

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner

v.

DH INTERNATIONAL LTD.
Patent Owner

Case No. IPR2025-00173
U.S. Patent No. 7,628,333

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 7,628,333**

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	SUMMARY OF THE '333 PATENT	1
A.	THE '333 PATENT'S ALLEGED INVENTION	1
B.	THE '333 PATENT'S PROSECUTION.....	4
C.	A PERSON OF ORDINARY SKILL IN THE ART	6
III.	OVERVIEW OF THE PRIOR ART	6
A.	OVERVIEW OF <i>McGREGOR</i>	6
B.	OVERVIEW OF <i>PALMER</i>	9
C.	OVERVIEW OF <i>TUTTLE</i>	12
IV.	PROCEDURAL REQUIREMENTS UNDER 37 C.F.R. § 42.104	14
A.	STANDING UNDER 37 C.F.R. § 42.104(A)	14
B.	CHALLENGE UNDER 37 C.F.R. § 42.104(B) AND RELIEF REQUESTED	15
C.	CLAIM CONSTRUCTION UNDER 37 C.F.R. § 42.104(B)(3)	15
	<i>i. "Invariable Activation Command"</i>	<i>16</i>
V.	THE CHALLENGED CLAIMS ARE UNPATENTABLE	20
A.	GROUND 1: CLAIMS 1, 2, AND 4-10 ARE OBVIOUS UNDER PRE-AIA 35 U.S.C. § 103 OVER <i>McGREGOR</i> IN VIEW OF <i>PALMER</i>	20
	<i>i. Claim 1</i>	<i>20</i>
	<i>ii. Claim 2.....</i>	<i>45</i>
	<i>iii. Claim 4.....</i>	<i>45</i>
	<i>iv. Claim 5</i>	<i>46</i>
	<i>v. Claim 6</i>	<i>48</i>
	<i>vi. Claim 7</i>	<i>50</i>
	<i>vii. Claim 8.....</i>	<i>50</i>
	<i>viii. Claim 9.....</i>	<i>50</i>
	<i>ix. Claim 10</i>	<i>51</i>
B.	GROUND 2: CLAIMS 3 AND 11-13 ARE OBVIOUS UNDER PRE-AIA 35 U.S.C. § 103 OVER <i>McGREGOR</i> IN VIEW OF <i>PALMER</i> AND IN FURTHER VIEW OF <i>TUTTLE</i>	54
	<i>i. Claim 3.....</i>	<i>55</i>
	<i>ii. Claim 11.....</i>	<i>60</i>
	<i>iii. Claim 12.....</i>	<i>62</i>
	<i>iv. Claim 13</i>	<i>63</i>
VI.	DISCRETIONARY CONSIDERATIONS.....	64
A.	THE BOARD SHOULD NOT DENY INSTITUTION UNDER <i>FINTIV</i>	64

B.	THE <i>GENERAL PLASTICS</i> FACTORS FAVOR INSTITUTION	65
VII.	CONCLUSION	67
VIII.	MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(A)(1)	68
A.	REAL PARTY-IN-INTEREST	68
B.	RELATED MATTERS.....	68
C.	LEAD AND BACK-UP COUNSEL	68

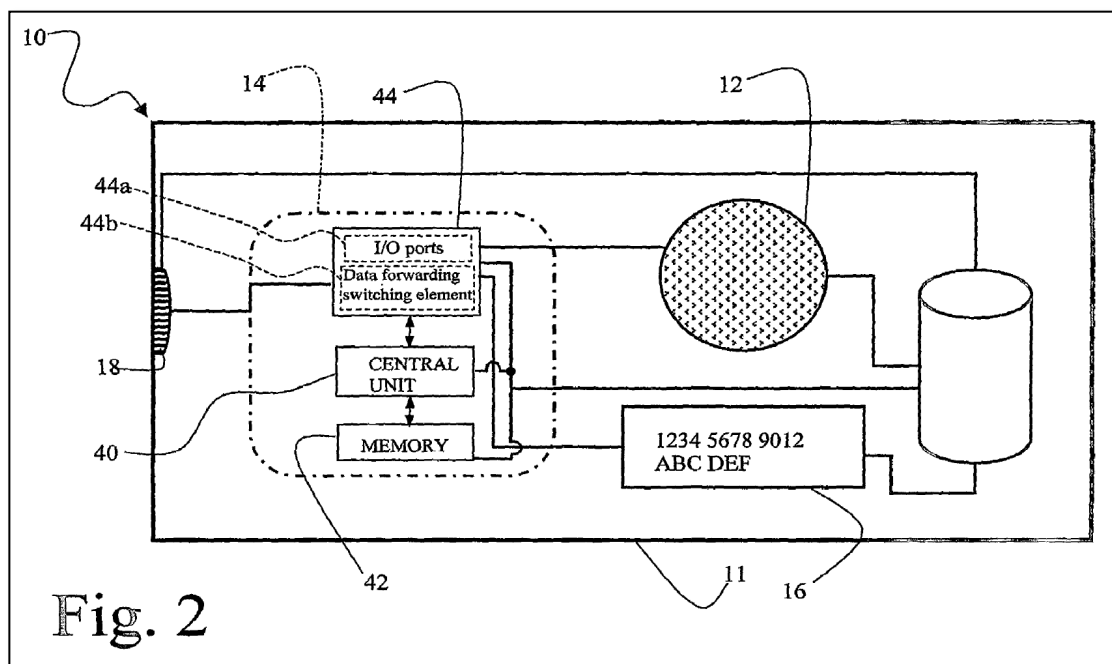
I. INTRODUCTION

Petitioner Apple Inc. (“Petitioner”) requests *Inter Partes* Review (“IPR”) of Claims 1-13 (the “Challenged Claims”) of U.S. Patent No. 7,628,333 (“the ’333 Patent”).

II. SUMMARY OF THE ’333 PATENT

A. The ’333 Patent’s Alleged Invention

The ’333 Patent is generally directed to “a portable electronic device capable of alternate data conveyance operations responsive to an invariable activation command.” ’333 *Patent* (Ex. 1001), 1:9-11. One such portable electronic device, depicted in Fig. 2, includes a “control device 12, an electronic circuit 14, a display screen 16, a transceiver 18 and power means 20” as well as “switching element 44b.” *Id.*, 4:19-30, 6:9, Fig. 2.



Id., Fig. 2.

Switching element 44b can take many forms, including (1) a “series of instructions programmed” on a microchip or (2) “a decisional logical circuit.” *Id.*, 6:4-17 (teaching that switching element can generally “be a physical structure, a virtual program, or both”). Portable electronic device 10 receives an activation cue from an external device via “transceiver 18[.]” *Id.*, 5:65-67. When an activation cue is received, the switching element 44b changes from a default state (i.e., an inactive state) to an “activated state[.]” *Id.*, 6:18-26.

Then, “upon control device 12 being selectively triggered” the portable device initiates a data conveyance operation dependent on the “state of switching element 44b.” *Id.*, 6:42-51. The control device 12 may be “a single manually activated button” or “a biometric parameter detector, for example a fingerprint scanner” that can be selectively triggered to issue an invariable activation command. *Id.*, 5:8, 5:13-14. The invariable activation command, in turn, results in the portable electronic device 10 initiating one of two data exchange operations depending on the state of the “switching element 44b[.]” *Id.*, 6:18-25.

If the control device is triggered while the switching element is in an activated state, “a data exchange will be initiated between the portable electronic device 10 and data exchange device 9.” *Id.*, 7:12-14. Alternatively, if the control device is triggered when the switching element is in a default, inactive state, “data will be

communicated to the portable electronic device holder by means of user interface device 16” (e.g., a display). *Id.*, 7:9-11.

In one example, the portable electronic device 10 acts as a “quick payment means, such as for paying public transportation fares.” *Id.*, 7:57-58. The “portable electronic device 10 would be a payment card with pre-stored electronic money[.]” *Id.*, 7:59-61. When the user wants to purchase a fare, the user would trigger the control device 12 within the range of “[d]ebit machine 9 . . . emit[ting] an activation cue[.]” *Id.*, 7:64-8:7. Since an activation cue is received the switching element is in an activated state. Subsequently, a wireless data exchange takes place between the portable electronic device and the debit machine 9, consisting of “any type of information required for electronic money transactions[.]” *Id.*, 7:64-8:7. If control device 12 is triggered outside the “emission range of a public transportation service debit machine 9,” no activation cue is received and the switching element remains in an inactive state. *Id.*, 8:24-29, 6:18-25. In this situation, data will be sent to display screen 16, displaying the “total amount of electronic money remaining[.]” instead of exchanging data with the debit machine 9. Data is displayed, rather than transmitted, in this inactive state because the debit machine 9 is presumed to be outside the communication range of the portable electronic device. *Id.*, 8:24-29.

In a second example the portable electronic device 10 is an electronic passport. In the presence of an activation cue, the switching element is in an activated

state and the portable electronic device 10 “transmit[s] identification data of the electronic passport owner[.]” *Id.*, 8:46-49. Where an activation cue is not received, the switching element is in an inactive state and the device 10 will “simply display this [identification data] on the display screen[.]” *Id.*, 8:46-49.

The ’333 Patent expressly teaches that the displayed data may be the same as the data transmitted (as in the passport example) or different from the data transmitted (as in the payment example). *Id.*, 8:64-9:3.

B. The ’333 Patent’s Prosecution

The ’333 Patent issued from U.S. Application Serial No. 10/552,912 (the “’912 Application”), filed on February 27, 2006. The ’912 Application was a U.S. national stage application of PCT Publication No. 2004/090805 filed on April 14, 2003. For the purposes of this Petition only, Petitioner applies April 14, 2003, as the priority date for the Challenged Claims.

A Non-Final Office Action issued on June 16, 2009, rejected claim 12 as anticipated. ’333 *File History*, (Ex. 1002), 153. The Examiner identified U.S. Patent No. 5,999,713 to Reiner et al. (“*Reiner*”) as anticipating the “two different conveyance functions” of the ’912 application by disclosing “contact-based and contactless” based data conveyance modes. *Id.*, 153-154. The Examiner stated that *Reiner* teaches how “[a] cue is received externally, namely a triggering through the

contacts, that causes switching into a contact-mode from the default of the contactless mode.” *Id.*, 154.

Within the same Office Action, the Examiner reviewed DE 101 46 804 to Riemschneider et al. (“*Riemschneider*”), which was also cited in the PCT written opinion. The Examiner found that *Riemschneider* did not teach the limitations of original claims 1-11 and 13-15, stating there was “no evidence of all of the limitations being met including the control device being selectively triggered to issue the invariable activation command such that if the switching element is in the activated state, a data exchange will be initiated through the instrumentality of the data transceiver for exchanging data between the electronic circuit and an external data exchange device and if the switching element is in the inactive state, data will be conveyed from the electronic circuit to the user interface device for communicating information to the portable electronic device holder.” *Id.*, 154-155. As such, those claims were placed in a state of allowance.

The applicant conducted an Examiner interview on July 10, 2009. Following the interview, the applicant cancelled original claim 12 and made several minor claim amendments via Examiner’s amendment. *Id.*, 198. Original, independent claims 1 and 11 (issued claim 10) were amended to include “cue receiver” and “data transceiver” as well as to specify the control device being “selectively” triggered. Original, independent claim 11 (issued claim 10) was amended to include an

electronic circuit in the portable electronic device. *Id.*, 204-208. A Notice of Allowance was issued on July 21, 2009, in which the Examiner reiterated that *Riemschneider* does not anticipate the claims. *Id.*, 208-209.

C. A Person of Ordinary Skill in the Art

A person of ordinary skill in the art at the time of the alleged invention of the '333 Patent ("POSITA") would have had a bachelor's degree in electrical engineering, computer engineering, or a similar discipline with at least two years' experience with wireless communication devices. More education can substitute for practical experience and vice versa. *Dec.*, ¶¶34-36.¹

III. OVERVIEW OF THE PRIOR ART

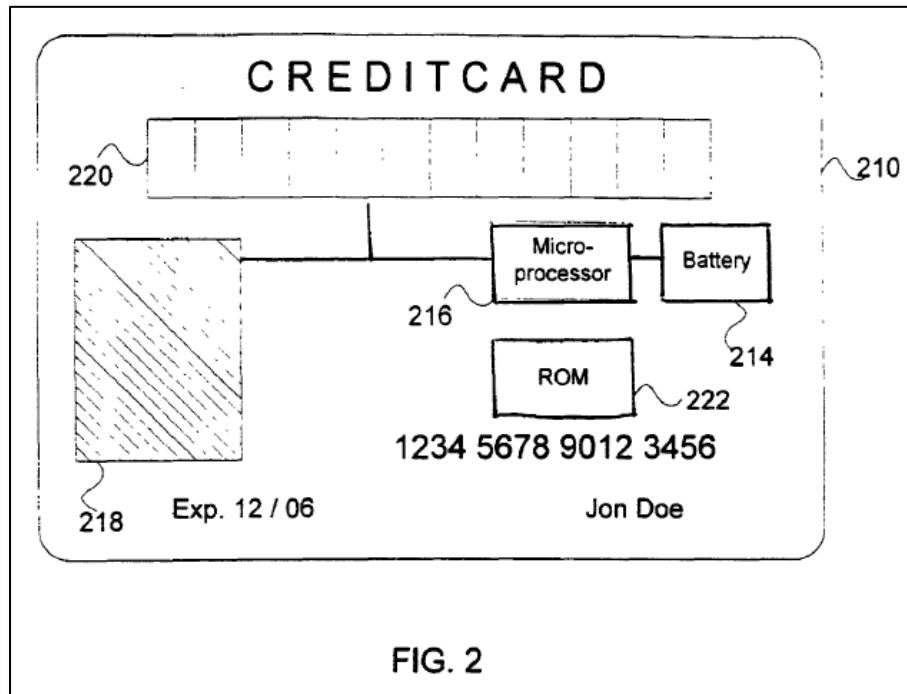
A. Overview of *McGregor*

U.S. Patent Application Publication No. 2002/0180584 to McGregor et al. ("*McGregor*") was filed on December 19, 2001, and is prior art to the '333 Patent under at least 35 U.S.C. §102(a) and §102(e) (pre-AIA). *McGregor* (Ex. 1004), (22). *McGregor* was neither cited nor discussed during prosecution of the '333 Patent. '333 Patent, (56).

