discloses and/or renders obvious limitations 11[pre]–[g] for the same reasons discussed above in connection with limitations 1[pre]–[g]. *See supra* §X.A.i–viii.

ii. 11[h]

103. *Waters* discloses “the state memory or switch logic are shared by two or more RFID tags.”

104. A single mobile terminal (e.g., a mobile telephone) can include multiple RFID tags, each of which is controlled by a shared controller that implements the logic described above (switch logic). EX1024, [0005], [0076]. *Waters* discloses that “mobile terminal 1 may be a handheld mobile telephone,” and that “multiple near field tags may be incorporated in a single SIM or mobile terminal. The SIM may control each of these tags separately.” *Id.*, [0005], [0076].

105. Therefore, in my opinion, *Waters* discloses limitation 11[h].

C. Independent Claim 14

i. 14[pre]–[c]

106. In my opinion, *Waters* discloses and/or renders obvious limitations 14[pre]–[c] for the same reasons discussed above in connection with limitations 1[pre]–[c]. *See supra* §X.A.i–iv.

ii. 14[d]

107. *Waters* renders obvious “integrated circuitry including...a state memory configured to store an ON/OFF state of the RFID tag, the ON/OFF state being responsive to timing using a resister-capacitor circuit.”

108. *Waters* likewise renders obvious “a state memory configured to store an ON/OFF state of the RFID tag” for the same reasons discussed above with respect to limitation 1[d]. *See supra* §X.A.v.

109. *Waters* also describes that its device can incorporate multiple timing-based functionalities. For example, tag 41, under control of SIM 15, can include a “round trip detector,” which operates when tag 41 is in an ON state and “sends a test signal when the near field tag 41 is being read/probed and expects a response within a certain round trip delay.” EX1024, [0055]–[0056]. The detector “measures the time taken for a signal to travel from the near field tag 41 to the reader and back to the tag 41,” to assess whether the near field tag 41 is within an acceptable range of an RFID reader. *Id.* If the response signal is not received from the RFID reader after a

“predetermined delay” (i.e., near field tag 41 is far from the RFID reader, which has an “RF field[] that [has] been greatly extended”), near field tag 41 enters the deactivated state (OFF state). *Id.* Additionally or alternatively, the near field tag 41 can “be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present.” *Id.*, Abstract. *Waters* also describes that the near field tag 41 can be enabled or disabled responsive to the time of day. *Id.*, [0041].

110. In my opinion, it would have been obvious to a POSITA that the timing functionality described above could be implemented using a resistor-capacitor (“RC”) circuit, as it was well known in the art to build timers using RC circuits. *See, e.g.*, EX1028, 10-1 (“RC networks are probably the most commonly used delay networks”); EX1029, 276–78 (discussing use of RC timers in RFID applications). In my opinion, a POSITA implementing such predetermined-time deactivation functionality would have recognized a resistor-capacitor timing circuit as a conventional, inexpensive, and predictable circuit for defining the duration of the temporary ON state.

111. Therefore, in my opinion, *Waters* renders obvious limitation 14[d].

iii. 14[e]–[g]

112. In my opinion, *Waters* discloses and/or renders obvious limitations 14[e]–[g] for the same reasons discussed above in connection with limitations 1[e]–

[g]. *See supra* §X.A.vi–viii.

D. Independent Claim 20

i. 20[pre]

113. In my opinion, *Waters* discloses limitation 20[pre] for the same reasons discussed above in connection with limitation 1[pre]. *See supra* §X.A.i.

ii. 20[a]

114. *Waters* discloses “a mechanical switch configured for selecting between two or more ON states of the RFID tag.”

115. As discussed above with respect to limitation 1[d], near field tag 41 (incorporated in SIM 15) is configured to transition between a jamming state (first ON state) and a transaction state (second ON state). *See supra* §X.A.v. *Waters* further discloses that this state transition is triggered by activation of a pressure sensor (mechanical switch) by a user. EX1024, [0053], [0056]. Therefore, the pressure sensor allows a user to select between the jamming state (first ON state) and transaction state (second ON state) by pressing and activating the pressure sensor. In my opinion, the pressure sensor discloses a mechanical switch because it controls circuit components by making or breaking an electrical connection in the device circuitry, responsive to its components being pressed (moved) by a user. *Id.*, [0053]. *Waters*’s pressure sensor is similar to the pressure-sensitive mechanical switch described in the ’156 Patent specification. EX1001, 8:19–23 (“In some

embodiments, Switch 170 is a mechanical contact switch activated by applying pressure to an outside surface of Switchable RFID Device 100. In some embodiments, when this pressure is applied the functionality of Tag 160 will be turned on, and when this pressure is not applied the functionality of Tag 160 will be off.”); *see also* §VII (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.”).

116. Additionally, *Waters* discloses that the jamming functionality “is disabled...when authorized use of the card is required.” EX1024, [0055]; *see supra* §X.A.v. *Waters* further discloses that the pressure 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.” EX1024, Abstract. In my opinion, a POSITA would understand these disclosures to mean that when the pressure sensor is activated by the user, (1) “authorized use” is required, and the jamming functionality is disabled, and (2) the device will enter a state in which a financial transaction can be carried out via RFID communication. Thus, in my opinion, when the user presses the pressure sensor, the device transitions from a jamming state (first ON state) to a transaction state (second ON state), such that RFID communication is enabled and a transaction can be facilitated. EX1024, Abstract, [0053], [0055], [0056].

117. Therefore, in my opinion, *Waters* discloses limitation 20[a].

iii. 20[b]–[e]

118. In my opinion, *Waters* discloses and/or renders obvious limitations 20[b]–[e] for the same reasons discussed above in connection with limitations 1[a]–[d]. *See supra* §X.A.ii–v.

iv. 20[f]

119. *Waters* renders obvious “integrated circuitry including...a switch logic configured to receive data from the input, and to determine whether or not to provide the second RF signal to the antenna for transmission, the determination being responsive to the state stored in the state memory or the mechanical switch.”

120. As discussed above with reference to limitation 1[b], near field tag 41 receives data from an input. *See supra* §X.A.iii. For example, the tag receives reader information through its inductive antenna, and the tag’s processing logic receives or processes the data delivered from the antenna-side input. EX1024, [0035]–[0037].

121. As discussed above with reference to limitation 20[a], near field tag 41 determines whether to provide financial transaction data (second RF signal) to the antenna for transmission, based on the pressure sensor (mechanical switch). *See supra* §X.D.ii. In the alternative, it is my opinion that, as discussed above with respect to limitation 1[g], it would have been obvious to a POSITA that such determination can be based on the state stored in state memory. *See supra* §X.A.viii.

122. Therefore, in my opinion, *Waters* renders obvious limitation 20[f].

E. Independent Claim 29

i. 29[pre]

123. In my opinion, *Waters* discloses limitation 29[pre] for the same reasons discussed above in connection with limitation 1[pre]. *See supra* §X.A.i.

ii. 29[a]

124. *Waters* renders obvious “a mechanical switch configured to set a state of the RFID tag stored in a state memory.”

125. As discussed above with reference to limitation 20[a], *Waters* discloses a pressure sensor (mechanical switch) configured to select between a jamming state (first ON state) and a transaction state (second ON state). *See supra* §X.D.ii. In my opinion, as further discussed above, it would have been obvious to a POSITA to store the current state (set by the mechanical switch) within memory (state memory). *See supra* §X.A.v.

126. Therefore, in my opinion, *Waters* renders obvious limitation 29[a].

iii. 29[b]–[f]

127. In my opinion, as discussed above, with reference to claim 1, *Waters* discloses and/or renders obvious limitations 29[b]–[e]. *See supra* §X.A.ii–v. As further discussed above with reference to claim 20, *Waters* renders obvious limitation 29[f]. *See supra* §X.D.iv.

F. Independent Claim 51

i. 51[pre]–[f]

128. In my opinion, *Waters* discloses and/or renders obvious limitations 51[pre]–[f] for the same reasons discussed above in connection with claims 1 and 20. *See supra* §§X.A, X.D.

G. Independent Claim 53

i. 53[pre]–[e]

129. In my opinion, *Waters* discloses and/or renders obvious limitations 53[pre]–[e] for the same reasons discussed above in connection with claims 1 and 20. *See supra* §§X.A, X.D.

ii. 53[f]

130. *Waters* discloses “providing an RF response, a content of data in the RF response being responsive to the comparison.”

131. As discussed above with reference to limitations 1[d] and 1[f], near field tag 41 can emit (provide an RF response) either (1) jamming signals (first content type) in a jamming state (first ON state), or (2) transaction data (second content type) in a transaction state (second ON state), based on whether a user is authenticated (i.e., whether an input PIN matches a stored PIN) (responsive to the comparison). *See supra* §§X.A.v, X.A.vii.

132. Therefore, in my opinion, *Waters* discloses limitation 53[f].

H. Independent Claim 54

i. 54[pre]–[a]

133. In my opinion, *Waters* discloses limitations 54[pre]–[a] for the same reasons discussed above in connection with claims 1 and 20. *See supra* §§X.A, X.D.

ii. 54[b]

134. In my opinion, *Waters* renders obvious “reading a state from a state memory, the state memory being configured to alternatively store an OFF state, a first ON state and a second ON state” for the same reasons discussed above in connection with limitations 1[d] and 1[g]. *See supra* §§X.A.v (storing an OFF state, a first ON state, and a second ON state in state memory), X.A.viii (reading the state from state memory to determine whether to provide a response signal).

iii. 54[c]–[d]

135. In my opinion, *Waters* discloses limitations 54[c]–[d] for the same reasons discussed above in connection with limitations 1[d] and 1[g]. *See supra* §§X.A.v (contents of response signal depend on whether the current state is the first ON state or the second ON state), X.A.viii (sending response signal using antenna depending on whether the current state is the first ON state or the second ON state).

I. Independent Claim 57

i. 57[pre]–[a]

136. In my opinion, *Waters* discloses limitations 57[pre]–[a] for the same reasons discussed above in connection with claim 1. *See supra* §X.A.

ii. 57[b]–[c]

137. In my opinion, *Waters* discloses limitations 57[b]–[c] for the same reasons discussed above in connection with limitations 54[b]–[c]. *See supra* §§X.H.ii–iii.

iii. 57[d]

138. In my opinion, *Waters* discloses “sending the response signal is responsive to a mechanical switch” for the same reasons discussed above in connection with limitation 20[f]. *See supra* §X.D.iv.

J. Independent Claim 60

i. 60[pre]–[a]

139. In my opinion, *Waters* discloses limitations 60[pre]–[a] for the same reasons discussed above in connection with claim 1. *See supra* §X.A.

ii. 60[b]–[c]

140. In my opinion, *Waters* discloses limitations 60[b]–[c] for the same reasons discussed above in connection with limitations 54[b]–[c]. *See supra* §§X.H.ii–iii.

iii. 60[d]

141. *Waters* renders obvious “changing the state in the state memory responsive to an RF signal.”

142. Tag 41, which is under control of the SIM 15 (RFID tag), can be “automatically deactivat[ed] after it has been read by a reader.” EX1024, [0052]–

[0054], [0074]. Therefore, the RFID tag may transition from a transaction state (second ON state) to a deactivated state (an OFF state), responsive to an interrogation signal (RF signal) received from the RFID reader.