McGregor provides a "system for increasing transaction security across existing infrastructure[.]" *McGregor*, Abstract. The disclosure is directed to

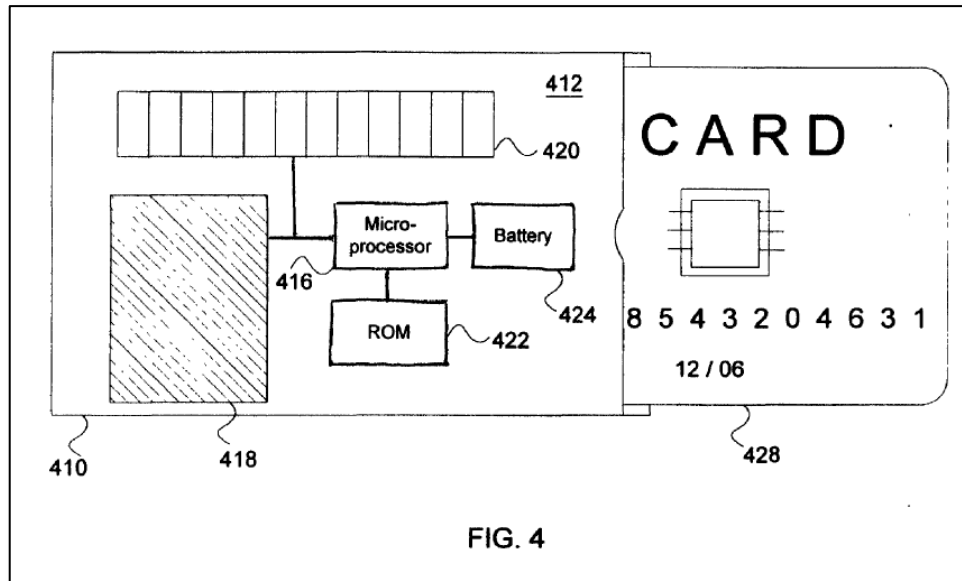
¹ All citations to "Dec." are to paragraph numbers in Ex. 1003, Declaration of Michael Buehrer.

improving credit card security via a “bio-metric smart card.” *Id.*, [0005]. Fig. 2 below illustrates one embodiment of the subject bio-metric smart card:



Id., Fig. 2. As illustrated, *McGregor's* card includes fingerprint scanner 218 for authenticating a user, microprocessor 216 for generating a security key upon successful authentication, and display 220 for displaying the key such that it can be conveyed to a credit card authorization service and used to approve a transaction. *Id.*, [0037-0042].

In a separate embodiment, *McGregor* describes a card reader (or wallet) 410 that has “substantially the same shape and form factor as available plastic credit and debit cards” and may be formed “such that a smart card can be inserted into the reader as shown in FIG. 4.” *Id.*, [0043].



Id., Fig. 4. Wallet 410, like the Fig. 2 bio-metric smart card, includes a “bio-metric reading apparatus such as fingerprint scanner 418 in electrical communication with a microprocessor 416” and “display 420.” *Id.*, [0043]-[0044], Fig. 4. Wallet 410 may also “include an IR or wireless transmitter to automatically transmit the security code to a transaction network.” *Id.*, [0044].

Both *McGregor* and the '333 Patent are directed to portable electronic devices. *Compare McGregor*, [0005], [0043] (disclosing a bio-metric smart card reader to enhance credit card security), *with* '333 Patent, Abstract (describing a portable electronic device), 5:12-19, 7:55-8:31 (describing biometric capabilities and an example embodiment where the device is a payment card for public transportation). Accordingly, *McGregor* is in the same field of endeavor as and is analogous art to the '333 Patent. *Dec.*, ¶¶65-68.

B. Overview of *Palmer*

U.S. Patent Application Publication No. 2003/0226041 to Palmer et al. (“*Palmer*”) was filed on March 27, 2003 and claims priority to U.S. Provisional Application No. 60/368,363 filed on March 28, 2002, and is prior art to the ’333 Patent under at least 35 U.S.C. §102(e) (pre-AIA).² *Palmer* (Ex. 1005), (22). *Palmer* was neither cited nor discussed during prosecution of the ’333 Patent. ’333 Patent, (56).

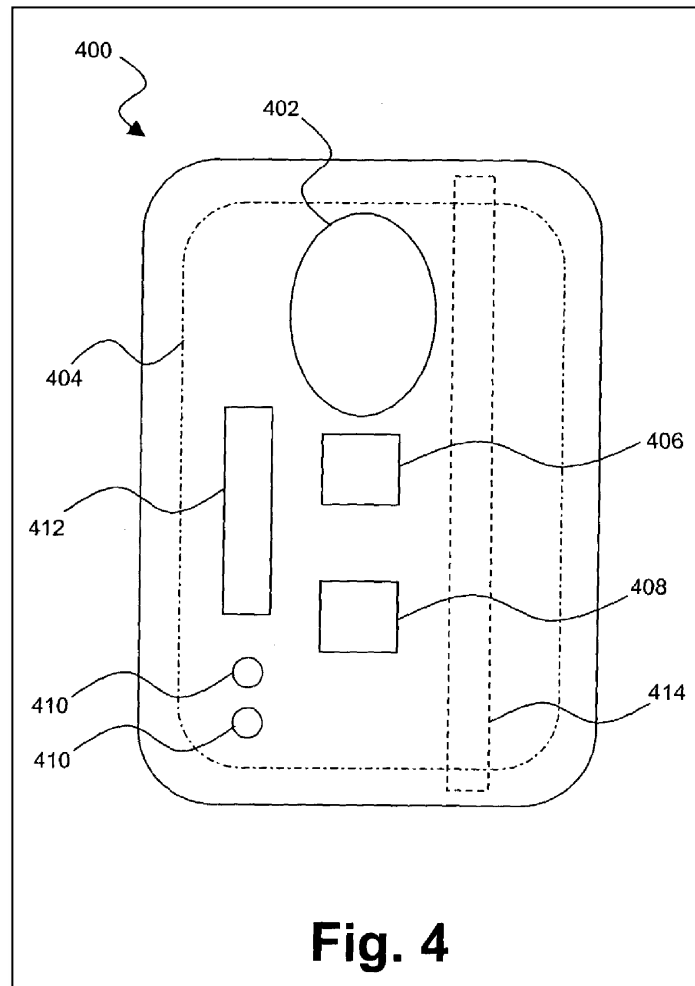
Palmer provides an apparatus for “effecting secure transactions in a contactless manner using biometric identity validation.” *Palmer*, Abstract. In one embodiment, device 400 has “a form factor similar to that of a credit card[,]” and contains “a fingerprint sensor 402, a [radio frequency] RF antenna 404, a first controller 406, second controller 408^[3], function selector buttons 410,” and “an electro-luminescent display 412[.]” *Id.*, [0030].

The first controller 406, which may be implemented as an Application Specific Integrated Circuit (“ASIC”), includes a “Random Access Memory

² If Patent Owner attempts to swear behind *Palmer*’s March 27, 2003 filing date, Petitioner reserves its right to establish that *Palmer* is prior art under §102(e) as of its March 28, 2002 provisional application.

³ For clarity the second controller, also called the “408 smart card chip” in *Palmer*, will be called “smartcard chip 408” throughout this petition.

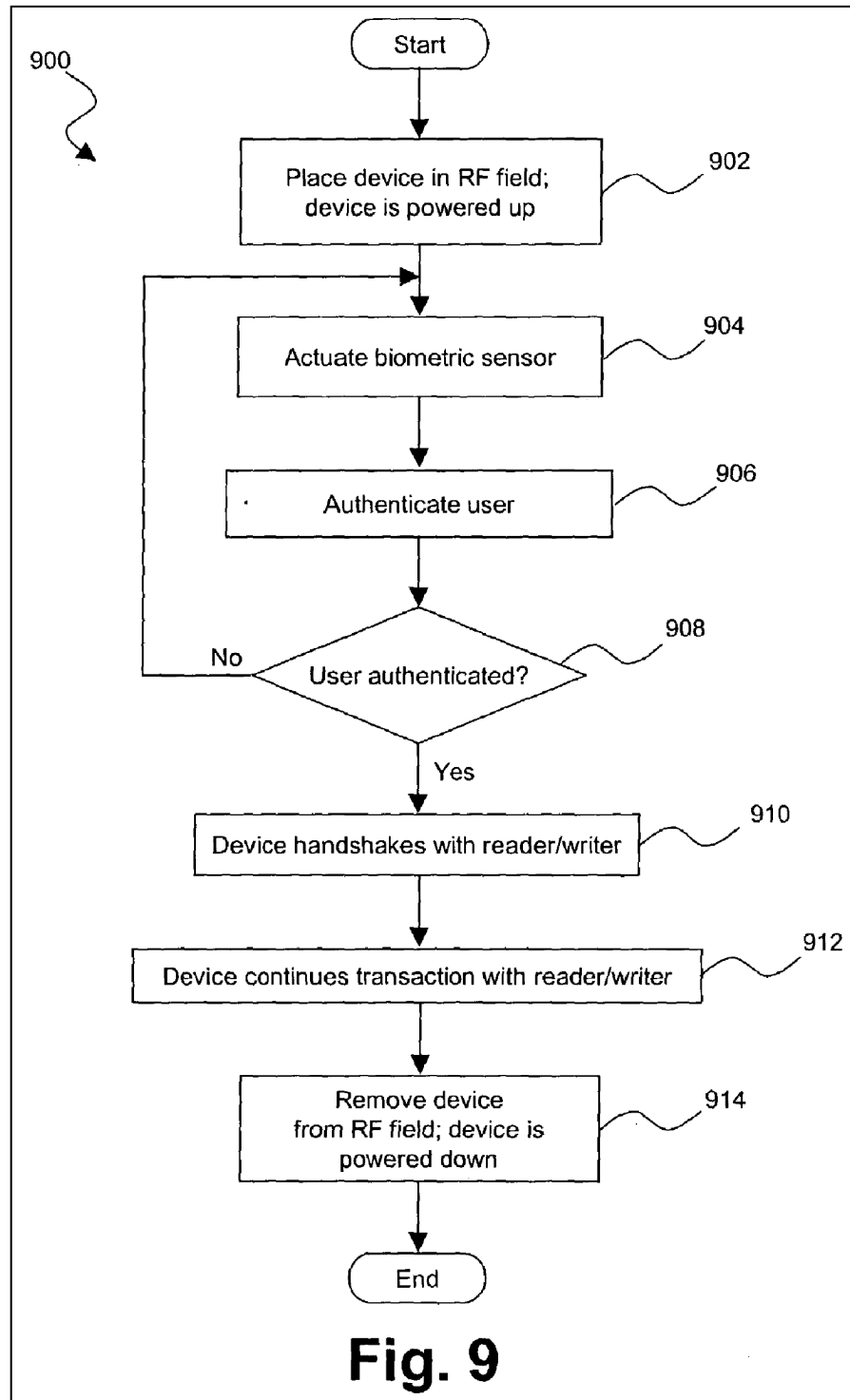
(“RAM”)) and may include a “non-volatile memory” to store fingerprint templates. *Id.*, [0031]. “Circuitry contained within the ASIC 406 provides an interface between the ASIC 406 and the fingerprint sensor 402.” *Id.*, [0032]. ASIC 406 also contains a “microprocessor core . . . for executing instructions” and may be “used to drive electroluminescent display 412[.]” *Id.*



Id., Fig. 4.

When placed within the RF field of a reader/writer device, RF antenna 404 “may capture RF energy . . . and may also support two-way communication with an

associated reader/writer device[.]” *Id.*, [0043]. Fig. 9 illustrates a process through which a user may verify their identity via this two-way communication link:



Id., Fig. 9. As illustrated, the device is placed in the reader/writer device's RF field at step 902,⁴ a user is authenticated using a fingerprint sensor at steps 904-906, the device performs a "handshake" process with the reader/writer after authenticating the user's fingerprint at step 910, and then the devices exchange data pursuant to the transaction. *Id.*, [0050-51].

Both *Palmer* and the '333 Patent are directed to portable electronic devices. *Compare Palmer*, [0030]-[0033] (disclosing an electronic device shaped like a credit card with a smartcard chip to support standard smart card interactions), *with '333 Patent*, 1:15-45 (describing issues with conventional smart cards), 5:12-19, 7:55-8:31 (describing an example embodiment where the device is a payment card for public transportation). Accordingly, *Palmer* is in the same field of endeavor as and is analogous art to the '333 Patent. *Dec.*, ¶¶69-73.