143. In my opinion, as discussed above with reference to limitation 1[d], it would have been obvious to a POSITA to store the current state in state memory. *See supra* §X.A.v. Consequently, the current state in state memory would be changed from a transaction state (second ON state) to a deactivated state (an OFF state), responsive to an interrogation signal (RF signal) received from the RFID reader.

144. Therefore, in my opinion, *Waters* renders obvious limitation 60[d].

K. Dependent Claims

i. Dependent Claims 2, 15

145. *Waters* discloses “the ON/OFF state of the RFID tag is OFF by default and temporally ON.” As discussed above with reference to limitation 1[d], near field tag 41 can, by default, enter a disabled (OFF) state, in which no RFID signals are communicated, and is only temporally or temporarily enabled when the user enters a PIN or presses a pressure sensor, after which it automatically reverts to the disabled state (OFF state). *See supra* §X.A.v; EX1024, [0053]–[0054].

146. Therefore, in my opinion, *Waters* discloses claims 2 and 15.

ii. Dependent Claims 3, 16

147. *Waters* renders obvious “the ON/OFF state of the RFID tag is stored in static memory” for the same reasons discussed above with reference to limitation 1[d]. *See supra* §X.A.v. In my opinion, as discussed above, when programming the RFID controller, it would have been obvious to a POSITA to store the ON/OFF state of near field tag 41 as a value of a state variable, such that operations (e.g., communication and state transitions) can be performed based on the current state. EX1026, 26, 47, 72–74. In my opinion, it would have been further obvious to a POSITA that data memory (which stores variable values) would be implemented as static RAM, as this was a well-known practice as of the time of invention. *Id.*

148. Therefore, in my opinion, *Waters* renders obvious claims 3 and 16.

iii. Dependent Claim 4

149. In my opinion, *Waters* renders obvious “the determination is responsive to which of the alternative ON states are stored in the state memory” for the same reasons discussed above in connection with limitation 1[g]. *See supra* §X.A.viii.

iv. Dependent Claim 5

150. *Waters* renders obvious “the RFID tag is disposed within a passport.” *Waters* teaches incorporating near field tag 41 into portable smart cards and credential devices employed “to obtain entry to a building (for example).” EX1024, Abstract, [0002]. Thus, in my opinion, it would have been obvious to a POSITA to

implement such an RFID tag within a passport, as RFID-enabled passports are used to “obtain entry” and were well-known at the time of invention. EX1030, 4, 14.

151. Therefore, in my opinion, *Waters* renders obvious claim 5.

v. Dependent Claim 6

152. In my opinion, *Waters* renders obvious “the state memory is configured to store in the alternative, an OFF state, a first ON state and a second ON state” for the same reasons discussed above in connection with limitation 1[d]. *See supra* §X.A.v.

vi. Dependent Claim 7

153. In my opinion, *Waters* renders obvious “the state memory is configured to store a first value indicating an ON/OFF state and a second value indicating one of at least two alternative ON states” for the same reasons discussed above in connection with limitation 1[d]. *See supra* §X.A.v.

vii. Dependent Claims 8, 13, 18, 25–26, 32, 55, 58

154. In my opinion, *Waters* discloses “the RFID tag is disposed within a cellular telephone.” SIM 15 (RFID tag) is incorporated in mobile terminal 1, which can be a handheld mobile telephone (cellular telephone). EX1024, [0020], [0034].

viii. Dependent Claims 9, 19, 27, 33, & 10, 28, 56, 59

155. In my opinion, *Waters* explains the tag/SIM structures may be “incorporated directly into the smart card or SIM 15 itself” and employed to make

payments (a financial card) or to obtain entry to a building (a keycard). *Id.*, Abstract, [0002], [0045], [0057].

ix. Dependent Claim 12

156. *Waters* renders obvious “the antenna is shared by several RFID tags.”

157. As discussed above with reference to limitation 11[h], *Waters* discloses that multiple near field tags may be incorporated in a single mobile terminal. *See supra* §X.B.ii. In view of this disclosure, in my opinion, a POSITA would have understood that *Waters*’s device, when implemented with multiple near field tags, would include a single antenna, which is shared by all near field tags of the device. This design would reduce space, component count, cost, and antenna coupling problems in a compact SIM or mobile terminal. Such a shared antenna would route received reader signals to a selected tag circuit and transmit the selected tag’s response via the same antenna.

158. Therefore, in my opinion, *Waters* renders obvious claim 12.

x. Dependent Claim 17

159. *Waters* discloses “the RFID tag is not remotely detectable using an RF signal when the ON/OFF state is OFF.” As discussed above with reference to limitation 1[d], near field tag 41 can enter a disabled state (OFF state). *See supra* §X.A.v. In that state, an RFID reader cannot obtain any information from near field tag 41, even when brought into close proximity, and thus near field tag 41 is not

remotely detectable. EX1024, [0037].

160. Therefore, in my opinion, *Waters* discloses claim 17.

xi. Dependent Claims 21, 30

161. In my opinion, *Waters* renders obvious “the input is further configured to receive power resulting from the first RF signal and to power the integrated circuitry using the power” for the same reasons discussed above in connection with limitations 1[a]–[b]. *See supra* §X.A.ii–iii.

xii. Dependent Claims 22, 31

162. In my opinion, *Waters* discloses “the integrated circuitry is configured for authorizing a transaction responsive to the mechanical switch” for the same reasons discussed above in connection with limitation 20[f]. *See supra* §X.D.iv.

xiii. Dependent Claim 23

163. In my opinion, *Waters* renders obvious “the mechanical switch must be activated and the state stored in the state memory must be an ON state before the second RF signal is transmitted” for the same reasons discussed above in connection with limitations 1[g] and 20[a]. *See supra* §§X.A.viii, X.D.ii.

xiv. Dependent Claim 24

164. In my opinion, *Waters* renders obvious “a key memory configured for storing a key for changing the state stored in the state memory, the switch logic being further configured to read the key from the key memory, to compare the received

data with the read key, and to change the state stored in the state memory responsive to the comparison between the received data with the read key” for the same reasons discussed above in connection with limitation 1[f]. *See supra* §X.A.vii.

xv. Dependent Claim 52

165. *Waters* renders obvious “the state memory is non-volatile memory” for the same reasons discussed above with reference to limitation 1[d] and claims 3 and 16. *See supra* §§X.A.v, X.K.ii. As discussed above, in my opinion, it would have been obvious to a POSITA to store the ON/OFF state of near field tag 41 as a value of a state variable. EX1026, 26, 47, 72–74. It is my opinion that it also would have been obvious to a POSITA that data memory (which stores variable values) would be implemented as non-volatile memory, such that the stored data can be retained after the device is powered off, as this was a well-known practice as of the time of invention. As *Pont* explains, “[i]n the power-down mode, the on-chip oscillator is stopped. Therefore all functions are stopped; only the contents of the on-chip RAM are maintained,” and “the values written to the port are held there until a new value is written or the device is reset.” *Id.*, 34, 47.

166. Therefore, in my opinion, *Waters* renders obvious claim 52.

XI. GROUND 1B: *WATERS* WITH *PONT* RENDERS OBVIOUS CLAIMS 1–33 AND 51–60

167. *Waters* with *Pont* renders obvious claims 1–33 and 51–60.

A. Motivation to Combine

168. Both *Waters* and *Pont* relate to mobile phone applications. *Waters* is directed to a mobile phone including components to control and carry out financial transactions using RFID communication. EX1024, [0020]. *Pont* is directed to software development for embedded devices, including mobile phone and smart card/SIM processors. EX1026, xi.

169. In particular, *Waters* uses SIM 15 and near field tag 41 to carry out its RFID functionality. EX1024, [0036]–[0037]. While *Waters* describes these features in functional terms, it lacks specific disclosure of how these features would be implemented at a software level. For example, *Waters* discloses that SIM 15 and near field tag 41 would interact with inputs and memory, but does not disclose *how* these components would read a switch input or *how* they would interact with memory to effectuate a desired output. *Pont* fills this gap by providing guidance on how to implement *Waters*’s operational states using conventional embedded controller state logic and state memory. Specifically, *Pont* teaches that “[m]uch of the activity in embedded systems involves reading pins (which may, for example, be connected to switches or keypads) and altering the value of other pins (which may, in turn, control anything...).” EX1026, 29, 192 (“system states will usually be represented by means of a switch statement in the operating system [interrupt service routine]”), 205 (“The system will operate in two or more states....Transitions

between states may be controlled by...system inputs or by a combination of time and inputs.”). Thus, in my opinion, a POSITA would turn to *Pont* for such knowledge, as *Pont* is a contemporary textbook which provides specific and relevant teachings related to programming techniques for embedded processors. *Id.*, xi. Such processors may include mobile phone processors, similar to the control components of SIM 15 and near field tag 41 of *Waters*. *Id.* In my opinion, *Pont* therefore provides useful guidance to a POSITA related to specific methods of programming a microprocessor to carry out mobile phone applications.

170. *Pont* discloses that a controller can interface with a switch, and change a device state based on the value of the switch, similar to the functionality described in *Waters*. EX1026, 71–74; EX1024, [0053]. As shown below, *Pont* teaches that to enable such functionality, a switch may be polled. EX1026, 72. On each iteration of the polling loop, the current value of the switch can be checked, and assigned to a switch state variable. *Id.* (storing the value of SWITCH_Get_Input() in the Sw_state variable). Then, the value of the switch state variable can be passed into a controller function, to perform logic based on the switch state. *Id.* (passing Sw_state into DISPLAY_SWITCH_STATUS_Update()). In the example provided by *Pont*, the controller changes the value of an output state variable, depending on the value of the switch state, to control the state of an LED based on a switch. *Id.*, 74 (assigning different values to the Output_port variable depending on the value of the Sw_state

variable).

```
/*-----*/
Switch_read.C (v1.00)
-----*/

A simple 'switch input' program for the 8051.
- Reads (and debounces) switch input on Pin1^0
- If switch is pressed, changes Port 3 output
/*-----*/

#include <Reg52.h>
// Connect switch to this pin
sbit Switch_pin = P1^0;
// Display switch status on this port
#define Output_port P3
```