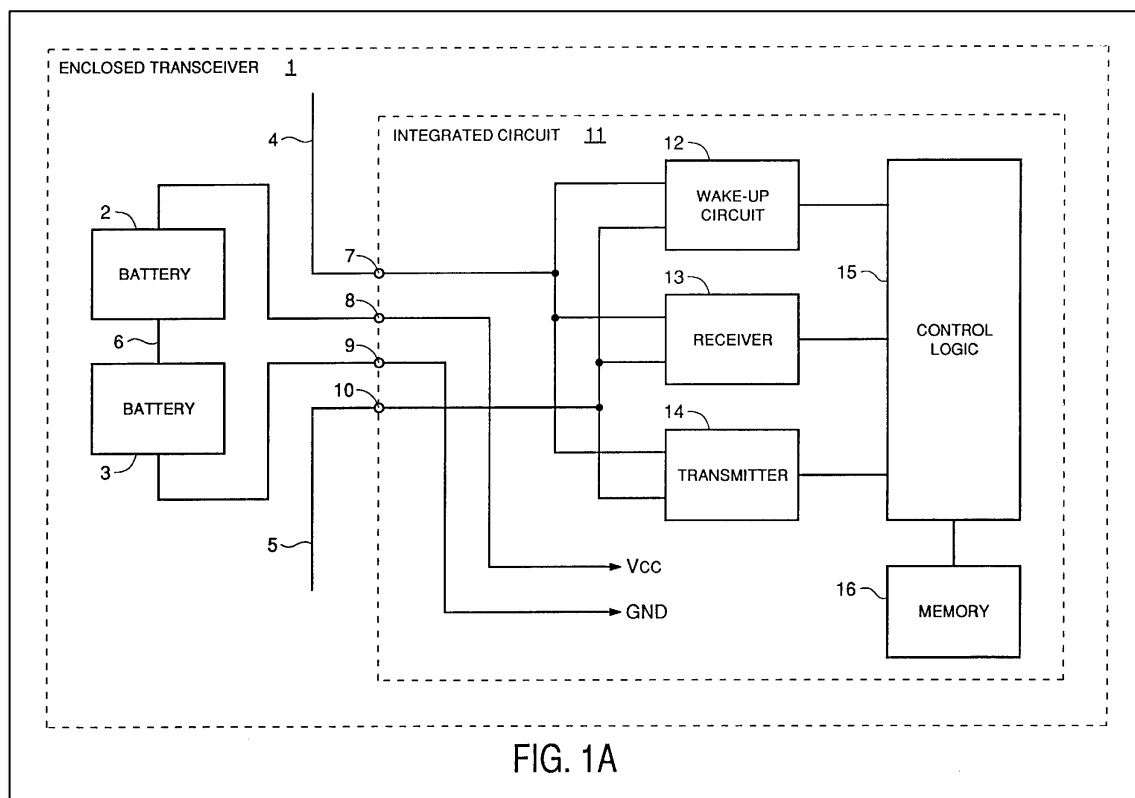
C. Overview of *Tuttle*

U.S. Patent No. 6,078,791 to Tuttle and Lake ("*Tuttle*") issued on June 20, 2000, and is prior art to the '333 Patent under at least 35 U.S.C. §102(b) (pre-AIA).

⁴ Although *Palmer* teaches that the RF field powers the device, *Palmer* expressly contemplates battery powered implementations that do not depend on inductive power. *Palmer*, [0043] ("[A] rechargeable battery may power the electronic components when no RF energy field is present.").

Tuttle (Ex. 1006), (45). *Tuttle* was neither cited nor discussed during prosecution of the '333 Patent. '333 Patent, (56).

Tuttle discloses “a non-contact method of object and person detection and location which can serve as a replacement for metal-to-metal contact in smart card applications.” *Tuttle*, 3:52-57. Specifically, *Tuttle* describes an enclosed transceiver 1 (shown in Fig. 1A) that “includes a pair of batteries 2 and 3, a dipole antenna 4 and 5, and an integrated circuit (IC) 11.” *Tuttle*, 5:67-6:2.



Tuttle, Fig. 1A. “Integrated circuit 11 is a transceiver including wake-up circuit 12, receiver 13, transmitter 14, control logic 15, and memory 16.” *Tuttle*, 6:14-16. Wake-up circuit 12 detects the existence of and processes a wireless signal, enabling

receiver 13 to receive and decode data in a signal, and transmitter 14 transmits data in a wireless signal. *Tuttle*, 6:17-30; (teaching that the wake-up circuit detects the energy of a transmitted wireless signal in an appropriate frequency band); *see also id.*, 7:4-16 (teaching that wake-up circuit processes initial “interrogation signals” before receiver 13 and transmitter 15 are able to exchange data with an interrogator device).

Both *Tuttle* and the '333 Patent are directed to portable electronic devices. *Compare Tuttle*, 3:52-57 (disclosing a smartcard for entering into a secured area), *with '333 Patent*, 8:42-50 (discussing example embodiment where the device is an electronic passport). Accordingly, *Tuttle* is in the same field of endeavor as and is analogous art to the '333 Patent. *Dec.*, ¶¶74-76.

IV. PROCEDURAL REQUIREMENTS UNDER 37 C.F.R. § 42.104

A. Standing Under 37 C.F.R. § 42.104(a)

Petitioner certifies that the '333 Patent is available for IPR and that Petitioner is not barred or estopped from requesting an IPR challenging the claims of the '333 Patent. Specifically, (1) Petitioner is not the owner of the '333 Patent, (2) Petitioner has not filed a civil action challenging the validity of the claims of the '333 Patent, and (3) this Petition is filed less than one year after the Petitioner was served with a complaint alleging infringement of the '333 Patent.

B. Challenge Under 37 C.F.R. § 42.104(b) and Relief Requested

In view of the prior art and evidence presented, Claims 1-13 of the '333 Patent are unpatentable and should be cancelled. 37 C.F.R. § 42.104(b)(1). Further, based on the prior art references identified below, IPR of the Challenged Claims should be granted. 37 C.F.R. § 42.104(b)(2).

Proposed Grounds of Unpatentability	Exhibits
<u>Ground 1:</u> Claims 1, 2, and 4-10 are obvious under pre-AIA 35 U.S.C. §103 over U.S. Patent Application Publication No. 2002/0180584 to McGregor et al. (" <i>McGregor</i> ") in view of U.S. Patent Application Publication No. 2003/0226041A1 to Palmer et al. (" <i>Palmer</i> ").	Ex. 1004 Ex. 1005
<u>Ground 2:</u> Claims 3 and 11-13 are obvious under pre-AIA 35 U.S.C. §103 over <i>McGregor</i> in view of <i>Palmer</i> and in further view of U.S. Patent No. 6,078,791 to Tuttle and Lake (" <i>Tuttle</i> ").	Ex. 1004 Ex. 1005 Ex. 1006

Section V identifies where each element of the Challenged Claims is found in the prior art. 37 C.F.R. § 42.104(b)(4). The exhibit numbers of the evidence relied upon to support the challenges are provided above and the relevance of the evidence to the challenges raised is provided in Section IV. 37 C.F.R. § 42.104(b)(5). Exhibits 1001-1019 are also attached.

C. Claim Construction Under 37 C.F.R. § 42.104(b)(3)

In this proceeding, claims are interpreted under the same standard applied by Article III courts (i.e., the *Phillips* standard). *See* 37 C.F.R § 42.100(b); *see also* 83

Fed. Reg. 197 (Oct. 11, 2018); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (*en banc*). Under this standard, words in a claim are given their plain meaning, which is the meaning understood by a person of ordinary skill in the art in view of the patent and file history. *Phillips*, 415 F.3d 1303, 1312–13. Petitioner submits that all terms be given their plain and ordinary meaning consistent with the *Phillips* standard. Petitioner does not waive any argument in any litigation that claim terms in the '333 Patent are indefinite or that additional terms need construction.

i. “*Invariable Activation Command*”

Independent claims 1 and 11, recite an “invariable activation command[.]” ’333 Patent, 9:65-67, 10:17-18, 12:8-10. The specification of the ’333 Patent describes multiple examples of an “invariable action command” in the context of a device capable of alternate data conveyance operations. In each instance, the command “activates” a data transfer and is “invariable” in that the user cannot control which path the subsequent data transfer follows. Instead, the state of a switching element dictates the data path. Because the Proposed Grounds teach an activation command that cannot be varied by the user (i.e., the decision to exchange data with an external device or to convey data within the device, is determined by the detected presence of an activation cue, rather than by the user), Petitioner does not believe an express construction of this phrase is required to resolve the issues

presented herein.⁵ Instead, the phrase should be interpreted broadly enough to capture the consistent meaning ascribed to it by the intrinsic record. As set forth below, the intrinsic record repeatedly and consistently describes an invariable activation command as a command to transmit data through either a first or second data conveyance operation, where the decision of which operation to use is outside of user control.

In a first example, the '333 Patent describes an invariable activation command that initiates a data transfer and stresses that the user will not be able to manually override the command:

In the case *where no activation cue was received* by portable electronic device 10, *data will be communicated to* the portable electronic device holder by means of *user interface device 16*. However, *if an activation cue was previously received* by portable electronic device 10, *a data exchange will be initiated between portable electronic device 10 and data exchange device 9*.

It is noted that, according to the present invention, *the activation command issued when control device 12 is triggered, is an invariable activation command*. That is to say that *the portable electronic device*

⁵ The Board “only construe[s] terms ‘that are in controversy, and only to the extent necessary to resolve the controversy[.]’” *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Ltd. Matal*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

holder will not be able to select to issue different activation commands

by means of control device 12 depending on whether the user considers that a data exchange operation should be accomplished with an external data exchange device 9, or whether the user wishes to display information on screen 16 on the basis of data stored in memory 42. The same invariable activation command will thus be issued upon control device 12 being triggered, and ***it is the state of switching element 44b***, resulting from the receipt or non-receipt of an activation cue by portable electronic device 10, ***that will be decisive as to the type of data conveyance that will occur.***

'333 Patent, 7:7-29.

In an example use, a user may accomplish a “quick payment” by receiving an activation cue from an exchange device, in this case, a payment debit machine. The user “could then trigger his control device” to authorize the portable electronic device. '333 Patent, 7:55-8:5. Triggering the control device issues an invariable activation command. '333 Patent, 7:15-17. At this point, the payment is made by transmitting data or displaying data on the display screen, depending on the reception of an activation cue or lack thereof. '333 Patent, 8:1-9, 8:24-29. In this example, “upon triggering control device 12, an invariable activation command would be issued that would result in two different possible data conveyance operations[.]” '333 Patent, 8:32-35. From this example, it's clear that the invariable

action command has the purpose of conveying data without allowing the user control over how the data is conveyed.

This definition is bolstered by arguments made in the prosecution of U.S. Patent No. 9,022,294, a continuation-in-part of the '333 Patent. There, the applicant stressed that the term “invariable” means the control device cannot determine which data path is used:

It is recalled that the gist of the present invention is to *provide a device that may issue one of two data conveyance operations responsive to an invariable command issued by a user-triggered control device, depending on whether or not an external cue has been received*. This provides the advantages of: (1) the user specifically controlling when the data conveyance operations will occur, since the user will trigger the control device himself; while (2) *simultaneously avoiding the need for the user to decide which conveyance operation will occur, since the electronic circuit will decide this for the user*.

Ex. 1007 ('294 File History), 124.

In light of the full intrinsic record, an “invariable activation command” should be interpreted broadly enough to capture a command to transmit data through either a first or second data conveyance operation, where the decision of which operation to use is outside of user control. The Petitioner reserves its rights to more concretely define this term in the parallel litigation.

V. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Ground 1: Claims 1, 2, and 4-10 are obvious under pre-AIA 35 U.S.C. § 103 over *McGregor* in view of *Palmer*

McGregor teaches a bio-metric smart card device that, upon authenticating a user's biometric data, generates and displays a security code that is used by the transaction network to approve the transaction. *McGregor* expressly teaches that the device can also be equipped with a wireless transceiver for *automatically* communicating the security code to the transaction network. However, *McGregor* doesn't describe the transmission hardware contemplated or how the system determines when to automatically transmit the security key. The proposed combination establishes that a POSITA would have been motivated to modify *McGregor's* device pursuant to *Palmer's* hardware and its process for determining when automatic wireless communications are possible, automatically transmitting a security code when the device detects the existence and availability of an external device. As explained below, the proposed modification would have resulted in a device with improved security.

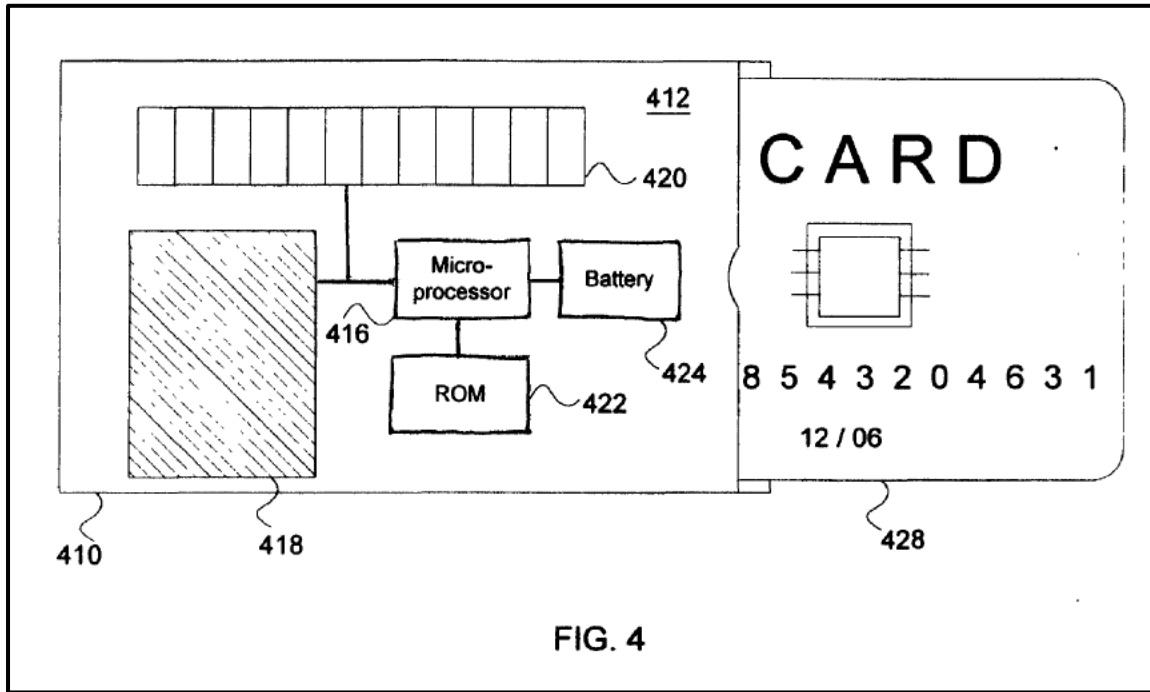
i. Claim 1

[1(Pre)] A portable electronic device, comprising:

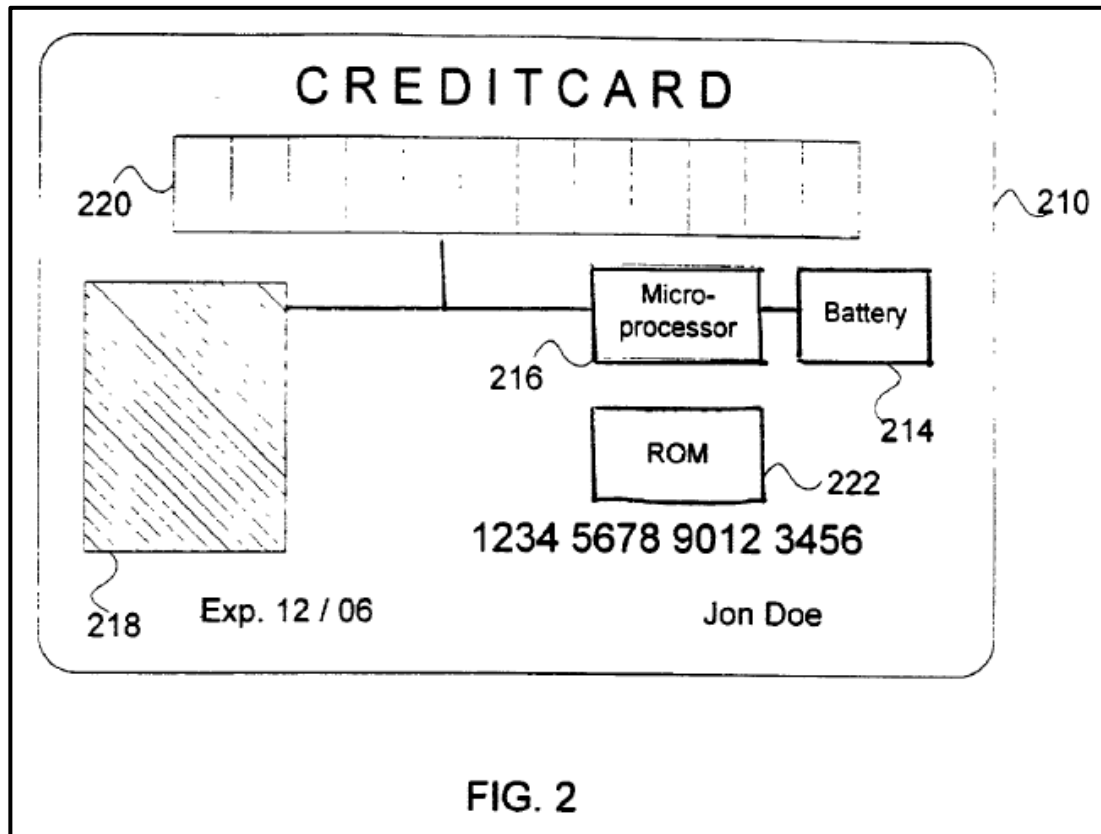
To the extent the preamble is limiting, *McGregor* discloses a portable electronic device. *Dec.*, ¶¶78-80.

The '333 Patent expressly contemplates the portable electronic device having the form factor of a card (*see* '333 Patent, Figs. 1-3) and containing components common to smart cards. '333 Patent, 4:61-62; *see also id.*, 7:55-8:41 (discussing embodiment where the portable electronic device is a payment card). *McGregor* similarly teaches a portable bio-metric smart card reader 410 (referred to as a “wallet”) with “substantially the same shape and form factor as available plastic credit and debit cards[.]” *McGregor*, [0043]; *see also id.*, [0037].⁶ Wallet 410 includes electronic components such as “fingerprint scanner 418 in electrical communication with a microprocessor 416.” *Id.*, [0043]; *see also id.*, [0037]. “A battery [424] may also be connected to provide power to microprocessor 416.” *Id.*, [0043]; *see also id.*, [0037]. Wallet 410 also includes a memory, specifically a “ROM 422, preferably an EEPROM,” and a display 420. *Id.*, [0043]-[0044]; *see also id.*, [0037]-[0038]. Wallet 410 is depicted in Fig. 4 below:

⁶ Both *McGregor*’s bio-metric smart card embodiment as depicted in Fig. 2 and its bio-metric smart card reader (wallet) embodiment as depicted in Fig. 4 satisfy the claims and are captured by the Proposed Grounds. To focus the discussion, Petitioner highlights the Fig. 4 wallet embodiment in its mapping and includes parallel citations to the Fig. 2 embodiment.



McGregor, Fig. 4. In a separate embodiment, *McGregor* teaches bio-metric smart card 210 that includes the same relevant components as reader 410. *Id.*, [0037] (describing smart card equipped with ROM 222, microprocessor 216, battery 214, and display 220).



Id., Fig. 2.

[1(a)] an electronic circuit capable of storing data therein, capable of processing data, and capable of data input and output;

McGregor discloses this limitation. *Dec.*, ¶¶81-84. For example, wallet 410 comprises electrical components, including battery 424, ROM 422, and microprocessor 416. *See* Fig. 4, [0043]-[0044]; Claim 1(Pre). Collectively, these components comprise an electronic circuit, as claimed. *Id.*

As part of the electronic circuit, ROM stores data, including “fingerprint or other bio-metric data, the encryption keys, and a transaction counter.” *McGregor*, [0043]; *see also id.*, [0037].

McGregor's microprocessor is capable of processing data, accepting data input, and outputting data. For example, the microprocessor accepts a fingerprint input, processes data to generate a security key, and outputs that security key data (e.g., wirelessly to a transaction network and/or to the display). *See, e.g., McGregor*, [0038-39]⁷ (teaching a security key code is generated in the microprocessor and then displayed on the card), [0044] (“Finger print scanner 418 . . . is connected to the microprocessor 416 to provide an input signal[.] [D]isplay 420 is configured to display dynamic numeric and/or textual data forwarded by microprocessor 416[.]

⁷ Although *McGregor* teaches that the microprocessor in its Fig. 2 embodiment generates a security key code, it does not expressly teach the microprocessor in its Fig. 4 embodiment is similarly responsible for generating a security key code. A POSITA would have understood that the Fig. 4 microprocessor does in fact generate a security key code. *Dec.*, ¶84. Where *McGregor* does describe generating a security key code, it is generated by the microprocessor after receiving a fingerprint input and confirming it matches. *See, e.g., McGregor*, [0013], [0039]-[0041], [0046], [0065]. Because *McGregor* expressly teaches that Fig. 4's microprocessor *receives* a fingerprint input and *outputs* a generated security key code (*id.*, [0044]), a POSITA would understand that the same microprocessor generated the security key code. Additionally, *McGregor* at [0044] teaches that its Fig. 4 embodiment implements the Fig. 3 flowchart, which expressly describes the microprocessor generating a security key code. *Dec.*, ¶84.

The wallet may include an IR or wireless transmitter to automatically transmit the security code to a transaction network.”); *Dec.*, ¶¶84.

[1(b)] a control device operatively linked to said electronic circuit, with an invariable activation command being issued when said control device is selectively triggered;

McGregor in view of *Palmer* teaches this limitation. *Dec.*, ¶¶85-109.

As discussed in Section IV.C, “invariable activation command” should be construed broadly enough to capture a command to transmit data through either a first or second data conveyance operation, where the decision of which operation to use is outside of user control. *McGregor* teaches a control device (e.g., fingerprint scanner 418) that is triggered by a user (e.g., a user entering their biometric data), causing a microprocessor to issue a command to display data (e.g., a security key code) and/or to automatically transmit that same data wirelessly. But *McGregor* does not describe the automatic wireless transmission functionality in detail. For example, it does not explain how the device determines whether to automatically transmit the data in lieu of (or in addition to) displaying the data. It also does not describe the transmission hardware used to accomplish this wireless transmission. The proposed combination relies on *Palmer*’s teachings for these implementation details. Namely, the combination proposes that a POSITA would have been motivated to modify *McGregor* pursuant to *Palmer* such that *McGregor*’s device automatically transmits its security key code when the device confirms the ***existence and availability*** of a

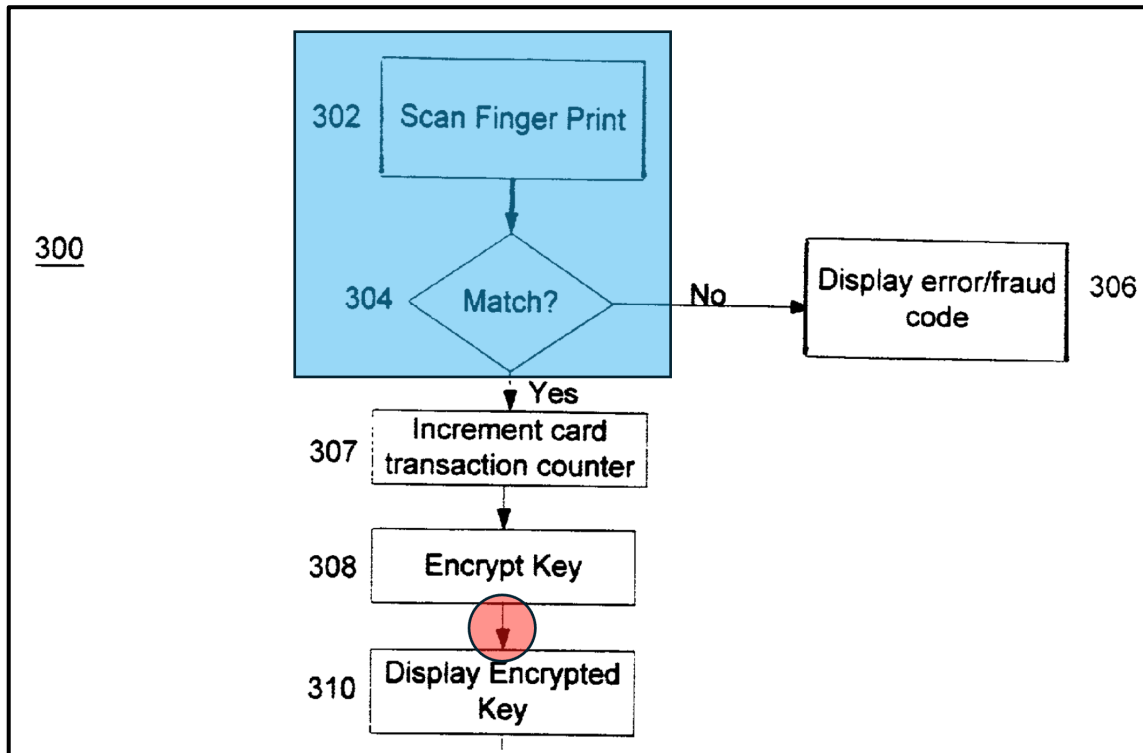
reader/writer device able to receive the code. The combination further proposes incorporating *Palmer's* transmission hardware into *McGregor's* device.

McGregor's User Authentication and Security Key Conveyance

McGregor discloses a control device operatively linked to said electronic circuit in the form of a “finger print scanner 418 . . . connected to the microprocessor 416[.]” *McGregor*, [0044]; *see also id.*, [0037]; *See* claim 1(a). The fingerprint scanner 418 is selectively triggered when “the user plac[es] a thumb or finger upon the surface of scanner 418[.]” *McGregor*, [0044]; *see also id.*, [0037], [0040] (noting the scan is compared to “a reference file representative of the user’s actual print”); *Dec.*, ¶88. A POSITA would have understood that the user engaging a fingerprint scanner to initiate the authentication and data conveyance process is selectively triggering, as claimed. *Dec.*, ¶¶88-89 (noting the ’333 Patent at 5:5-19 describes a “device holder [] selectively trigger[ing] a data conveyance operation” by pressing a button or entering a fingerprint using a “fingerprint scanner” and concluding a POSITA would understand *McGregor* teaches a similar process where its user intentionally initiates an authentication and data conveyance by entering a fingerprint via scanner 418).

If the fingerprint scan is a match, “the microprocessor . . . generates [] a numeric or alphanumeric security key.” *McGregor*, [0041]. Once generated, the security key is sent to display 420, allowing the user to input (or otherwise forward)

the security key to authorize a transaction. *McGregor*, [0041]. Fig. 3 shows the fingerprint scanner 418 (i.e., control device) being selectively triggered in steps 302-304 (annotated in blue) and the security key being sent to the display prior to step 310, where the key is displayed. *McGregor*, Fig. 3.⁸



⁸ Fig. 3 and its relevant discussion in the specification are focused on and use the numbering of smartcard embodiment 210. These teachings equally apply to the wallet 410 embodiment. *McGregor*, [0044] (“The display 420 is configured to display dynamic numeric and/or textual data forwarded by microprocessor 416, and is intended to accompany the account number for all transactions in the manner outlined above with reference to FIG. 3.”); *Dec.*, ¶90 (noting that a POSITA would have understood that Fig. 3’s flowchart and corresponding description apply to both the Fig. 2 card embodiment and Fig. 4 wallet embodiment).