Logic based on
input state variable

Assigning input state variable

Polling input pin

```
// Return values from Switch_Get_Input()
#define SWITCH_NOT_PRESSED (bit) 0
#define SWITCH_PRESSED (bit) 1

// Function prototypes
void SWITCH_Init(void);
bit SWITCH_Get_Input(const unsigned char DEBOUNCE_PERIOD);
void DISPLAY_SWITCH_STATUS_Init(void);
void DISPLAY_SWITCH_STATUS_Update(const bit);
void DELAY_LOOP_Wait(const unsigned int DELAY_MS);

/*-----*/
void main(void)
{
    bit Sw_state;

    // Init functions
    SWITCH_Init();
    DISPLAY_SWITCH_STATUS_Init();

    while(1)
    {
        Sw_state = SWITCH_Get_Input(30);
        DISPLAY_SWITCH_STATUS_Update(Sw_state);
    }
}

/*-----*/
SWITCH_Init()
    Initialisation function for the switch library.

/*-----*/
void SWITCH_Init(void)
{
    Switch_pin = 1; // Use this pin for input
}

/*-----*/
SWITCH_Get_Input()
    Reads and debounces a mechanical switch as follows:
```

```
1. If switch is not pressed, return SWITCH_NOT_PRESSED.
2. If switch is pressed, wait for DEBOUNCE_PERIOD (in ms),
   then:
   a. If switch is still pressed, return SWITCH_PRESSED.
   b. If switch is not pressed, return SWITCH_NOT_PRESSED.

See Switch_Wait.H for details of return values.

/*-----*/
bit SWITCH_Get_Input(const unsigned char DEBOUNCE_PERIOD)
{
    bit Return_value = SWITCH_NOT_PRESSED;

    if (Switch_pin == 0)
    {
        // Switch is pressed

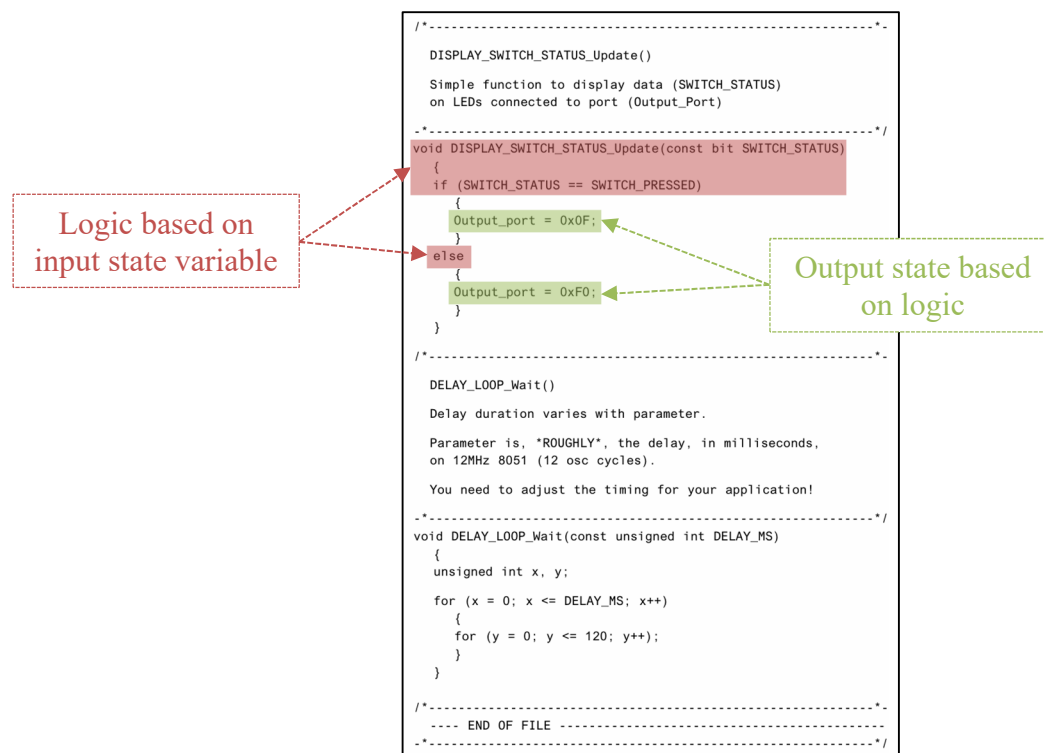
        // Debounce - just wait...
        DELAY_LOOP_Wait(DEBOUNCE_PERIOD);

        // Check switch again
        if (Switch_pin == 0)
        {
            Return_value = SWITCH_PRESSED;
        }
    }

    // Now return switch value
    return Return_value;
}

/*-----*/
DISPLAY_SWITCH_STATUS_Init()
    Initialization function for the DISPLAY_SWITCH_STATUS library.

/*-----*/
void DISPLAY_SWITCH_STATUS_Init(void)
{
    Output_port = 0xF0;
}
```



EX1026, 71–74.

171. *Pont* additionally teaches that the value of the output state variable is stored in RAM. EX1026, 26 (variables are stored in memory), 192–198 (showing that the “state of the system” would be stored in a memory variable (Light_state_G) that tracks the system’s presently selected state, while the switch statement code implements logic that reads the state and controls the device operation accordingly). Thus, RAM can correspond to a state memory, because it stores data indicating the current state of the device.

172. Based on these teachings, it is my opinion that a POSITA would have been motivated to apply *Pont*’s control structure to *Waters*, such that an output state variable stores the active state of the RFID functionality. For example, according to

Pont's teachings, a POSITA would understand that in *Waters*, a polling loop would be used to check the current value of a mechanical switch. On each iteration of the polling loop, the switch value would be assigned to a switch state variable. Then, the value of the switch state variable would be passed to a controller function. The controller function would then apply logic to ascertain the current state of the RFID transaction functionality, as taught by *Waters*. The function would assign this state to an RFID state variable and use the value of this variable to control the downstream operations of the device. As taught by *Pont*, the implementation of such logic would require that the RFID state is stored in RAM, which can correspond to a state memory.

173. Moreover, it is my opinion that a POSITA would have had a reasonable expectation of success in making this combination. For example, *Pont* discloses that its teachings are directly applicable to embedded processors in mobile phones, as well as low-cost and low-power devices (similar to smart cards). EX1026, xi, 2–5, 33. The *Waters-Pont* combination therefore entails nothing more than applying known elements (software controllers) in a known structure (mobile phones) using known methods (programming in C) to achieve a well-understood and predictable benefit (reliable control of mobile phone processes). In my opinion, a POSITA would reasonably expect this combination to succeed without undue experimentation, as it relies on well-established programming techniques and

produces understood results.

B. “State Memory” Claims: 1, 4, 6–7, 11, 14, 20, 23–24, 29, 51–54, 57, 60

174. *Waters-Pont* renders obvious a “state memory,” as recited in claims 1, 4, 6–7, 11, 14, 20, 23–24, 29, 51–54, 57, and 60.

175. As discussed above, in my opinion, based on *Pont*’s teachings, a POSITA would have understood that the device of *Waters* would include memory, which would store information reflecting the current state of the device. *See supra* §XI.A. The device memory (state memory) would store the current value of a device state variable (jamming (first ON state), transaction (second ON state), or deactivated (OFF state)). *Id.*; *see also supra* §X.A.v.

176. Except for the implementation of the state memory described above, *Waters-Pont* is identical to *Waters*. Therefore, the remaining limitations of claims 1, 4, 6–7, 11, 14, 20, 23–24, 29, 51–54, 57, and 60 are disclosed and/or rendered obvious by *Waters-Pont* for the same reasons discussed above, with respect to *Waters*. *See supra* §X.

177. Therefore, in my opinion, *Waters-Pont* renders obvious the “state memory” limitation of claims 1, 4, 6–7, 11, 14, 20, 23–24, 29, 51–54, 57, and 60.

C. Claims 2–3, 5, 8–10, 12–13, 15–19, 21–22, 25–28, 30–33, 55–56, 58–59

178. As discussed above, except for the implementation of the state memory described above, *Waters-Pont* is identical to *Waters*. Therefore, in my opinion,

claims 2–3, 5, 8–10, 12–13, 15–19, 21–22, 25–28, 30–33, 55–56, and 58–59 are disclosed and/or rendered obvious by *Waters-Pont* for the same reasons discussed above, with respect to *Waters*. See *supra* §X.

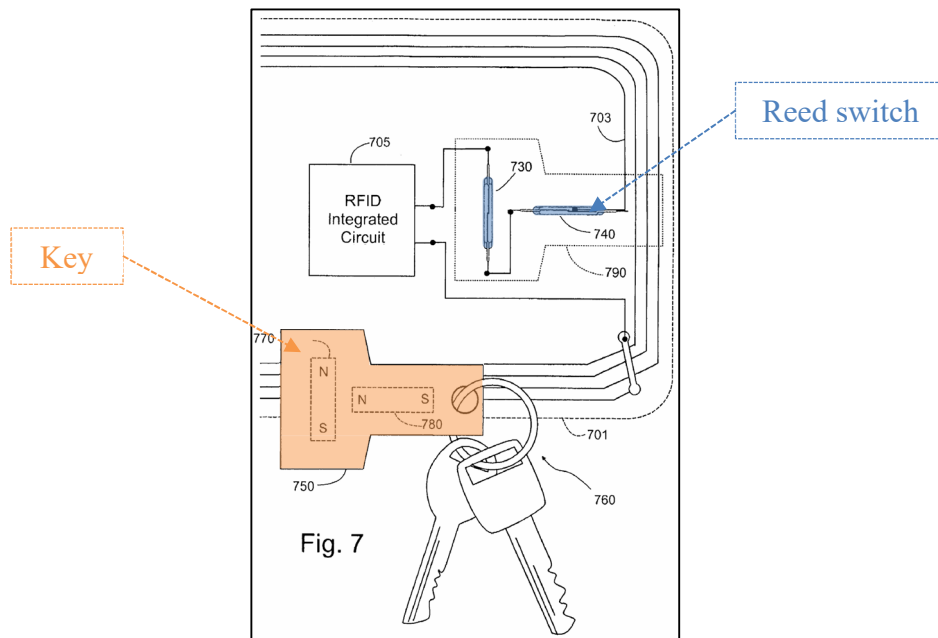
XII. GROUND 1C: *WATERS* WITH *SELKER* RENDERS OBVIOUS CLAIMS 39–43

179. *Waters* with *Selker* renders obvious claims 39–43.

A. Motivation to Combine

180. Both *Waters* and *Selker* relate to RFID payment technologies. *Waters* is directed to a mobile phone including components to control and carry out financial transactions using RFID communication; *Waters* discloses that “the mobile terminal 1 includes a near field or RFID tag 41,” and that “mobile terminal 1 may be a handheld mobile telephone.” EX1024, [0034], [0043]. *Selker* is directed to a mechanism for protecting RFID payment cards from unauthorized misuse. EX1027, [0004] (“[t]he present invention helps protect a contactless information storage device, such as an RFID payment card, from unauthorized misuse”). Similar to *Waters*, and as further discussed below, *Selker* relates to a manually operated mechanical switch that enables and disables RFID transmission, a passive RFID circuit powered through an antenna, automatic deactivation after the user releases the switch, a mechanical/fluid timing mechanism, and multiple switches selectively connecting portions of the antenna. EX1027, [0004]–[0009].

181. As discussed above, *Waters* discloses a pressure sensor (mechanical switch), which enables and disables RFID communication to enhance data security in RFID applications. EX1024, [0050], [0053]. According to *Waters*, this pressure sensor can prevent skimming. *Id.* *Selker* likewise addresses the issue that “because RF-enabled devices such [as] payment cards can be read at a distance with a suitable transmitter and receiver, it is possible to surreptitiously obtain information from the card while it remains in its cardholder’s possession. In addition to non-contact data transfer, wireless communication can also allow non-line-of-sight communication, meaning that an RF-enabled device may be read while it remains in the cardholder’s wallet or purse.” EX1027, [0003]. Therefore, *Selker* teaches that security can be further improved by implementing a reed switch and key mechanism, which is “functionally flexible in order to work in cards and other devices having a variety of shapes and sizes.” *Id.*, [0004], [0027], [0031], FIG. 7. *Selker* discloses that the switch should be normally open, to prevent unauthorized skimming when the device is not in use. *Id.*, [0004], [0006]. According to *Selker*, this mechanism provides “enhanced security” and “helps protect” the RFID device “from unauthorized misuse.” *Id.*, [0004], [0019].



Id., FIG. 7.