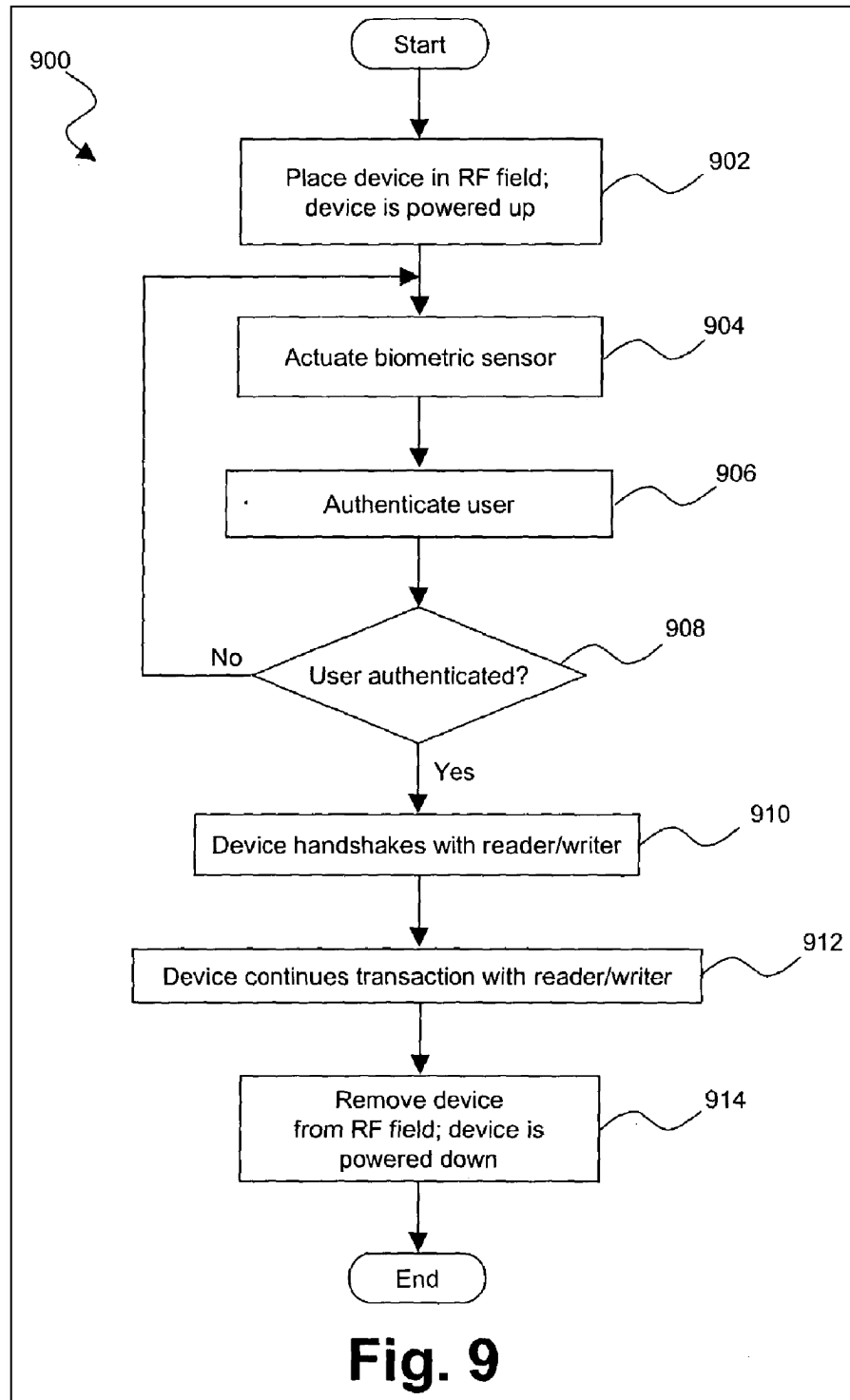
McGregor, Fig. 3, excerpt, annotated.

McGregor also teaches that the device may be equipped with “an IR or wireless transmitter to automatically transmit the security code to a transaction network.” *McGregor*, [0044]. However, *McGregor* does not elaborate on how or when such automatic transmission would occur. Given *McGregor*’s silence on how this feature would be implemented, a POSITA would have looked to teachings in the art to guide its implementation. For a number of reasons discussed below, a POSITA would have been motivated to implement *McGregor*’s device pursuant to *Palmer* such that the security code would be automatically transmitted when the device detects the existence and availability of an external reader/writer device available to receive the security code.

Palmer’s RF Field Detection, Handshake Process, and Wireless Transmission

Like *McGregor*, *Palmer* teaches a device takes the “form factor similar to that of a credit card[,]” containing a fingerprint sensor, RF antenna, and a display. *Palmer*, [0030]. Also, like *McGregor*, *Palmer*’s device is used to authenticate its user via biometrics (e.g., a fingerprint) to facilitate and secure a financial transaction. *Palmer* describes a process through which its device is placed within the RF field of a financial transaction reader/writer device, triggering the authentication process that includes (1) authenticating a user’s fingerprint, (2) a handshake communication between the device and reader/writer, and (3) a two-way communication between

the user device and the reader/writer device furthering a transaction. Fig. 9 illustrates this process:



Id., Fig. 9. As illustrated, the device is placed in the reader/writer's RF field at step 902,⁹ a user is authenticated using a fingerprint sensor at steps 904-906, the device performs a handshake process with the reader/writer at step 910 after authenticating the user's fingerprint, and then the device wirelessly exchanges data with the reader/writer device to "continue[] the desired transaction[.]" *Id.*, [0050-51]; *Dec.*, ¶92.

A POSITA would have known that handshakes were well-established in computer science as a back-and-forth communication between two devices, often used to establish a set of encryption keys used to secure subsequent communications between the devices. *Dec.*, ¶93. Although *Palmer* does not go into detail about the specific signals exchanged in its contemplated handshake, consistent with the common purpose of a handshake, it teaches that communications "between the device [] and the reader/writer device . . . may be secured using mechanisms such as data encryption." *Palmer*, [0023], [0033] (noting the device "may perform various encryption functions to support secure communications"); *Dec.*, ¶93-94.

⁹ Although *Palmer* teaches that the RF field powers the device, *Palmer* expressly contemplates battery powered implementations that do not depend on inductive power. *Palmer*, [0043] ("[A] rechargeable battery may power the electronic components when no RF energy field is present.").

Proposed Combination of *McGregor* and *Palmer* and Motivation to Combine *McGregor* and *Palmer*

A POSITA would have been motivated to implement *Palmer's* (1) RF field detection and handshake processes and (2) *Palmer's* transceiver hardware in *McGregor's* device. Specifically, *Palmer's* process of identifying an RF field generated by a reader/writer device and establishing a two-way communication link with that device would be implemented to dictate when *McGregor's* wallet device should “automatically transmit the security code to a transaction network.” *Dec.*, ¶¶95-105. When no RF field is detected and no two-way communication link is established, *McGregor's* device exclusively displays the security key code on the device's display for the user to manually enter/forward. *Id.* A POSITA would have been motivated to make this modification for a number of reasons.

First, the proposed combination applies *Palmer's* known technique to implement *McGregor's* device, which is ready for improvement, yielding predictable results. Namely, a POSITA would have recognized that *Palmer's* process of detecting an RF field and handshaking with the reader to determine whether short-range wireless communications are possible was a well-established practice. *Id.*, ¶¶95-96. A POSITA would also have recognized that, by failing to describe how its wallet device “automatically transmit[s] the security code to a transaction network[,]” *McGregor* is ready for improvement, i.e., guidance from the art as to how this automatic transmission would be implemented. *Id.*, ¶¶95-97.

Finally, detecting the existence of an RF field and handshaking as a threshold for establishing a two-way communication link over which to communicate a security code would have yielded obvious results. *Id.* It is well-accepted practice in the field of communications that a communication link should be setup and confirmed operable before transmitting data. *Id.*, ¶¶95-98. Further, the practice of handshaking to ensure secure communications would have similarly yielded predictable results, given the prevalence of handshaking in secure data communications at the time. *Id.*, ¶¶95-99.

Second, a POSITA would have recognized that implementing *Palmer's* process into *McGregor's* wallet would improve *McGregor's* similar device in the same way it benefits *Palmer*. *Dec.*, ¶100. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007) (“[I]f a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious[.]”). In both systems, detecting an RF field as a precursor to setting up a two-way communication link to exchange transaction-related data ensures the external reader-writer device is in-range, operable, and available to receive the data before the data transmission is attempted. *Dec.*, ¶100. Further, performing a handshake process to ensure data exchanged is secure would have benefitted *McGregor* in the same way it benefits *Palmer*. *Id.* A POSITA would have expected these benefits to apply to *McGregor's* system in the

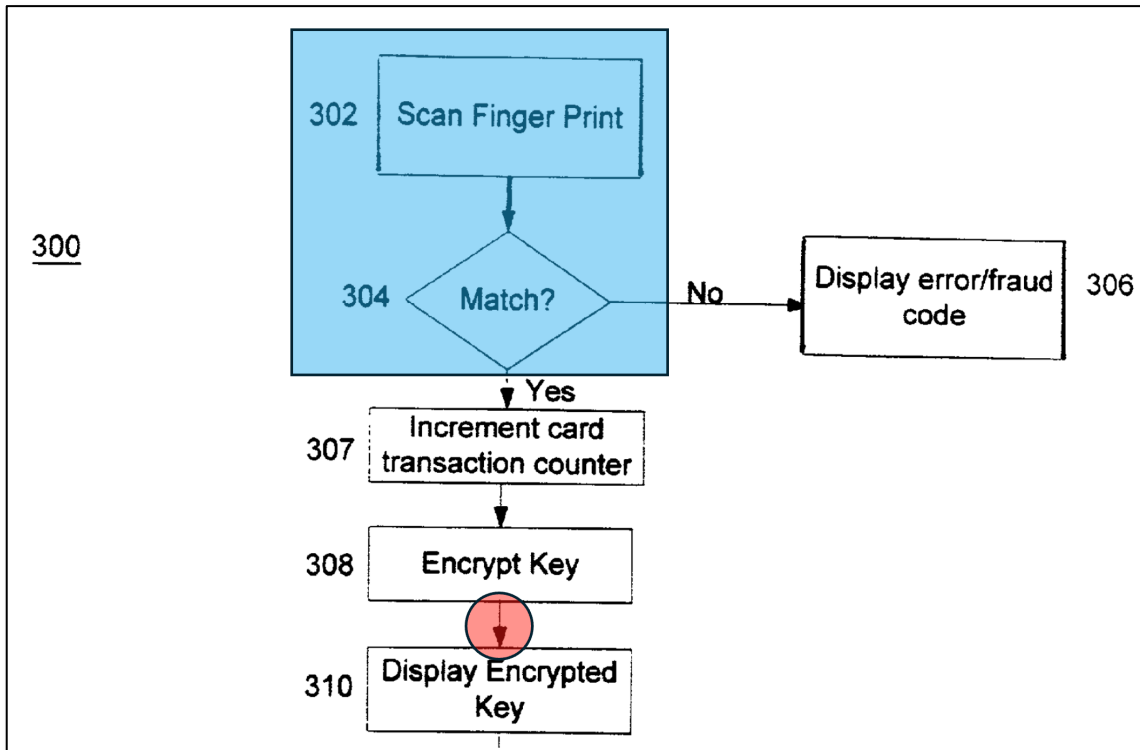
same way they apply to *Palmer's* given their similarities in structure and function. *Dec.*, ¶¶100-101. Indeed, both systems utilize portable electronic devices, sized similarly to credit cards, which utilize biometric user validation to perform financial transactions. *Compare McGregor*, [0012], [0037], *with Palmer*, [0002], [0061], [0030]; *Dec.*, ¶¶100-101. Further, the reader of *McGregor* and reader/writer of *Palmer* are both external devices used to process financial transactions. *Compare McGregor*, [0012], [0039], *with Palmer*, [0029], [0051]; *Dec.*, ¶¶102-103 (explaining that financial transactions were well known to require security, which *Palmer's* handshake process enables).

Finally, such modifications would have been well within a POSITA's skill, supporting a reasonable expectation of success. *Dec.*, ¶¶104-105. First, as discussed above, *McGregor* and *Palmer* describe starkly similar systems, both of which use card-based devices to communicate wirelessly with transaction network reader/writer devices. *Id.*, ¶104. Regarding *Palmer's* hardware, given the similar form factors and functionalities, a POSITA would have expected to easily incorporate *Palmer's* transceiver hardware in *McGregor's* device. *Id.* It would also have been a straightforward implementation of *Palmer's* teachings in *McGregor's* system to first detect an RF field and establish a two-way communication link over which a handshake process can proceed before "automatically transmit[ing] the security code to a transaction network." *Id.*, ¶¶104-105.

McGregor's Microprocessor Issues an Invariable Activation Command in the Proposed Combination

As discussed in Section IV.C, “invariable activation command” should be construed broadly enough to capture a command to transmit data through either a first or second data conveyance operation, where the decision of which operation to use is outside of user control. In the Proposed Combination, after a user enters their fingerprint and a security key code is generated, *McGregor's* microprocessor causes the security key code to be displayed on the card and/or transmitted through a wireless network if an RF field is detected and a two-way communication link established. Because these distinct data paths are determined by the RF field detection process, rather than by user choice, the data transmission command issued by *McGregor's* microprocessor is invariable, as claimed. *Dec.*, ¶106. In other words, the user has no ability to prevent the automatic wireless transmission if the device has established a communication link with the reader/writer device. *Id.*

McGregor teaches that the transition from step 308 to step 310 within *McGregor's* Fig. 3 demonstrates that when the security key is created, it is automatically displayed without any additional user input.



McGregor, Fig. 3 (annotated); *Dec.*, ¶¶107. In the modified device, the invariable activation command generated by *McGregor*'s microprocessor would cause the security key code to be wirelessly transmitted instead of displaying *or* in addition to displaying. *Dec.*, ¶¶107-108. While the claims do require transmitting data when an activation cue has been received (e.g., when handshake signals are exchanged), they do not exclude a device that both displays and transmits its data when an activation cue has been received. *Id.* Accordingly, whether *McGregor*'s device automatically transmits the security key code instead of or in addition to displaying that data does not impact the Proposed Grounds. *Id.*

[1(c)] a user interface device operatively linked to said electronic circuit;

McGregor discloses this limitation. *Dec.*, ¶¶109-111.

McGregor discloses a display 420 that is “configured to display dynamic numeric and/or textual data forwarded by microprocessor 416[.]” *McGregor*, [0044]; *see also id.*, [0038]. Specifically, display 420 displays the security key after a user has been authenticated via the fingerprint scanner. *McGregor*, [0040], [0041]. A POSITA would understand that display 420 is a user interface device at least because it communicates data to the user. *Dec.*, ¶¶109-110. Finally, display 420 is operatively linked to the said electronic circuit, as claimed, because it displays data received from microprocessor 416, which is part of the electronic circuit. *See Claim* [1(a)]; *Dec.*, ¶¶110-111.