182. It is my opinion that based on these teachings, a POSITA would have been motivated to implement *Selker*'s reed switch and key mechanism in the device of *Waters* to achieve improved device security as taught in *Selker*. *Id.*, [0004], [0027], [0031], FIG. 7. To do so, a POSITA would have replaced *Waters*'s pressure sensor (mechanical switch) with a set of two perpendicular reed switches, as taught by *Selker*, to securely authenticate a user in possession of a key. *Id.*, FIG. 7 (reproduced above), [0031]. As *Selker* teaches, "different keys, or different placements of a single key[] may be used to selectively close only certain on-card switches to provide the needed connections." *Id.*, [0031]. As discussed above, the jamming functionality of *Waters*'s device is disabled when "authorized use" is required. EX1024, [0055]; see *supra* §X.A.v. Therefore, a POSITA would

implement the *Waters-Selker* device such that the near field tag 41 transitions from the jamming state (first ON state) to a transaction state (second ON state), when the magnetic key is placed in close proximity to the set of reed switches. As taught by *Waters*, near field tag 41 may later automatically enter a deactivated state (OFF state), in which RFID communication is disabled, after it has been read by an RFID reader. EX1024, [0052], [0057].

183. Moreover, in my opinion, a POSITA would have had a reasonable expectation of success in making this combination. For example, *Waters* discloses similar security measures. EX1024, [0050], [0053] (discussing pressure sensors to prevent skimming). Meanwhile, *Selker* provides an alternative reed switch and key mechanism, which provides further enhanced security. EX1027, [0003]–[0004], [0019]. The *Waters-Selker* combination therefore entails nothing more than applying known elements (a reed switch and key mechanism) in a known structure (mobile phones) using known methods (basic circuit design) to achieve a well-understood and predictable benefit (improved device security). In my opinion, a POSITA would reasonably expect this combination to succeed without undue experimentation, as it relies on well-established circuit design techniques and produces understood results.

B. Independent Claim 39

i. 39[pre]

184. Except for the implementation of the reed switch and key mechanism

described above, *Waters-Selker* is identical to *Waters*. Therefore, in my opinion, limitation 39[pre] is rendered obvious by *Waters-Selker* for the same reasons discussed above, with respect to *Waters*. *See supra* §X.

ii. 39[a]

185. *Waters-Selker* renders obvious a “mechanical switch responsive to a state of a mechanical security device.”

186. In my opinion, as discussed above, based on *Selker*’s teachings, a POSITA would have replaced the pressure sensor of *Waters* with a set of two perpendicular reed switches (mechanical switch), as taught by *Selker*, to achieve enhanced security. *See supra* §XII.A. As further taught by *Selker*, the set of reed switches (mechanical switch) is normally open. EX1027, [0027], FIG. 7. When a magnetic key (mechanical security device) is brought in close proximity to the set of reed switches (mechanical switch), the circuit is closed, and the key-holding user is thereby authenticated. *See supra* §XII.A; EX1027, [0027]. Therefore, in *Waters-Selker*, the set of reed switches (mechanical switch) is responsive to the magnetic key (mechanical security device). *Id.*

187. Therefore, in my opinion, *Waters-Selker* renders obvious limitation 39[a].

iii. 39[b]–[f]

188. Except for the implementation of the reed switch and key mechanism

described above, *Waters-Selker* is identical to *Waters*. Therefore, in my opinion, limitations 39[b]–[f] are rendered obvious by *Waters-Selker* for the same reasons discussed above, with respect to *Waters*. *See supra* §§X.A.ii–v, X.D.iv.

C. Dependent Claims

i. Dependent Claim 40

189. In my opinion, *Waters-Selker* discloses “the integrated circuitry is configured for authorizing a transaction responsive to the mechanical switch” for the same reasons discussed above in connection with limitation 20[f]. *See supra* §X.D.iv.

ii. Dependent Claim 41

190. In my opinion, *Waters-Selker* discloses “the RFID tag is disposed within a cellular telephone” for the same reasons discussed above in connection with claims 8, 13, 18, 25–26, 32, 55, and 58. *See supra* §X.K.vii.

iii. Dependent Claim 42

191. In my opinion, *Waters-Selker* discloses “the RFID tag is disposed within passport, identity card, driver's license, immigration document, student identity card, library card, financial card, social security card, military ID card, key, keycard, or identification document” for the same reasons discussed above in connection with claims 9, 19, 27, and 33. *See supra* §X.K.viii.

iv. Dependent Claim 43

192. In my opinion, *Waters-Selker* discloses “the RFID tag is disposed within a passport, driver’s license, financial card, military ID card, key, or keycard” for the same reasons discussed above in connection with claims 9, 19, 27, and 33. *See supra* §X.K.viii.

XIII. GROUND 2A: DUA RENDERS OBVIOUS CLAIMS 1–10, 14–38 AND 44–59

193. *Dua* renders obvious claims 1–10, 14–38, and 44–59.

A. Independent Claim 1

i. 1[pre]

194. *Dua* discloses “a RFID tag.”

195. As discussed above with reference to Ground 1A, the ’156 Patent uses the term “RFID tag” to encompass a Radio Frequency Identification Device, which includes a “tag” that facilitates RFID communication. *See supra* §X.A.i.

196. Similarly, *Dua*’s wireless device is equipped with hardware and software that enables RFID communication (RFID tag) to transmit credentials and facilitate a transaction. EX1023, [0378], [0383], [0423], [0495].

197. Therefore, in my opinion, *Dua* discloses limitation 1[pre].

ii. 1[a]

198. *Dua* renders obvious “an antenna configured to receive data in a first RF signal, to receive energy from the first RF signal, and to transmit data in a second

RF signal, the transmission of the second RF signal being powered by the energy received from the first RF signal.”

199. *Dua* explains its techniques relate to smart card technology, including a “contactless smart card.” EX1023, [0009]. *Dua* discloses that “[b]oth the reader and the card have antennas and it is via this contactless link that the two communicate via radio frequency (RF) when in close proximity.” *Id.* In my opinion, a POSITA would understand *Dua*’s “communicat[ion] via radio frequency” to be two-way RFID communication between the reader and the card, in which the card both receives and transmits data via RFID signals. Therefore, *Dua* discloses an antenna that receives data in a first RF signal (from the reader), and transmits data in a second RF signal (to the reader).

200. *Dua* further states that such devices “typically receive power for on-card electronic functions via [the] electromagnetic signal [received from the reader].” *Id.* Therefore, *Dua* discloses that the card antenna is configured to receive energy from the first RF signal (from the reader), and that the transmission of a second RF signal (to the reader) is powered by the energy received from the first RF signal.

201. In my opinion, to the extent *Dua*’s express disclosure is insufficient, an RFID antenna configured to receive and transmit data necessarily flows or is a natural result of *Dua*’s RFID communication functionality, which cannot be

implemented without such an antenna. *See, e.g.*, EX1023, [0009]; EX1029, 41. Moreover, it would have been further obvious to a POSITA that, similar to the well-known smart card devices described by *Dua* (discussed above), *Dua*'s wireless device could be "passive," such that energy is also received by the antenna from the signal emitted by the RFID reader (first RF signal) and used to power transmission of the payment credentials (second RF signal), as such technology was well-known as of the time of invention. As *Dua* states, "[m]ost contactless cards typically receive power for on-card electronic functions via [the] electromagnetic signal [received from the reader]." EX1023, [0009].

202. Therefore, in my opinion, *Dua* renders obvious limitation 1[a].

iii. 1[b]

203. *Dua* renders obvious "integrated circuitry including an input configured to receive data from the antenna and to receive power resulting from the energy received from the antenna."

204. *Dua* discloses that similar RFID-enabled communication devices utilize embedded "integrated circuits" to implement their functionality. EX1023, [0007]. *Dua* also discloses that its device includes an RFID interface, which enables RFID communication. *Id.*, [0309], [0378], [0383], [0495]. In my opinion, an input to receive input data and power from the antenna and an output to provide output data to the antenna, necessarily flows or is a natural result of *Dua*'s disclosure of

RFID communication enabled by an embedded RFID interface and related integrated circuitry. The antenna must be electrically coupled to the integrated circuitry through an input/interface that conveys the received data and power, because without such an input, the integrated circuitry could neither process the RFID signals received from the reader nor operate using the received RF energy.

205. Further, as discussed above, *Dua* discloses that its wireless device receives data and power from an RFID reader. *See supra* §XIII.A.ii. Therefore, in my opinion, an input to receive data and energy from the RFID antenna, such that the data and power can be transmitted from the antenna to the RFID circuitry of the wireless device, necessarily flows or is a natural result of such functionality, which cannot be implemented without an input.

206. It is also my opinion that it would have been further obvious to a POSITA that the functionality discussed above would be implemented as integrated circuitry. For example, a POSITA would understand that at the time of invention, integrated circuits were commonly used in mobile phone and RFID applications to provide communications and control functionality, with increased efficiency and decreased cost, compared to other methods. *See* EX1029, 292–293; EX1026, 4.

207. Therefore, in my opinion, *Dua* renders obvious limitation 1[b].

iv. 1[c]

208. *Dua* renders obvious “integrated circuitry including...an output

configured to provide the second RF signal to the antenna for transmission.”

209. In my opinion, as discussed above, integrated circuitry including an output to provide output data to the antenna necessarily flows or is a natural result of *Dua*’s RFID interface and disclosed RFID communication functionality. See *supra* §XIII.A.iii. For example, *Dua* describes that its device “communicates” with a reader, which requires signal transmission via an output. EX1023, [0009] (“Both the reader and the card have antennas and it is via this contactless link that the two communicate via radio frequency (RF) when in close proximity”), [0353]–[0354] (describing transmission of information to a reader). This functionality cannot be implemented without such an output.

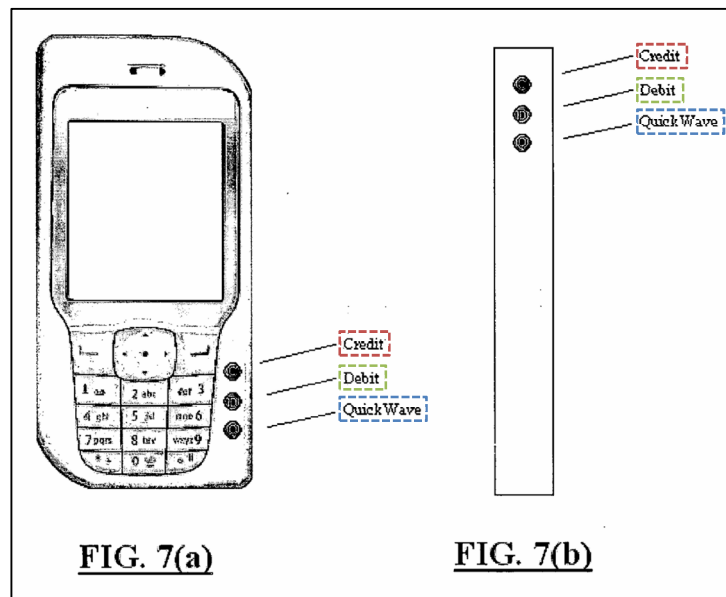
210. Further, *Dua*’s device transmits data, including payment credentials (second RF signal) to an RFID reader through an RFID interface. *Dua* discloses that “[w]hen the wireless device is placed in proximity to the reader, the selected credential(s) are automatically transmitted by the RFID chip in the wireless device to the reader.” EX1023, [0309], [0378], [0383], [0423]. It would have been obvious to a POSITA that such functionality requires an output to provide the payment credential data (second RF signal) to the antenna, such that the data can be transmitted to the RFID reader by the antenna.