[1(d)] a data transceiver operatively linked to said electronic circuit, said data transceiver being for exchanging data between said electronic circuit and an external data exchange device, and for receiving a selectively emitted activation cue from a source external to said portable electronic device;

As set forth above with reference to limitation [1(b)], the Proposed Combination relies on *McGregor*’s modified wallet device exchanging data (e.g., security key code) with an external data exchange device (e.g., reader/writer device) when a selectively emitted activation cue (e.g., one or more handshake signals received from the reader/writer device) is received from a source external to the portable electronic device (e.g., the reader/writer device).

A data transceiver operatively linked to said electronic circuit.

McGregor in view of *Palmer* teaches this limitation. *Dec.*, ¶¶113-115. *McGregor* discloses that wallet 410 can send the security key “directly [] via IR or

other wireless technology” via an “IR or wireless transmitter[.]” *McGregor*, [0053], [0044]. The combination implements *Palmer*’s hardware and techniques to achieve the wireless transmission contemplated by *McGregor*. See Claim [1(b)]. *Palmer*’s device 400 includes an RF antenna 404 and smartcard chip 408 that “support two-way communication” with external devices. *Palmer*, [0033], [0043]. A POSITA would have understood that the smartcard chip 408 receives and sends data through the RF antenna 404 to facilitate two-way communication. *Dec.*, ¶¶114-115. Further, the RF antenna 404 and smartcard chip 408 would be operatively connected to *McGregor*’s electronic circuit to function as intended. This configuration allows the modified *McGregor* device to transmit the security key generated by the microprocessor 416 via RF. *Id.*, ¶115. Thus, *Palmer*’s smartcard chip 408 is a data transceiver operatively linked to *McGregor*’s electronic circuit. *Id.*

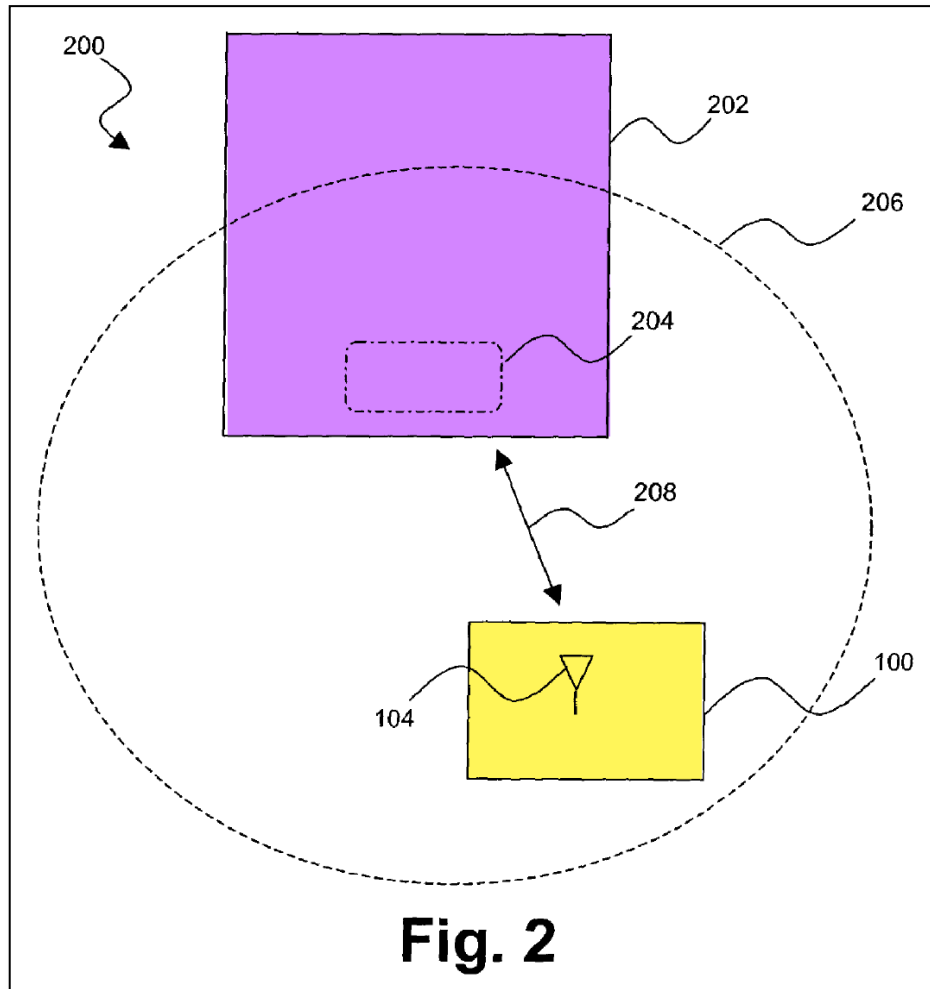
Said data transceiver being for exchanging data between said electronic circuit and an external data exchange device

McGregor teaches that the wallet “may include an IR or wireless transmitter to automatically transmit the security code to a transaction network.” *McGregor*, [0044], [0053]. A POSITA would understand an IR transmitter is limited in range and, therefore, must communicate with a nearby short-range base station to transmit the security code to the transaction network. *Dec.*, ¶¶116-117 (explaining that a POSITA would have understood *McGregor*’s automatic transmission to be accomplished via IR or other short-range communication technology). *McGregor*

teaches retailer-based readers connected to the transaction network to facilitate short-range communications with the portable device. *McGregor*, [0039] (“The displayed security key is [] communicated or transmitted to the credit card authorization service [] through a reader[.]”)¹⁰, *Dec.*, ¶¶118 (explaining that a reader or other merchant device capable of short-range communication wirelessly receives the security key code from *McGregor*’s wallet device).

Palmer teaches a reader device consistent with that described by *McGregor*. Namely, *Palmer*’s reader/writer device 202 is an example of a short-range communication capable reader device designed to (1) communicate wirelessly with a smart card and (2) to communicate transaction data with the transaction network. *Palmer*, [0027-28] (teaching that reader/writer device 202 communicates wirelessly with smart card devices and is also connected to a network). Fig. 2 of *Palmer* shows the relationship between reader/writer device 202 and a portable electronic device 100:

¹⁰ A POSITA would have understood that the reader discussed in *McGregor* [0039] is a point-of-sale card reader (called a retailer-based reader throughout this petition) operated by a retailer to perform in-person retail transactions. *Dec.*, ¶118. Further, a POSITA would understand that, in both the wallet embodiment of Fig. 4 and the smart card embodiment of Fig. 2, the devices communicate data with a retailer-based reader to perform in-person financial transactions (compared to telephone or online transactions, as discussed in *McGregor* [0039]). *Dec.*, ¶118.



Palmer, Fig. 2 (annotated). As illustrated, “exemplary environment 200” “enables contactless interaction” between reader/writer device 202 (annotated in purple) and device 400 (annotated in yellow) via “a two-way communication link 208[.]” *Palmer*, [0027]. This contactless interaction includes a “communications handshake process” and continuing “the desired transaction” (each a data exchange) between device 400 and the external reader/writer 202 “via a contactless two-way communication link.” *Palmer*, [0051].

To the extent Patent Owner disputes that *McGregor* teaches an external data exchange device for wirelessly communicating with its wallet device, a POSITA would have been motivated and found it obvious to implement *McGregor*'s system with the reader/writer 202 described in *Palmer. Dec.*, ¶¶120-121. Indeed, a POSITA would have recognized that *Palmer*'s reader/writer device 202 is a reader device that serves the same purpose as the reader contemplated by *McGregor*—wirelessly communicating with a smart card device and exchanging data with the transaction network. *Id.* The motivations to make this additional modification to *McGregor* are the same as those set forth with reference to limitation [1(b)]. *Id.* (explaining that the motivations for modifying *McGregor*'s system pursuant to *Palmer*'s RF field detection and handshake processes and transmission hardware also motivate implementing *Palmer*'s reader/writer device as an exemplary device through which *McGregor*'s wireless communications would occur).

For receiving a selectively emitted activation cue from a source external to said portable electronic device.

The '333 Patent does not define “selectively emitted[.]” The term is not used outside the claims and summary of the invention, which simply restates the claim language. The patent's use of “selectively” in other contexts, however, provides insight into the meaning of “selectively emitted[.]” For example, the patent repeatedly describes a user “selectively” triggering a data conveyance. *See '333 Patent*, 5:5-7, 6:42-65. In this context, “selectively” appears to mean that some

specific action occurs to cause the event, e.g., the user engages the device to trigger a data conveyance.

Applying the same logic to a “selectively emitted activation cue[,]” this phrase should require some intervening action that causes the activation cue to be transmitted. Even under this interpretation, the Proposed Combination satisfies the limitation. Namely, as set forth with reference to limitation [1(b)], *Palmer’s* process first detects an RF field and then engages in a handshake process in which data is exchanged between the smart card device and reader/writer device. At least because the activation cue (e.g., the one or more handshake signals that establish a communication link) are sent in response to the user bringing the smart card device within the RF field and in response to the smart card device initiating the handshake process, *Palmer’s* process satisfies the claims “selectively emitted activation cue” language. *Dec.*, ¶¶122-124. That is, there are multiple intervening acts that cause the reader/writer device to emit its activation cue (e.g., handshake signals). *Id.*

[1(e)] a data conveyance switching element operatively linked to said electronic circuit, said switching element being in an activated state upon an activation cue having been received by said data transceiver, and being in an inactive state when no activation cue was received by said data transceiver; and;

McGregor in view of *Palmer* teaches this limitation. *Dec.*, ¶¶125-127. This limitation requires a switching element that is either an activated state or inactivated state, depending on whether an activation cue is received. The ’333 Patent states that “switching element 44b can be a physical structure, a virtual program, or both.” ’333

Patent, 6:16-17; *see id.*, 6:11-12 (teaching that the element can be “a series of instructions programmed onto the microchip”).

McGregor’s device modified pursuant to *Palmer*’s processes satisfies this limitation. Namely, as discussed above with reference to limitation [1(b)], *McGregor*’s microprocessor is responsible for transmitting a security key code to the device’s display and/or automatically transmitting the code in the event a wireless reader/writer device has been detected and a handshake operation has been performed (pursuant to *Palmer*’s teachings). Accordingly, *McGregor*’s microprocessor is a switching element (1) that is placed into an activated state after receiving a handshake signal (an activation cue) that establishes a communication during the handshake process and (2) that remains in an inactivated state if no reader/writer device is detected. *Dec.*, ¶¶125-127.

[1(f)] power means for providing power to said portable electronic device;

McGregor discloses this limitation. *Dec.*, ¶¶128-129. For example, *McGregor* discloses “[a] battery [] connected to provide power to microprocessor 416.” *McGregor*, [0043]; *see also id.*, [0037]. Alternatively, *McGregor* contemplates other forms of power: “movement of card reader 410 (as with an automatic watch) or contact of the card or by a solar panel.” *McGregor*, [0043]; *see also id.*, [0037]. The battery 424 or alternative source of power is connected to the microprocessor 416,

which is a part of the electronic circuit of the wallet 410. *See* claim 1(pre); *McGregor*, [0043]; *see also id.*, [0037].

[1(g)] wherein upon said control device being selectively triggered to issue an[] invariable activation command: if said switching element is in said activated state, a data exchange will be initiated through the instrumentality of said data transceiver for exchanging data between said electronic circuit and an external data exchange device;

The combination of *McGregor* and *Palmer* teaches this limitation. *Dec.*, ¶130. As set forth in the preceding limitations, *McGregor* modified based on the teachings of *Palmer* automatically transmits a security key code to an external reader device after an RF field of the wireless reader/writer device has been detected, a user enters their fingerprint for authorization (i.e., selectively triggers the device to send data), and a handshake operation is completed between *McGregor's* device and the reader/writer device. When the RF signal is detected and a handshake signal is received (cue signal) establishing a communication link, *McGregor's* microprocessor (i.e., switching element) is placed in an activated state. As discussed with reference to limitation [1(b)], the command issued by *McGregor's* microprocessor to convey the security key code is “invariable” in that the microprocessor being in an activated state dictates how the data is conveyed, rather than providing any user control over the conveyance. *Dec.*, ¶130. As discussed above with reference to limitation [1(b)], the invariable activation command generated by *McGregor's* microprocessor would cause the security key code to be wirelessly

transmitted instead of displaying *or* in addition to displaying. *Id.* While the claims do require transmitting data via the transceiver when an activation cue has been received (e.g., when the handshake signals are exchanged), they do not exclude a device that both displays and transmits its data when an activation cue has been received. *Id.* Accordingly, whether *McGregor*'s device automatically transmits the security key code *instead of or in addition to* displaying that data is of no moment to the Proposed Grounds. *Id.*

[1(h)] wherein upon said control device being selectively triggered to issue an[] invariable activation command: . . . if said switching element is in said inactive state, data will be conveyed from said electronic circuit to said user interface device for communicating information to the portable electronic device holder.

The combination of *McGregor* and *Palmer* teaches this limitation. *Dec.*, ¶131-132. As set forth in the preceding limitations, *McGregor*'s wallet device modified based on the teachings of *Palmer*, when a user enters their fingerprint for authorization (i.e., selectively triggers the device to send data), automatically displays a security key code (i.e., data) to the wallet device's display (i.e., user interface device for communicating information to the portable electronic device holder) where no RF field of a wireless reader/writer device has been detected. Absent detecting an RF field of a reader/writer device and performing a handshake process, the wallet's microprocessor (i.e., switching element) remains in an inactivated state. And, as discussed with reference to limitation [1(b)], the command issued by *McGregor*'s microprocessor to convey the security key code is

“invariable” in that the microprocessor being in an inactivated state dictates how the data is conveyed, rather than providing any user control over the conveyance. *Id.*

ii. Claim 2

A portable electronic device as defined in claim 1, wherein said user interface device is a display screen.