211. Therefore, in my opinion, *Dua* renders obvious limitation 1[c].

v. 1[d]

212. *Dua* renders obvious “integrated circuitry including...a state memory configured to store an ON/OFF state including two or more ON states of the RFID tag.”

213. *Dua* discloses a system architecture including at least three states (an OFF state and multiple ON states). By default, *Dua*’s wireless device is in a deactivated state (OFF state), in which no credentials will be transmitted to an RFID reader. EX1023, [0383], [0395]. *Dua* discloses that “the existence of a button in an RFID-enabled wireless device that controls activation of the wallet application and transmission of credentials via RF could eliminate a similar fraud risk,” and that “[p]ressing buttons 1 or 2, may prompt the user to input a PIN before RF communication can be enabled.” *Id.*, [0383], [0395]. *Dua*’s wireless device may transition from the deactivated state (OFF state) to one of several transaction states (ON states), in which payment credentials are transmitted to an RFID reader, when a “hot button” associated with a particular transaction state is pressed by a user. These hot buttons include (1) a “QuickWave” hot button, which activates a QuickWave state (first ON state), (2) a “Credit” hot button, which activates a credit card state (second ON state), and (3) a “Debit/ATM” hot button, which activates a debit card state (third ON state). *Id.*, [0388]–[0395], FIG. 7.



EX1023, FIG. 7.

214. In the QuickWave state (first ON state), the wireless device can transmit credentials that have a reader key associated with them. EX1023, [0392]; *see infra* §XIII.A.vi (discussing QuickWave and reader key functionality in detail). In the credit card state (second ON state), the wireless device can transmit the QuickWave credentials, plus credit card credentials. *Id.*, [0392]–[0393]. In the debit card state (third ON state), the wireless device can transmit the QuickWave credentials, plus debit card credentials. *Id.* Each of these states corresponds to a unique ON state, because the wireless device will transmit different data through RFID communication, depending on the transmission type.

215. Thus, *Dua* discloses a deactivated state (OFF state), in which RF communication is disabled and the wallet application is dormant, a QuickWave state

(first ON state), in which RF communication is enabled to transmit a selected QuickWave credential, a credit card state (second ON state), in which RF communication is enabled to transmit a credit card credential, and a debit card state (third ON state), in which RF communication is enabled to transmit a debit card credential.

216. Further, *Dua*'s wireless device includes memory, and in my opinion, it would have been obvious to a POSITA to store the current state (deactivated, QuickWave, credit card, or debit card) of the wireless device in this memory (state memory), to enable implementation of the logic described above (transitioning from the deactivated state to a QuickWave state, credit card state, or debit card state, depending on which hot button was pressed by the user). EX1023, [0193]. For example, *Dua* discloses that its device incorporates processing and secure storage capabilities, stored credential/profile selections, and software controlling the RF interface. Specifically, the wireless device includes a software-based "wallet application," which controls the wireless device to carry out the described storage and logical processing functionality. EX1023, [0333], [0354]. As discussed above with reference to Ground 1A, it would have been obvious to a POSITA to store the current state as a variable in memory (state memory), such that the wallet application can interact with the RFID circuitry to carry out the functionality described above. *See supra* §X.

217. Therefore, in my opinion, *Dua* renders obvious limitation 1[d].

vi. 1[e]

218. *Dua* discloses “integrated circuitry including...a key memory configured for storing a key for changing the ON/OFF state stored in the state memory.”

219. *Dua*’s wireless device can store reader keys (keys) in memory (key memory) to associate particular credentials with certain readers. A reader key is transmitted by a credential issuer to the wireless device, to be linked with a credential that is associated with the reader key. For example, *Dua* discloses that “[t]he key is sent with an electronic credential record to a wireless device during the issuance process.” EX1023, [0353]; [0365]. The key is then stored in the wireless device’s memory (key memory), as “[t]he wallet application stores the ‘reader key’ with the electronic credential to which it is linked.” *Id.*, [0354]. All RFID readers associated with the issuer also store a corresponding key, because “[t]he same reader key is programmed in all reader devices employed by an organization.” *Id.*, [0353]. At the start of a transaction, an RFID reader associated with the issuer transmits its key to the wireless device, as “the key is transmitted from the reader to the wireless device’s RFID chip during a proximity transaction.” *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 (key), which was received and stored during the

issuance process. As *Dua* explains, “[t]he 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,” and “[i]f 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.” *Id.*, [0353], [0354]. Then, the wallet application completes a transaction using the selected credential. *Id.* Such functionality “allows a reader device to automatically capture certain credential information from a wireless device without the end-user having to scroll through different screens within the wallet application and pressing multiple buttons on his device.” *Id.*, [0355]. Therefore, the reader key (key), which is stored in memory (key memory) is used to transition from a deactivated state (OFF state) to a QuickWave state (first ON state), credit card state (second ON state), or debit card state (third ON state), depending on which credential (QuickWave, credit, or debit) is associated with a particular reader key (key). In my opinion, as discussed above with reference to limitation 1[d], it would have been obvious to a POSITA to store the current state in state memory. *See supra* §XIII.A.v.

220. Therefore, in my opinion, *Dua* discloses limitation 1[e].

vii. 1[f]

221. *Dua* renders obvious “integrated circuitry including...a switch logic configured to receive data from the input, to read the key from the key memory, to

compare the received data with the read key, and to change the ON/OFF state stored in the state memory responsive to this comparison.”

222. As discussed above with reference to limitation 1[e], *Dua* discloses logic to receive a key (data) from an RFID reader through RFID communication (from the input), read a reader key (key) from memory (key memory), and compare the key (data) with the reader key (key), to determine a transition from a deactivated state (OFF state) to a QuickWave state (first ON state), credit card state (second ON state), or debit card state (third ON state). *See supra* §XIII.A.vi.

223. In my opinion, as further discussed above with reference to limitation 1[d], it would have been obvious to a POSITA to store the current state in state memory. *See supra* §XIII.A.v.

224. Therefore, in my opinion, *Dua* renders obvious limitation 1[f].

viii. 1[g]

225. *Dua* renders obvious “the switch logic being further configured to determine whether or not to provide the second RF signal to the antenna for transmission, the determination being responsive to the ON/OFF state stored in the state memory.”

226. As discussed above with reference to limitation 1[d], *Dua* discloses logic to determine whether to provide payment credentials (second RF signal) to the antenna for transmission, based on the current state (QuickWave, credit, debit, or

deactivated) stored in state memory. *See supra* §XIII.A.v.

227. Therefore, in my opinion, *Dua* renders obvious limitation 1[g].

B. Independent Claim 14

i. 14[pre]–[c]

228. In my opinion, *Dua* discloses and/or renders obvious limitations 14[pre]–[c] for the same reasons discussed above in connection with limitations 1[pre]–[c]. *See supra* §XIII.A.i–iv.

ii. 14[d]

229. *Dua* renders obvious “integrated circuitry including...a state memory configured to store an ON/OFF state of the RFID tag, the ON/OFF state being responsive to timing using a resistor-capacitor circuit.”

230. When a hot button is pressed, the wireless device transitions from a deactivated state (OFF state) to a QuickWave state (first ON state), credit state (second ON state), or debit state (third ON state) for a 30-second period. EX1023, [0395]. Once this 30-second period has elapsed, the device returns to the deactivated state (OFF state). *Id.*; *see also id.*, [0383]. In my opinion, as discussed above with reference to Ground 1, it would have been obvious to a POSITA that this timing functionality could be implemented using a resistor-capacitor (“RC”) circuit, as it was well known in the art to build timers using RC circuits. *See, e.g.*, EX1028, 10-1 (“RC networks are probably the most commonly used delay networks”); EX1029,

276–78 (discussing use of RC timers in RFID applications). A POSITA implementing such predetermined-time deactivation functionality would have recognized a resistor-capacitor timing circuit as a conventional, inexpensive, and predictable circuit for defining the duration of the temporary ON state.

231. Therefore, in my opinion, *Dua* renders obvious limitation 14[d].

iii. 14[e]–[g]

232. In my opinion, *Dua* discloses and/or renders obvious limitations 14[e]–[g] for the same reasons discussed above in connection with limitations 1[e]–[g]. *See supra* §XIII.A.vi–viii.

C. Independent Claim 20

i. 20[pre]

233. In my opinion, *Dua* discloses limitation 20[pre] for the same reasons discussed above in connection with limitation 1[pre]. *See supra* §XIII.A.i.

ii. 20[a]

234. *Dua* discloses “a mechanical switch configured for selecting between two or more ON states of the RFID tag.”

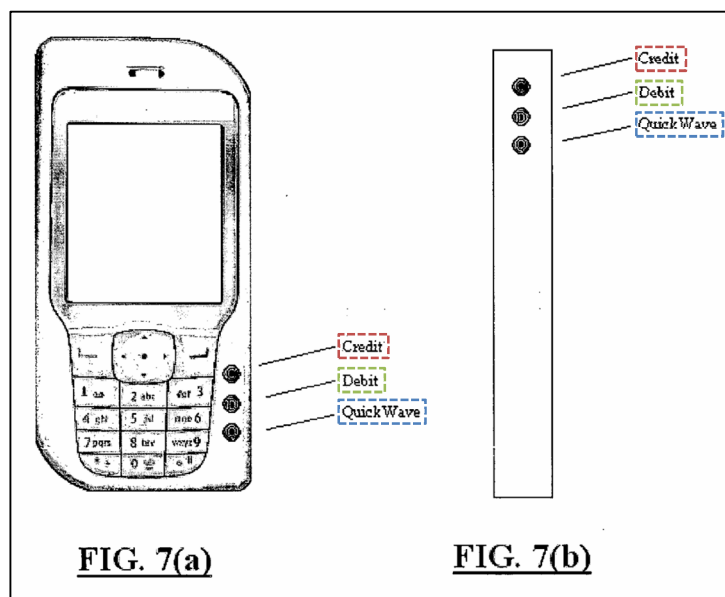
235. As discussed above with reference to limitation 1[d], the wireless device includes three hot buttons (one or more mechanical switches). *See supra* §XIII.A.v. The hot buttons are physical, user-operated buttons located on the wireless device. EX1023, [0393] (the buttons are “press[ed]” by a user), [0396]

(“The wallet application-specific buttons as described above can be any size, shape, or color on the front of the mobile device, on the back of the device, or on any side of the device”), FIG. 7. Each hot button allows a user to select between several ON states by pressing and activating the hot button. Therefore, each hot button discloses a mechanical switch because it controls circuit components by making or breaking an electrical connection in the device circuitry, responsive to its components being pressed (moved) by a user. *See supra* §VII (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.”). *Dua*’s hot buttons are similar to the pressure-sensitive mechanical switch described in the ’156 Patent specification. EX1001, 8:19–23 (“In some embodiments, Switch 170 is a mechanical contact switch activated by applying pressure to an outside surface of Switchable RFID Device 100. In some embodiments, when this pressure is applied the functionality of Tag 160 will be turned on, and when this pressure is not applied the functionality of Tag 160 will be off.”); *see also* §VII (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.”).

236. According to *Dua*, a “QuickWave” hot button selects a QuickWave state (first ON state), a “Credit” hot button selects a credit card state (second ON

state), and a “Debit/ATM” hot button selects a debit card state (third ON state).

EX1023, [0388]–[0395], FIG. 7.



EX1023, FIG. 7.