McGregor discloses this limitation. *Dec.*, ¶133. For example, *McGregor* discloses a display 420 (a user interface device). *See* claim 1(c). “The display region [420] preferably comprises an LED array, LCD, or other similar, low-cost display mechanism.” *McGregor*, [0039], [0043]. A POSITA would have understood an LED array or LCD constitute a display screen. *Dec.*, ¶133.

iii. Claim 4

A portable electronic device as defined in claim 1, wherein said control device is a biometric parameter detector.

McGregor discloses this limitation. *Dec.*, ¶¶134-135. For example, *McGregor* discloses a fingerprint scanner 418. *See* Claim [1(b)]. A POSITA would have understood that the fingerprint scanner is a biometric parameter detector. *Dec.*, ¶¶134-135. Indeed, the title of *McGregor* is a “bio-metric smart card, bio-metric smart card reader, and method of use[.]” *McGregor*, Title.

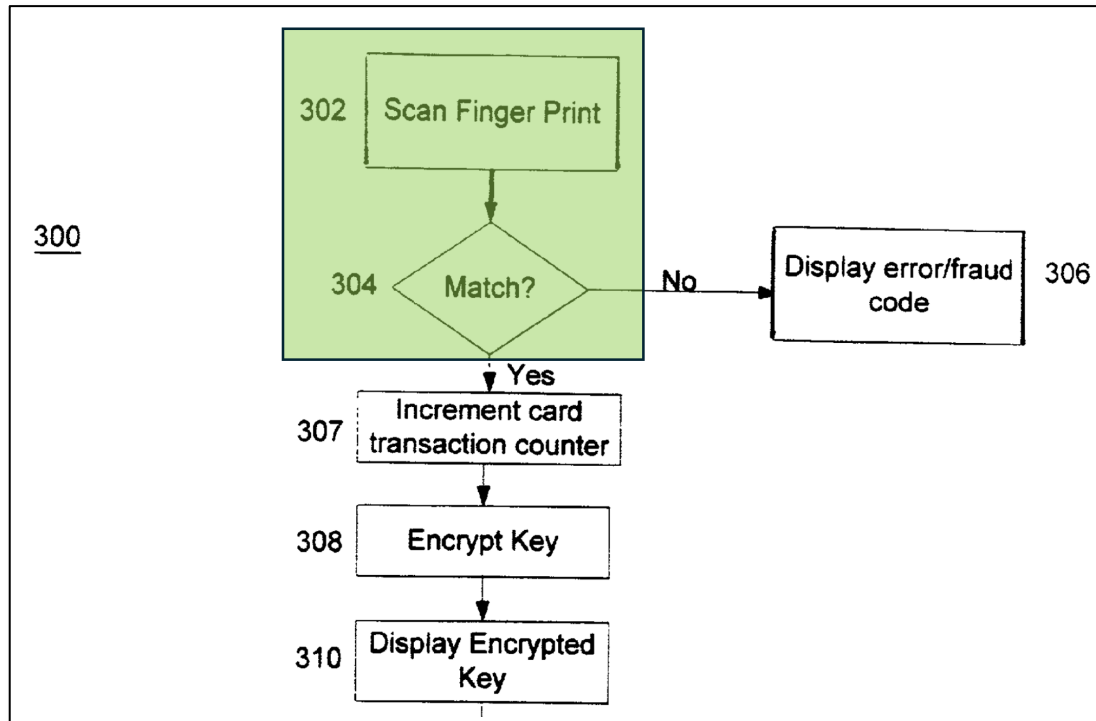
iv. *Claim 5*

A portable electronic device as defined in claim 4, wherein said biometric parameter detector is a fingerprint scanner capable of obtaining a fingerprint scan, and whereby said control device is triggered when the fingerprint scan matches a fingerprint image pre-saved in said electronic circuit.

McGregor discloses this limitation. *Dec.*, ¶136-137. For example, *McGregor* discloses a biometric parameter detector in the form of a fingerprint scanner 418. *See Claim 4. McGregor* teaches matching a fingerprint to a pre-saved fingerprint in the electronic circuit:

[T]he user places his or her thumb or finger upon fingerprint scanner [418]. In the alternative, step 302 might be replaced with any other form of bio-metric authentication that provides positive identification that an authorized user is, in fact, attempting to use the account number found on the card. The results of scan step 302 are then compared (either by scanner [418] alone or in cooperation with microprocessor [416]) at step 304 to a reference file representative of the user's actual print. The reference file might be stored in scanner [418], in microprocessor [416], or in a separate memory unit (ROM [422]).

McGregor, [0040]. The microprocessor 416 and ROM 422 are parts of the electronic circuit. *See Claim [1(a)].*



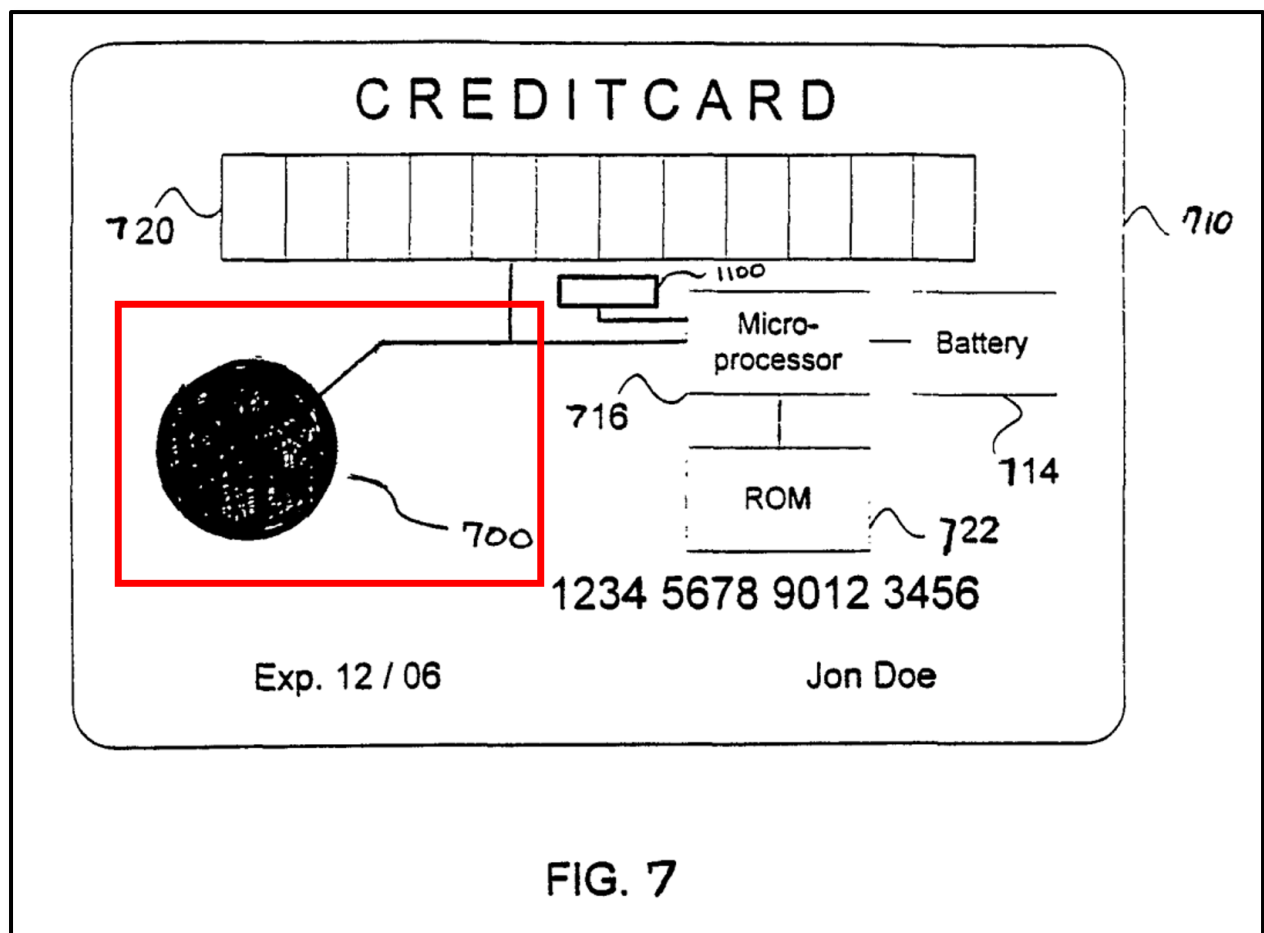
McGregor, Fig. 3, excerpt, annotated.

Scanning a fingerprint that matches a stored fingerprint constitutes selectively triggering the fingerprint scanner 418. *McGregor*, Fig. 3; *Dec.*, ¶¶136-137. As shown in Fig. 3, Step 304 (annotated in green), “[i]f a match is found . . . the microprocessor [416] increments an activation/transaction counter at step 307 and generates therewith a numeric or alphanumeric security key.” *McGregor*, [0041]. In the context of this limitation, triggering the control device does not imply initiating or triggering the fingerprint scanner to turn on. *Dec.*, ¶137.

v. Claim 6

A portable electronic device as defined in claim 1, wherein said control device is a manually activated button, and whereby said control device is triggered when the button is pressed.

McGregor discloses this limitation. *Dec.*, ¶¶138-142. For example, *McGregor* discloses an embodiment of a smartcard 710 where “a button or other activation device 700” has the functionality of fingerprint scanner 218. *McGregor*, [0058]. Fig. 7 shows the button or other activation device 700 (i.e., control device) on smartcard 710, as shown in the red box.



McGregor, Fig. 7, annotated.

McGregor further discloses that the button “provides a signal that initiates production of an encrypted key that is displayed on display 720.” *McGregor*, [0059]. As such, the button is the claimed control device. A POSITA would have understood that the button must be manually activated (i.e., pressed). *Dec.*, ¶¶138-139.

A POSITA would have recognized that the button in smart card 710 would be straightforwardly implemented in the wallet 410 embodiment, replacing its biometric sensor. *Dec.*, ¶¶138-140. This presents a straightforward tradeoff between cost and security. Namely, the biometric sensor equipped in the wallet 410 provides an additional layer of security, allowing the user to be authenticated using unique fingerprint data before a transaction may proceed. The button actuator in Fig. 7 would not permit this additional layer of security to be realized, but a POSITA would have recognized that biometric sensors are more expensive than simple buttons. Accordingly, whether to implement *McGregor*’s wallet with a biometric sensor (e.g., the Fig. 4 embodiment) or with a simple button (e.g., the Fig. 7 embodiment) is just a tradeoff between cost and security. *Dec.*, ¶¶141-142. A POSITA would have expected success in making this simple substitution between a biometric sensor and simple button. *Id.*

vi. Claim 7

A portable electronic device as defined in claim 1, wherein said electronic circuit comprises said switching element.

McGregor in view of *Palmer* teaches this limitation. See Claim [1(e)]; *Dec.*, ¶143. For example, *McGregor* and *Palmer* teach a portable electronic device with an electronic circuit. See Claims [1(a)] and [1(d)]. Further, *McGregor* in view of *Palmer* teaches a switching element programmed as software onto microprocessor 416, which is part of the electronic circuit. See *McGregor*, [0085]; see Claim [1(e)]. A POSITA would have understood that since the switching element is part of the microprocessor 416, it is part of the electronic circuit. *Dec.*, ¶143.

vii. Claim 8

A portable electronic device as defined in claim 7, wherein said electronic circuit comprises a microchip, and wherein said switching element is a series of instructions programmed onto said microchip.

McGregor in view of *Palmer* teaches this limitation. See Claims [1(e)], 7.

viii. Claim 9

A portable electronic device as defined in claim 1, wherein said switching element comprises a logical circuit.

The '333 Patent provides little detail regarding the claimed “logical circuit.” At best, it suggests that implementing switching element as a “decisional logical circuit” is an alternative to implementing switching element as “instructions programmed onto [a] microchip[.]” ’294 Patent, 6:9-17. To the extent Patent Owner contends that Claim 9 captures software-driven switching (e.g., software switching

that relies on logical circuits), despite the patent distinguishing software implementations from logical circuit implementations, *McGregor* in view of *Palmer* teaches this limitation. *See* Claim [1(e)]. A POSITA would have understood that a microprocessor such as microprocessor 416 consists of multiple logical circuits to run logical operations. *Dec.*, ¶145. A POSITA would understand that a software switch executed by a microprocessor comprises a logical circuit. *Id.*.

ix. Claim 10

[10(Pre)] A data exchange system comprising

To the extent the preamble is limiting, *McGregor* in view of *Palmer* teaches this limitation. *Dec.*, ¶146. For example, *McGregor* in view of *Palmer* teaches a device that has two-way communication (i.e., data exchange) with a reader/writer device. *See* Claim [1(d)]. A POSITA would understand that together, a portable electronic device and a reader/writer device constitutes a data exchange system. *Dec.* ¶146.

[10(a)] a data exchange device comprising a first electronic circuit, a first data transceiver and a cue emitter; and

McGregor in view of *Palmer* teaches this limitation. *Dec.*, ¶¶147-151. As discussed with reference to limitation [1(d)], *McGregor* teaches retailer-based readers connected to the transaction network that facilitate short-range communications with wallet 410. *McGregor*, [0039] (“The displayed security key is [] communicated or transmitted to the credit card authorization service [] through a

reader[.]”); *Dec.*, ¶148 (explaining that a reader or other merchant device capable of short-range communication wirelessly receives the security key code from *McGregor’s* wallet device). As also explained in this mapping, *Palmer* teaches a reader device consistent with that described by *McGregor*, and a POSITA would have been motivated to implement *Palmer’s* reader/writer device 202 in *McGregor’s* system to (1) communicate wirelessly with a smart card and (2) to communicate transaction data with the transaction network. *Dec.*, ¶148.

For both *McGregor’s* retailer-based readers and *Palmer’s* reader/writer 202 (each a “data exchange device”), a POSITA would understand that they include a cue emitter (e.g., for performing a handshake with wallet 410) and a first data transceiver (e.g., for exchanging handshake data and transaction data wirelessly with wallet 410). A POSITA would have further understood that each reader includes a first electronic circuit for controlling the communications and processing the software that governs at least the communications processes implemented by these readers. *Dec.*, ¶¶149-150.