237. When a hot button is pressed, communication of QuickWave, credit, or debit credentials is enabled for a 30-second period, based on which button was pressed. *Id.*, [0395], *see also* [0393] (the credit and debit buttons can also be programmed to enable transmission of both a credit/debit credential and a QuickWave credential when near a reader with a “reader key”). Therefore, in my opinion, a POSITA would have understood that in the scenario where a first hot button is pressed (and an ON state is activated for 30 seconds), and then a second hot button is pressed within the 30-second window, the second hot button will cause a transition from one ON state to a different ON state, thus selecting between the

two ON states. For example, if a user first presses the “QuickWave” button, and then 15 seconds later, presses the “Credit” button (mechanical switch), the device will select the credit card state (second ON state) from between the credit card state and the QuickWave state. *Id.*; compare EX1001, 21:41–49. In this scenario, after the “QuickWave” button is pressed, the device will transmit only QuickWave credentials if the “Credit” button is not pressed, but will transmit both QuickWave and credit card credentials if the “Credit” button is pressed. EX1023, [0393] (“Pressing [the ‘Credit’ or ‘Debit’ buttons] could in addition to transmitting a payment method, also transfer a PIN-less [i.e., QuickWave] credential”). This functionality is similar to that described with reference to the enabling embodiment of the ’156 Patent, in which “Tag 160 will transmit a limited amount of data when Switch 170 is off and a less limited amount of data when Switch 170 is on. For example, Tag 160 may be configured to respond with data indicating the name of a person when switch 170 is off and to respond with the data including the name, an address, and account number and a telephone number when Switch 170 is on.” EX1001, 9:6–11.

238. Alternatively, *Dua* explains that its hot buttons can be implemented in a variety of ways, with flexibility in their appearance and functionality. EX1023, [0396] (“The wallet application-specific buttons as described above can be any size, shape, or color on the front of the mobile device, on the back of the device, or on

any side of the device. (The front of the device is typically the side with the display and keypad.) The button or buttons may also have iconic or text representations either on them or next to them in order to signal their function. In cases where there are multiple buttons associated with the wallet application, the buttons may appear on the device close together or be in different parts of the device.”). Therefore, in my opinion, a POSITA would have considered it an obvious design choice to implement *Dua*’s three wallet buttons as a single, three-way selector switch, having a first position for “QuickWave” functionality, a second position for “Credit” functionality, and a third position for “Debit” functionality. This implementation would preserve the functionality of *Dua*’s device, while reducing the number of components and complexity of its design.

239. Therefore, in my opinion, *Dua* discloses limitation 20[a].

iii. 20[b]–[e]

240. In my opinion, *Dua* discloses and/or renders obvious limitations 20[b]–[e] for the same reasons discussed above in connection with limitations 1[a]–[d]. *See supra* §XIII.A.ii–v.

iv. 20[f]

241. *Dua* renders obvious “integrated circuitry including...a switch logic configured to receive data from the input, and to determine whether or not to provide the second RF signal to the antenna for transmission, the determination being

responsive to the state stored in the state memory or the mechanical switch.”

242. As discussed above with reference to limitation 1[b], the wireless device receives data from an input. *See supra* §XIII.A.iii; EX1023, [0309] (“The wallet application handles processing of incoming credentials and extensions...[and] enabling communication with an embedded RF interface or smart card”).

243. As discussed above with reference to limitation 20[a], the wireless device determines whether to provide payment credentials (second RF signal) to the antenna for transmission, based on whether a hot button (mechanical switch) was pressed. *See supra* §XIII.C.ii. In the alternative, as discussed above with respect to limitation 1[g], such determination can be based on the state stored in state memory. *See supra* §XIII.A.viii.

244. Therefore, in my opinion, *Dua* renders obvious limitation 20[f].

D. Independent Claim 29

i. 29[pre]

245. In my opinion, *Dua* discloses limitation 29[pre] for the same reasons discussed above in connection with limitation 1[pre]. *See supra* §XIII.A.i.

ii. 29[a]

246. *Dua* discloses “a mechanical switch configured to set a state of the RFID tag stored in a state memory.”

247. As discussed above with reference to limitation 20[a], *Dua* discloses hot buttons (mechanical switches) configured to select between a QuickWave state (first ON state), credit card state (second ON state), and a debit card state (third ON state). *See supra* §XIII.C.ii. As further discussed above, the current state (set by the mechanical switch) is stored within memory (state memory). *See supra* §XIII.A.v.

248. Therefore, in my opinion, *Dua* discloses limitation 29[a].

iii. 29[b]–[f]

249. In my opinion, as discussed above with reference to claim 1, *Dua* discloses and/or renders obvious limitations 29[b]–[e]. *See supra* §XIII.A.ii–v. As further discussed above with reference to claim 20, *Dua* renders obvious limitation 29[f]. *See supra* §XIII.C.iv.

E. Independent Claim 34

i. 34[pre]

250. As discussed above with reference to limitation 1[pre], in my opinion, *Dua* discloses limitation 34[pre]. *See supra* §XIII.A.i.

ii. 34[a]

251. As discussed above with reference to limitation 20[a], in my opinion, *Dua* discloses limitation 34[a]. *See supra* §XIII.C.ii.

iii. 34[b]–[e]

252. As discussed above with reference to limitations 1[a]–[d], in my

opinion, *Dua* discloses limitations 34[b]–[e]. *See supra* §XIII.A.ii–v.

iv. 34[f]

253. As discussed above with reference to limitation 20[f], in my opinion, *Dua* discloses limitation 34[f]. *See supra* §XIII.C.iv.

v. 34[g]

254. *Dua* renders obvious “the state logic being further configured to store a plurality of alternative ON states.”

255. I note “the state logic” is not introduced or defined elsewhere in Claim 34. However, this appears to be a typographical error, as throughout the ’156 Patent claims and specification, the state *memory* is described as storing a device state. Additionally, in my opinion, a POSITA would not consider “logic” to be capable of storing a device state. To the extent that the Board may consider this to be a typographical error, and interpret “state logic” as referring to “state memory,” it is my opinion that it would have been obvious to a POSITA to store a QuickWave state (first ON state), a credit card state (second ON state), and a debit card state (third ON state) in the wireless device memory (state memory), as discussed above with reference to limitation 1[d]. *See supra* §XIII.A.v. In addition to the examples discussed above, *Dua*’s wallet application allows a user to “create and store different profiles in advance,” with each stored profile linked to one or more credential. EX1023, [0380]. When a particular profile is selected, the device automatically

transmits the credential(s) linked to that profile. *Id.* *Dua* also discloses stored mappings between different physical buttons and transmission of respective credit, debit/ATM, and QuickWave credentials. *Id.*, [0392]–[0394]. In my opinion, a POSITA would understand each stored profile, credential selection, or button mapping to define an alternative ON state, because each configuration causes the enabled RFID interface to transmit different response data.

256. Therefore, in my opinion, *Dua* renders obvious limitation 34[g].

vi. 34[h]

257. *Dua* discloses “the mechanical switch being configured for switching the RFID tag from an OFF state to one of the plurality of alternative ON states.”

258. As discussed above with reference to limitation 20[a], each hot button (mechanical switch) may select a QuickWave state (first ON state), credit card state (second ON state), or debit card state (third ON state). *See supra* §XIII.C.ii. In the scenario where the device is in a deactivated state (OFF state), and a hot button (mechanical switch) is then pressed, the device will switch from an OFF state to an ON state. EX1023, [0383], [0386].

259. Therefore, in my opinion, *Dua* discloses limitation 34[h].

F. Independent Claim 44

i. 44[pre]

260. In my opinion, *Dua* discloses a “method of changing a state of an RFID

Tag” for the same reasons discussed above in connection with limitations 1[d]–[f].

See supra §XIII.A.v–vii.

ii. 44[a]–[b]

261. In my opinion, *Dua* discloses limitations 44[a]–[b] for the same reasons discussed above in connection with limitations 1[a]–[b]. *See supra* §XIII.A.ii–iii.

iii. 44[c]

262. In my opinion, *Dua* discloses “reading a key from a key memory” for the same reasons discussed above in connection with limitations 1[e]–[f]. *See supra* §XIII.A.vi–vii.

iv. 44[d]

263. In my opinion, *Dua* discloses “using an integrated circuit to compare the first data received through the RF antenna with the key read from the key memory, the integrated circuit powered by the received energy” for the same reasons discussed above in connection with limitations 1[a]–[b] and 1[f]. *See supra* §§XIII.A.ii–iii (integrated circuit is powered by received energy), XIII.A.vii (first data is compared to key).

v. 44[e]

264. In my opinion, *Dua* discloses “determining a state of a mechanical switch in the RFID tag” for the same reasons discussed above in connection with limitation 20[a]. *See supra* §XIII.C.ii.

vi. 44[f]

265. In my opinion, *Dua* renders obvious “writing data to state memory responsive to the comparison only if the mechanical switch is activated, the data written to the state memory being configured to change the RFID tag from a first state to a second state” for the same reasons discussed above in connection with limitations 1[f] and 20[a]. *See supra* §§XIII.A.vii (writing data to state memory responsive to comparison), XIII.C.ii (changing ON states only if mechanical switch is activated).

G. Independent Claim 51

i. 51[pre]–[e]

266. In my opinion, *Dua* discloses and/or renders obvious limitations 51[pre]–[e] for the same reasons discussed above in connection with limitations 44[pre]–[f]. *See supra* §XIII.F.i–vi.

ii. 51[f]

267. In my opinion, *Dua* discloses “the first state and the second state are alternative ON states” for the same reasons discussed above in connection with limitation 1[d]. *See supra* §XIII.A.v.

H. Independent Claim 53

i. 53[pre]–[e]

268. In my opinion, *Dua* discloses and/or renders obvious limitations 53[pre]–[e] for the same reasons discussed above with reference to limitations

44[pre]–[f]. *See supra* §XIII.F.i–vi.

ii. 53[f]

269. *Dua* discloses “providing an RF response, a content of data in the RF response being responsive to the comparison.”

270. As discussed above with reference to limitations 1[d] and 1[f], after receiving a key from an RFID reader, the wireless device can provide a response transmission (RF response) including specific payment credentials (content of data in the RF response), based on which stored reader key corresponds to the received key (responsive to the comparison). *See supra* §§XIII.A.v, XIII.A.vii.

271. Therefore, in my opinion, *Dua* discloses limitation 53[f].

I. Independent Claim 54

i. 54[pre]–[a]

272. In my opinion, *Dua* discloses limitations 54[pre]–[a] for the same reasons discussed above in connection with limitations 44[pre] and 44[b]. *See supra* §§XIII.F.i–ii.

ii. 54[b]

273. In my opinion, *Dua* renders obvious “reading a state from a state memory, the state memory being configured to alternatively store an OFF state, a first ON state and a second ON state” for the same reasons discussed above in connection with limitations 1[d] and 1[g]. *See supra* §§XIII.A.v (storing an OFF

state, a first ON state, and a second ON state in state memory), XIII.A.viii (reading the state from state memory to determine whether to provide a response signal).

iii. 54[c]–[d]

274. In my opinion, *Dua* discloses limitations 54[c]–[d] for the same reasons discussed above in connection with limitations 1[d] and 1[g]. *See supra* §§XIII.A.v (contents of response signal depend on whether the current state is the first ON state or the second ON state), XIII.A.viii (sending response signal using antenna depending on whether the current state is the first ON state or the second ON state).

J. Independent Claim 57

i. 57[pre]–[a]

275. In my opinion, *Dua* discloses limitations 57[pre]–[a] for the same reasons discussed above in connection with limitations 44[pre] and 44[b]. *See supra* §§XIII.F.i–ii.

ii. 57[b]–[c]

276. In my opinion, *Dua* discloses limitations 57[b]–[c] for the same reasons discussed above in connection with limitations 54[b]–[c]. *See supra* §§XIII.I.ii–iii.

iii. 57[d]

277. In my opinion, *Dua* discloses “sending the response signal is responsive to a mechanical switch” for the same reasons discussed above in connection with limitation 20[f]. *See supra* §XIII.C.iv.

K. Dependent Claims

i. Dependent Claims 2, 15

278. *Dua* renders obvious “the ON/OFF state of the RFID tag is OFF by default and temporally ON.” As discussed above with reference to limitation 1[d], *Dua*’s wireless device is in a deactivated state (OFF state) by default, and transitions to one of several transaction states (ON states) only temporarily, when a “hot button” is pressed by the user. *See supra* §XIII.A.v. When RF communication is enabled, the device remains in an ON state for a 30-second window, following which “the application will disable RF communication and the application may shutdown or go into its normal dormant state” (OFF state). EX1023, [0383], [0395].

279. Therefore, in my opinion, *Dua* renders obvious claims 2 and 15.

ii. Dependent Claims 3, 16

280. *Dua* renders obvious “the ON/OFF state of the RFID tag is stored in static memory” for the same reasons discussed above with reference to limitation 1[d]. *See supra* §XIII.A.v. In my opinion, as discussed above, it would have been obvious to a POSITA to store the current state (deactivated, QuickWave, credit card, or debit card) of the wireless device in device memory (state memory). *Id.* It also would have been obvious to a POSITA that device memory storing variable values would be implemented as static RAM, as this was a well-known practice as of the time of invention. EX1026, 24, 26, 34, 47.

281. Therefore, in my opinion, *Dua* renders obvious claims 3 and 16.

iii. Dependent Claim 4

282. In my opinion, *Dua* renders obvious “the determination is responsive to which of the alternative ON states are stored in the state memory” for the same reasons discussed above in connection with limitation 1[g]. *See supra* §XIII.A.viii.

iv. Dependent Claim 5

283. *Dua* renders obvious “the RFID tag is disposed within a passport.” *Dua* discloses that the wireless device may include contactless smart card technology, and specifically addresses the use of such technology in access control applications. EX1023, [0009], [0011]–[0012]. *Dua* further discloses that the wireless device with the wallet application can serve as a replacement for identity documents with RFID functionality. *Id.*, [0333], [0342]. It is my opinion that it therefore would have been obvious to a POSITA to incorporate the RFID functionality of *Dua*’s wireless device within a passport, as such identity documents with RFID capability were well-known as of the time of invention. EX1030, 4, 14.

284. Therefore, in my opinion, *Dua* renders obvious claim 5.

v. Dependent Claim 6

285. In my opinion, *Dua* renders obvious “the state memory is configured to store in the alternative, an OFF state, a first ON state and a second ON state” for the same reasons discussed above in connection with limitation 1[d]. *See supra*

§XIII.A.v.

vi. Dependent Claim 7

286. In my opinion, *Dua* renders obvious “the state memory is configured to store a first value indicating an ON/OFF state and a second value indicating one of at least two alternative ON states” for the same reasons discussed above in connection with limitation 1[d]. *See supra* §XIII.A.v.

vii. Dependent Claims 8, 18, 25–26, 32, 37, 55, 58

287. In my opinion, *Dua* discloses “the RFID tag is disposed within a cellular telephone.” *Dua*’s hardware and software enabling RFID communication (RFID tag) is disposed in a wireless device, which is preferably a cellular telephone. EX1023, [0026], [0041], FIG. 7.

viii. Dependent Claims 9, 19, 27, 33, 38

288. In my opinion, *Dua* renders obvious “the RFID tag is disposed within a passport, identity card, driver’s license, immigration document, student identity card, library card, financial card, social security card, military ID card, key, keycard, or identification document” for the same reasons discussed above in connection with claim 5. *See supra* §XIII.K.iv.

ix. Dependent Claims 10, 28, 50, 56, 59

289. In my opinion, *Dua* renders obvious “the RFID tag is disposed within a passport, driver’s license, financial card, military ID card, key, or keycard” for the

same reasons discussed above in connection with claim 5. *See supra* §XIII.K.iv.

x. Dependent Claim 17

290. *Dua* discloses “the RFID tag is not remotely detectable using an RF signal when the ON/OFF state is OFF.” As discussed above with reference to limitation 1[d], *Dua*’s wireless device can enter a deactivated state (OFF state). *See supra* §XIII.A.v. In that state, the wireless device does not transmit credentials, and thus the RFID interface (RFID tag) is not remotely detectable using an RF signal. EX1023, [0383], [0386], [0395].

291. Therefore, in my opinion, *Dua* discloses claim 17.

xi. Dependent Claims 21, 30, 35

292. In my opinion, *Dua* renders obvious “the input is further configured to receive power resulting from the first RF signal and to power the integrated circuitry using the power” for the same reasons discussed above in connection with limitations 1[a]–[b]. *See supra* §XIII.A.ii–iii.

xii. Dependent Claims 22, 31, 36

293. In my opinion, *Dua* discloses “the integrated circuitry is configured for authorizing a transaction responsive to the mechanical switch” for the same reasons discussed above in connection with limitation 20[f]. *See supra* §XIII.C.iv.

xiii. Dependent Claim 23

294. *Dua* renders obvious “the mechanical switch must be activated and the

state stored in the state memory must be an ON state before the second RF signal is transmitted” for the same reasons discussed above with reference to limitations 1[g] and 20[a]. *See supra* §§XIII.A.viii, XIII.C.ii. As discussed above, a hot button (mechanical switch) must be pressed in order to transition from the deactivated state (OFF state) to an ON state, and the wireless device will only transmit payment credentials (second RF signal) when it is in an ON state. *Id.*

295. Therefore, in my opinion, *Dua* renders obvious claim 23.

xiv. Dependent Claim 24

296. In my opinion, *Dua* renders obvious “a key memory configured for storing a key for changing the state stored in the state memory, the switch logic being further configured to read the key from the key memory, to compare the received data with the read key, and to change the state stored in the state memory responsive to the comparison between the received data with the read key” for the same reasons discussed above in connection with limitation 1[f]. *See supra* §XIII.A.vii.

xv. Dependent Claim 45

297. *Dua* discloses “the first state is a state in which the RFID tag will not transmit an RF signal.” As discussed above with reference to limitation 1[d], *Dua*’s wireless device may be in a deactivated state (first state/OFF state), in which no credentials will be transmitted (the RFID tag will not transmit an RF signal). *See supra* §§XIII.A.v, XIII.K.x.

298. Therefore, in my opinion, *Dua* discloses claim 45.

xvi. Dependent Claim 46

299. *Dua* renders obvious “using an integrated circuit to compare the first data received through the RF antenna with the key is only performed if the state of the mechanical switch is ON.” As discussed above with reference to limitations 1[f] and 20[a], *Dua* discloses logic to receive a key (first data) from an RFID reader, compare the received key with a stored reader key (key), and transition from a deactivated state (OFF state) to an ON state. *See supra* §§XIII.A.vii, XIII.C.ii. *Dua* further discloses that a hot button (mechanical switch) must be pressed to enable RF communication. EX1023, [0383], [0386], [0395]. In my opinion, it would have been obvious to a POSITA that this comparison would only be performed after the hot button (mechanical switch) is activated (ON), as the RF communication that enables receipt of the first data is only enabled after a hot button (mechanical switch) is pressed.

300. Therefore, in my opinion, *Dua* renders obvious claim 46.

xvii. Dependent Claims 47, 52

301. *Dua* renders obvious “the state memory is non-volatile memory” for the same reasons discussed above with reference to limitation 1[d] and claims 3 and 16. *See supra* §§XIII.A.v, XIII.K.ii. In my opinion, as discussed above, it would have been obvious to a POSITA to store the current state of *Dua*’s wireless device

in device memory (state memory). *Id.* It also would have been obvious to a POSITA that device memory storing variable values would be implemented as non-volatile memory, such that the stored data can be retained after the device is powered off, as this was a well-known practice as of the time of invention. *See, e.g.,* EX1026, 34, 47.

302. Therefore, in my opinion, *Dua* renders obvious claims 47 and 52.

xviii. Dependent Claim 48

303. In my opinion, *Dua* discloses “automatically returning to the OFF state.” As discussed above with reference to limitations 1[d] and 14[d], when a hot button is pressed, the wireless device transitions from a deactivated state (OFF state) to an ON state for a 30-second interval, after which the device automatically returns to the deactivated state (OFF state). *See supra* §§XIII.A.v, XIII.B.ii; EX1023, [0383], [0395].

xix. Dependent Claim 49

304. In my opinion, *Dua* discloses “sending a response signal using the RF antenna if the second state is an ON state” for the same reasons discussed above in connection with limitation 53[f]. *See supra* §XIII.H.ii.

XIV. GROUND 2B: *DUA* WITH *PONT* RENDERS OBVIOUS CLAIMS 1–10, 14–38 AND 44–59

305. *Dua* with *Pont* renders obvious claims 1–10, 14–38, and 44–59.

A. Motivation to Combine

306. Both *Dua* and *Pont* are directed to mobile phone applications. *Dua* is directed to a mobile phone including components to control and carry out financial transactions using RFID communication. EX1023, [0025], [0333]. *Pont* is directed to mobile phone processors, which can be used to control operations. EX1026, xi.

307. Specifically, *Dua* uses the wireless device's processor, running a software-based "wallet application," to control the RFID interface and related components to carry out RFID transaction functionality. EX1023, [0041], [0333]. While *Dua* describes these features in functional terms, it lacks specific disclosure of how these features would be implemented at a software level. For example, *Dua* discloses that the wallet application can read a hot button input and interact with device memory to select and transmit credentials, but does not disclose *how* a processor would read such a switch input or *how* a processor would interact with memory to effectuate a desired output. EX1023, [0388]–[0395]. *Pont* fills this gap by providing guidance on how to implement *Dua*'s operational states using conventional embedded controller state logic and state memory. Specifically, *Pont* teaches that "[m]uch of the activity in embedded systems involves reading pins (which may, for example, be connected to switches or keypads) and altering the value of other pins (which may, in turn, control anything...)." EX1026, 29, 192 ("system states will usually be represented by means of a switch statement in the

operating system [interrupt service routine]”), 205 (“The system will operate in two or more states....Transitions between states may be controlled by...system inputs or by a combination of time and inputs.”). Thus, in my opinion, a POSITA would turn to *Pont* for such knowledge, as *Pont* is a contemporary textbook which provides specific and relevant teachings related to programming techniques for embedded processors. *Id.*, xi. Such processors can include mobile phone processors, similar to the mobile phone processor of *Dua*. *Id.* *Pont* therefore provides useful guidance to a POSITA related to specific methods of programming a microprocessor to carry out mobile phone applications.

308. As discussed above with reference to Ground 1B, *Pont* discloses that a controller can be programmed to interface with a switch and change a device state based on the value of the switch, similar to the functionality described in *Dua*, and that to enable such functionality, the state would be stored in an output state variable. *See supra* §XI.A. As further discussed above, *Pont* also teaches that the value of the output state variable is stored in RAM, which corresponds to a state memory, because it stores information indicating the current state of the device. *Id.*

309. It is my opinion that based on these teachings, a POSITA would have been motivated to apply *Pont*’s control structure to *Dua*, such that an output state variable stores the active state of the RFID functionality. For example, according to *Pont*’s teachings, a POSITA would understand that in *Dua*, a polling loop would be

used to check the current value of a hot button (mechanical switch). On each iteration of the polling loop, the switch value would be assigned to a switch state variable. Then, the value of the switch state variable would be passed to a controller function of the wallet application. The controller function would then apply logic to determine the current state of the RFID transaction functionality, as taught by *Dua*. The function would assign this state to an RFID state variable and use the value of this variable to control the downstream functions of the device. As taught by *Pont*, the implementation of such logic would require that the RFID state is stored in RAM, which can correspond to a state memory.

310. Moreover, in my opinion, a POSITA would have had a reasonable expectation of success in making this combination. For example, *Pont* discloses that its teachings are directly applicable to embedded processors in mobile phones. EX1026, xi, 2. The *Dua-Pont* combination therefore involves nothing more than applying known elements (software control) in a known structure (mobile phones) using known methods (programming in C) to achieve a well-understood and predictable benefit (reliable control of mobile phone processes). A POSITA would reasonably expect this combination to succeed without undue experimentation, as it relies on established programming techniques and produces understood results.

B. “State Memory” Claims: 1, 4, 6–7, 14, 20, 23–24, 29, 34, 44, 47, 51–54, 57

311. *Dua-Pont* renders obvious a “state memory,” as recited in claims 1, 4,

6–7, 14, 20, 23–24, 29, 34, 44, 47, 51–54, and 57.

312. In my opinion, as discussed above, based on *Pont*'s teachings, a POSITA would have understood that the device of *Dua* would include RAM, which would store information representing the current state of the device. *See supra* §XIV.A. For example, the device RAM (state memory) would store the current value of a device state variable (QuickWave (first ON state), credit card (second ON state), debit card (third ON state), or deactivated (OFF state)). *Id.*

313. Except for the implementation of the state memory described above, *Dua-Pont* is identical to *Dua*. Thus, the remaining limitations of claims 1, 4, 6–7, 14, 20, 23–24, 29, 34, 44, 47, 51–54, and 57 are disclosed and/or rendered obvious by *Dua-Pont* for the same reasons discussed above, with respect to *Dua*. *See supra* §XIII.

314. Thus, in my opinion, *Dua-Pont* renders obvious the “state memory” limitation of claims 1, 4, 6–7, 14, 20, 23–24, 29, 34, 44, 47, 51–54, and 57.

C. Claims 2–3, 5, 8–10, 15–19, 21–22, 25–28, 30–33, 35–38, 45–46, 48–50, 55–56, 58–59

315. As discussed above, except for the implementation of the state memory described above, *Dua-Pont* is identical to *Dua*. Thus, in my opinion, claims 2–3, 5, 8–10, 15–19, 21–22, 25–28, 30–33, 35–38, 45–46, 48–50, 55–56, and 58–59 are disclosed and/or rendered obvious by *Dua-Pont* for the same reasons discussed above, with respect to *Dua*. *See supra* §XIII.

XV. GROUND 2C: *DUA* WITH *SELKER* RENDERS OBVIOUS CLAIMS 39–43

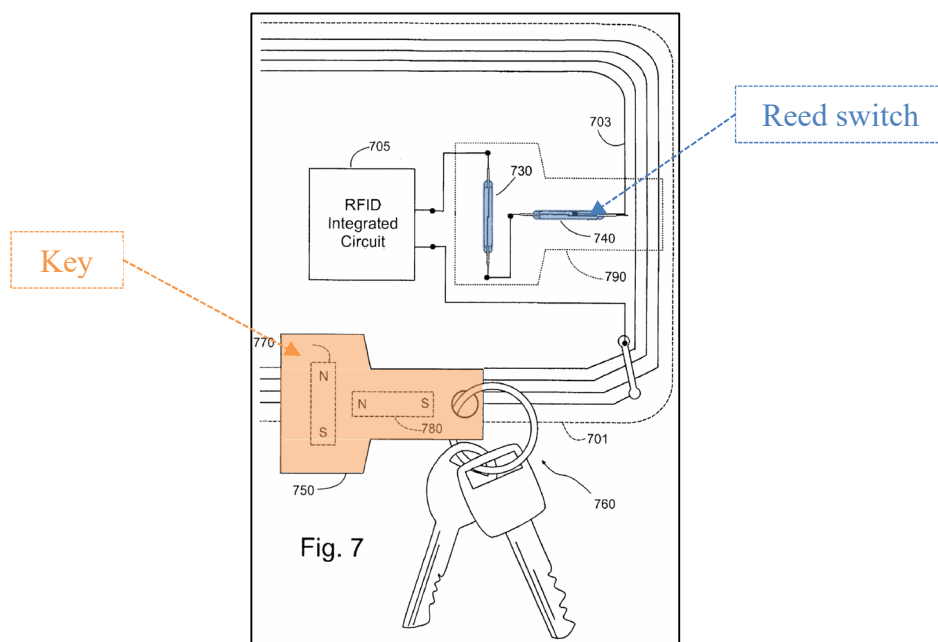
316. *Dua* with *Selker* renders obvious claims 39–43.

A. Motivation to Combine

317. Both *Dua* and *Selker* are directed to RFID payment technologies. *Dua* is directed to a wireless device, such as a cellular telephone, that can carry out financial transactions using RFID communication. EX1023, [0026], [0041], [0296], FIG. 7. *Selker* is directed to a mechanism to protect RFID payment cards from unauthorized misuse. EX1027, [0004].

318. *Dua* discloses the implementation of hot buttons (mechanical switches), which enable RFID communication and control the transmission of credentials, to improve data security in RFID applications. *Dua* explains that “[b]ecause of the sensitive nature of information stored in the wallet application, users want to ensure that they have complete control over the transmission of information to an external reader such as at a retail point-of-sale,” and that “the existence of a button in an RFID-enabled wireless device that controls activation of the wallet application and transmission of credentials via RF could eliminate a similar fraud risk.” EX1023, [0382]–[0383], [0392]–[0395]. Thus, as discussed above, the use of hot buttons can prevent an unauthorized bad actor from reading (skimming) credentials from the wireless device. *Id.* *Selker* similarly addresses the issue that “because RF-enabled devices such [as] payment cards can be read at a

distance with a suitable transmitter and receiver, it is possible to surreptitiously obtain information from the card while it remains in its cardholder's possession. In addition to non-contact data transfer, wireless communication can also allow non-line-of-sight communication, meaning that an RF-enabled device may be read while it remains in the cardholder's wallet or purse." EX1027, [0003]. Thus, *Selker* teaches that security can be further improved by implementing a reed switch and key mechanism, which is "functionally flexible in order to work in cards and other devices having a variety of shapes and sizes." *Id.*, [0004], [0027], [0031], FIG. 7.



Id., FIG. 7.

319. According to *Selker*, this mechanism provides "enhanced security" and "helps protect" the RFID device "from unauthorized misuse." *Id.*, [0004], [0019]. Thus, in my opinion, a POSITA would have been motivated to implement *Selker*'s

reed switch and key mechanism in the device of *Dua* to achieve the heightened security taught by *Selker*, with respect to especially sensitive financial accounts, such as debit accounts. *Id.*, [0004], [0027], [0031], FIG. 7. To do so, a POSITA would have understood to replace *Dua*'s "Debit" hot button (mechanical switch) with a set of perpendicular reed switches, as taught by *Selker*. *Id.* Thus, to authenticate themselves and enable a sensitive debit transaction, a user can place the magnetic key in close proximity to the reed switches, which would close the switch circuit, similar to pressing *Dua*'s original hot button.

320. Moreover, in my opinion, a POSITA would have had a reasonable expectation of success in making this combination. For example, *Dua* discloses similar security measures. EX1023, [0392]–[0395] (discussing hot buttons to prevent skimming). Meanwhile, *Selker* provides an alternative reed switch and key mechanism, which provides further enhanced security. EX1027, [0004], [0019]. The *Dua-Selker* combination therefore involves nothing more than applying known elements (a reed switch and key mechanism) in a known structure (mobile phones) using known methods (basic circuit design) to achieve a well-understood and predictable benefit (improved security). It is my opinion that a POSITA would reasonably expect this combination to succeed without undue experimentation, as it relies on established circuit design techniques and produces understood results.

B. Independent Claim 39

i. 39[pre]

321. Except for the implementation of the reed switch and key mechanism described above, *Dua-Selker* is identical to *Dua*. Thus, in my opinion, limitation 39[pre] is rendered obvious by *Dua-Selker* for the same reasons discussed above, with respect to *Dua*. *See supra* §XIII.A.i.

ii. 39[a]

322. *Dua-Selker* renders obvious a “mechanical switch responsive to a state of a mechanical security device.”

323. In my opinion, as discussed above, based on *Selker*’s teachings, a POSITA would have replaced *Dua*’s “Debit” hot button (mechanical switch) with a set of two perpendicular reed switches (mechanical switch), as taught by *Selker*, to achieve enhanced security. *See supra* §XV.A. As further taught by *Selker*, the set of reed switches (mechanical switch) is normally open. EX1027, [0027], FIG. 7. When a magnetic key (mechanical security device) is brought in close proximity to the set of reed switches (mechanical switch), the circuit is closed. *Id.* Thus, in *Dua-Selker*, the set of reed switches (mechanical switch) is responsive to the magnetic key (mechanical security device). *Id.*

324. Thus, in my opinion, *Dua-Selker* renders obvious claim 39[a].

iii. 39[b]–[f]

325. Except for the implementation of the reed switch and key mechanism described above, *Dua-Selker* is identical to *Dua*. Thus, in my opinion, limitations 39[b]–[f] are rendered obvious by *Dua-Selker* for the same reasons discussed above, with respect to *Dua*. *See supra* §§XIII.A.ii–v, XIII.C.iv.

C. Dependent Claims

i. Dependent Claim 40

326. In my opinion, *Dua-Selker* discloses “the integrated circuitry is configured for authorizing a transaction responsive to the mechanical switch” for the same reasons discussed above with respect to limitation 20[f]. *See supra* §XIII.C.iv.

ii. Dependent Claim 41

327. In my opinion, *Dua-Selker* discloses “the RFID tag is disposed within a cellular telephone” for the same reasons discussed above with respect to claims 8, 18, 25–26, 32, 37, 55, and 58. *See supra* §XIII.K.vii.

iii. Dependent Claim 42

328. In my opinion, *Dua-Selker* discloses “the RFID tag is disposed within passport, identity card, driver's license, immigration document, student identity card, library card, financial card, social security card, military ID card, key, keycard, or identification document” for the same reasons discussed above with respect to claims 9, 19, 27, 33, and 38. *See supra* §XIII.K.viii.

iv. Dependent Claim 43

329. In my opinion, *Dua-Selker* discloses “the RFID tag is disposed within a passport, driver’s license, financial card, military ID card, key, or keycard” for the same reasons discussed above with respect to claims 10, 28, 50, 56, and 59. *See supra* §XIII.K.ix.

XVI. CONCLUSION

330. 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 September 18, 2026.

A handwritten signature in cursive script, appearing to read "Sayfe Kiaei".

By: _____
Dr. Sayfe Kiaei