To the extent Patent Owner argues the first data transceiver and cue emitter must be a singular element, *McGregor* in view of *Palmer* discloses it. Namely, *Palmer* teaches that its communications may be conducted using “one or more antennae 204[.]” *Palmer*, [0027]. A POSITA would understand this means that the first data transceiver and cue emitter utilize a single antenna. *Dec.*, ¶151.

[10(b)] a portable electronic device, comprising:

McGregor discloses this limitation. See Claim [1(Pre)].

[10(c)] a second electronic circuit capable of storing data therein, capable of processing data, and capable of data input and output;

McGregor in view of *Palmer* teaches this limitation. See Claim [1(a)]. The electronic circuit described in Claim [1(a)] and the claimed second electronic circuit are both the circuit of the portable smartcard device. *Dec.*, ¶153.

[10(d)] a control device operatively linked to said second electronic circuit, with an invariable activation command being issued when said control device is selectively triggered;

McGregor in view of *Palmer* teaches this limitation. See Claims [1(b)] and [10(c)].

[10(e)] a user interface device operatively linked to said second electronic circuit;

McGregor discloses this limitation. See Claims [1(c)] and [10(c)].

[10(f)] a second data transceiver operatively linked to said second electronic circuit;

McGregor in view of *Palmer* teaches this limitation. See Claims [1(d)] and [10(c)]. The data transceiver described in Claim [1(d)] and the second data transceiver of this claim both refer to the transceiver of the portable electronic device. *Dec.*, ¶156.

[10(g)] a data conveyance switching element operatively linked to said second electronic circuit, and

McGregor in view of *Palmer* teaches this limitation. See Claims [1(e)] and [10(c)].

[10(g)(i)] switching element being in an activated state upon an activation cue having been received by said second data transceiver, and being in an inactive state when no activation cue was received by said second data transceiver; and

McGregor in view of *Palmer* discloses this limitation. See Claims [1(e)], [10(f)-(g)].

[10(h)] power means for providing power to said portable electronic device;

McGregor discloses this limitation. See Claims [1(f)] and [10(b)].

[10(i)] wherein upon said control device being selectively triggered to issue said invariable activation command: if said switching element is in its activated state, a data exchange will occur between said first data transceiver and said second data transceiver, thereby exchanging data between said data exchange device and said portable electronic device;

McGregor in view of *Palmer* teaches this limitation. See Claim [1(g)].

[10(j)] wherein upon said control device being selectively triggered to issue said invariable activation command: . . . if said switching element is in its inactive state, data is forwarded to said user interface device for communicating information to the portable electronic device holder.

McGregor in view of *Palmer* teaches this limitation. See Claim [1(h)].

B. Ground 2: Claims 3 and 11-13 are obvious under pre-AIA 35 U.S.C. § 103 over *McGregor* in view of *Palmer* and in further view of *Tuttle*

Claim 3 is dependent on Claim 1, additionally requiring that the portable electronic device utilize a distinct data transmitter, data receiver, and cue receiver.

Claims 11-13 similarly require multiple communication ports. As set forth below, a POSITA would have been motivated to implement the combination of *McGregor* and *Palmer* with distinct data transmitter, data receiver, and cue receiver ports pursuant to the teachings of *Tuttle*.

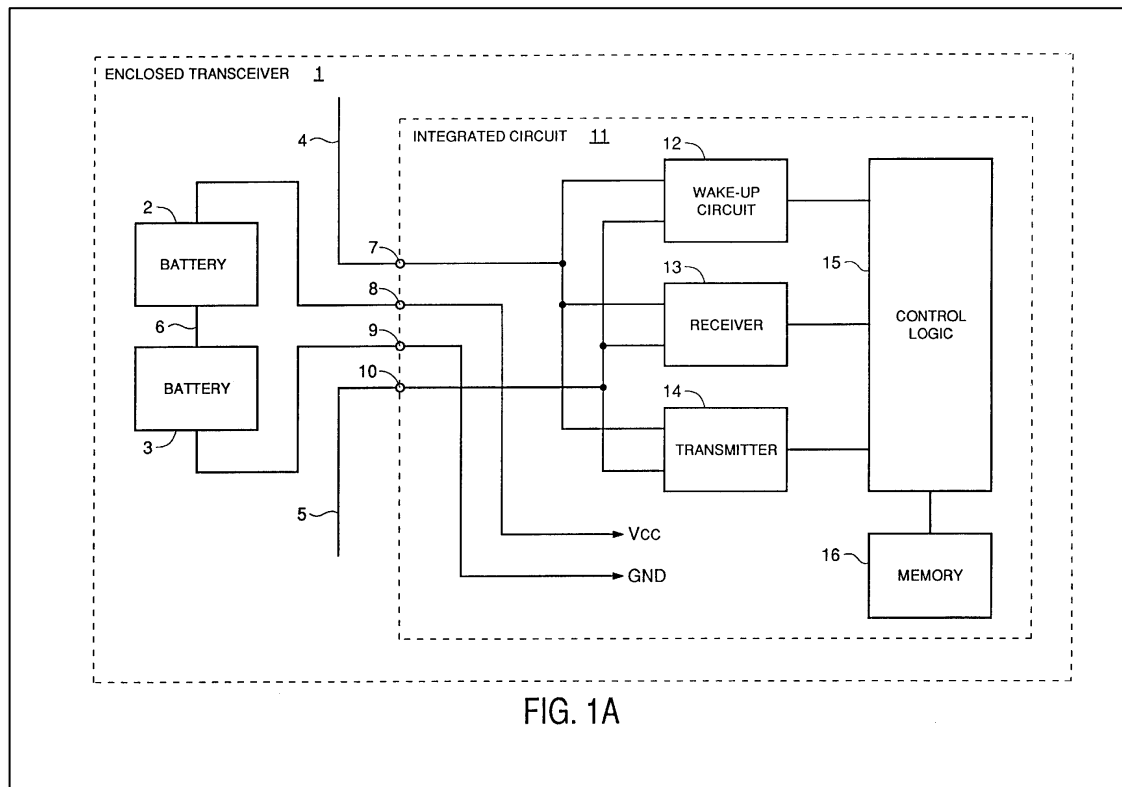
i. Claim 3

A portable electronic device as defined in claim 1, wherein said data transceiver comprises a data transmitter, a data receiver distinct from said data transmitter, and a cue receiver distinct from said data receiver.

McGregor in view of *Palmer* and *Tuttle* teaches this limitation. *Dec.*, ¶¶163-167. As discussed in Ground 1, *McGregor* in view of *Palmer* teaches a portable electronic device with a data transceiver capable of two-way communication and receiving an activation cue via RF antenna 404 and smartcard chip 408. *See* Claim 1. *Palmer* teaches that its communications may be conducted using “one or more antennae,” which suggests that certain transmission and reception functionality may be dedicated to separate antennae. But *Palmer* does not elaborate beyond suggesting multiple antennae. A POSITA would have looked to chip designs in the prior art, such as *Tuttle*’s integrated circuit 11, to guide separating receiving and transmitting functionalities to distinct antennae. *Dec.*, ¶163.

Tuttle discloses an integrated circuit 11, “a four terminal device operating as communicating means for transmitting and receiving radio signals.” *Tuttle*, 6:7-9. Further, integrated circuit 11 “is a transceiver including wake-up circuit 12, receiver

13, transmitter 14, control logic 15, and memory 16.” *Tuttle*, 6:14-16. A POSITA would have understood that a chip such as the smartcard chip 408 would include one or more integrated circuits. *Dec.*, ¶164 (explaining that “chip” refers to a silicon substrate computer chip containing an integrated circuit, and that the terms are often used interchangeably). Fig. 1A depicts the integrated circuit 11.



Tuttle, Fig. 1A

Tuttle provides detail on an integrated circuit that would allow smartcard chip 408 to achieve the functions outlined in *Palmer*. For example, *Palmer* discloses detecting the presence of an RF field via RF antenna 404 emitted from the external reader/writer device 202, “device 400 captures power, energizing its electronics.”

Palmer, [0050]; *Dec.*, ¶165. However, in embodiments where the device is powered by a battery, a POSITA would have understood that energizing the electronics initiates device software on the smartcard chip to “support two-way communication with an associated reader/writer device” instead of solely powering the device 400. *Palmer*, [0043]; *Dec.*, ¶165; *see* Claims [1(b)], [1(d)]. In the combination of *McGregor*, *Palmer*, and *Tuttle*, RF antenna 404 picks up signals from the external reader/writer device and provides them to the smartcard chip 408 of *Palmer*, allowing the smartcard chip to detect the existence of (e.g., detecting an RF field) and availability of (e.g., exchanging handshake signals) a reader/writer device before initiating data exchange with the reader/writer device. *Tuttle* similarly discloses that initial RF signals are detected and processed before data is sent to and received from an external device. Namely, *Tuttle* teaches “interrogation signals . . . [are] first processed by [the] sleep/wake up circuit 12[,] . . . bring[ing] integrated circuit 11 out of a “sleep” mode into a “waked” mode[.]” *Tuttle*, 7:4-10. After the device is placed into a waked mode, data is received via receiver 13 and transmitted via transmitter 15. *Tuttle*, 7:10-16. A POSITA would understand that the interrogation signals of *Tuttle* are functionally similar to the handshake signals disclosed by *Palmer*. *Dec.*, ¶165. In both cases, initial signaling is processed to establish a communication channel over which data communication can occur. *Id.* *Tuttle* also teaches that the integrated circuit 11 includes a receiver and a transmitter:

Received data is provided by receiver 13 to control logic 15. Control logic 15 writes received data into memory 16. . . . If a response is appropriate, control logic 15 reads transmit data from memory 16 and ***enables transmitter 14 for sending the transmit data*** as a second radio signal on antenna 4 and 5.

Tuttle, 6:20-29. In the *McGregor-Palmer-Tuttle* combination, data transmission to and from the reader/writer device will be done through transmitter 14 and receiver 13, respectively. *Tuttle* discloses the integrated circuitry 11 (a transceiver) includes wake-up circuit 12, receiver 13, and transmitter 14 that are separate from one another. *See Tuttle* 6:14-17, Fig. 1A. Therefore, the combination of *McGregor*, *Palmer*, and *Tuttle* discloses a data transmitter, a data receiver distinct from said data transmitter, and a cue receiver distinct from said data receiver.

A POSITA would be motivated to incorporate *Tuttle* into the *Palmer-McGregor* combination. *Dec.*, ¶¶166-167. Namely, a POSITA would have understood that the *Palmer-McGregor* combination requires implementation details beyond those disclosed in *Palmer*, such as how to detect readers and exchange data, and would have looked for guidance from known wireless systems, specifically focusing on those with chips capable of automatic wireless data transmission. *Dec.*, ¶167. *KSR Int’l Co.*, 550 U.S. 398 at 421 (“When there is a design need . . . and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If this

leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense.”); *see also In re Translogic Technology, Inc.*, 504 F.3d 1249, 1262 (Fed. Cir 2007) (“[I]n looking for a multiplexer circuit for the individual 2:1 multiplexers disclosed in Gorai, a person of ordinary skill in the art would have solved this design need by ‘pursu[ing] known options within his or her technical grasp.’”). One such system is *Tuttle’s* integrated circuit 11 comprising wake-up circuit 12, receiver 13, transmitter 14, control logic 15, and memory 16. For example, *Tuttle* teaches that the wake-up circuit 12 “senses in band energy [(an interrogation signal)] and switches from a sleep mode to an operating (waked) mode.” *Tuttle*, 4:27-29. When in an operating mode, the receiver 13 and transmitter 14 receive and send data in conjunction with the control logic 15 and memory 16. *See Section III.C.* A POSITA would understand that chips used for detecting, receiving, and transmitting RF signals can have components that are more or less integrated into the chip, and that implementing a chip with separate wake-up circuit, receiver, and transmitter components is a simple design choice. *Dec.*, ¶166. Finally, a POSITA would have expected success in implementing *Tuttle’s* design into the *Palmer-McGregor* combination. *Id.*, ¶167. The hardware and software at issue is straightforward in nature and would have been well within the capabilities of a POSITA. *Id.*

ii. *Claim 11*

[11(Pre)] A method for data exchange with a portable electronic device of the type comprising; an electronic circuit capable of storing data therein, capable of processing data, and capable of data input and output, a control device operatively linked to said circuit, a user interface device operatively linked to said circuit, communication ports operatively linked to said circuit, a switching element operatively linked to said electronic circuit and being in a default inactive state, and power means for providing power to said portable electronic device, said method comprising the steps of:

To the extent the preamble is limiting, *McGregor* in view of *Palmer* and *Tuttle* teaches this limitation. *Dec.*, ¶¶168-170. For example, *McGregor* in view of *Palmer* discloses each of the portable electronic devices, electronic circuit capable of storing and processing data, and data input and output, control device operatively linked to said circuit, user interface linked to said circuit, switching element linked to said circuit, default inactive state, and power means. *See* Ground 1, Claim [1(Pre)-1(h)].

Tuttle discloses communication ports operatively linked to a circuit for data exchange. *Dec.*, ¶169. Specifically, *Tuttle* describes an integrated circuit 11 that “is a transceiver including wake-up circuit 12, receiver 13, transmitter 14, control logic 15, and memory 16.” *Tuttle*, 6:14-16. The wake-up circuit 12, receiver 13, and transmitter 14 would be understood to be communication ports since they correspond with the communication ports described by the ’333 Patent, “namely a data transmitter 18a, a data receiver 18b, and a cue receiver 19.” ’333 Patent, 9:30-33; *Dec.*, ¶169. Accordingly, the *McGregor-Palmer-Tuttle* combination teaches communication ports operatively linked to said circuit. *Dec.*, ¶¶169-170.

[11(a)] awaiting for an activation cue to be received at a predetermined one of said communication ports;

McGregor in view of *Palmer* and *Tuttle* teaches this limitation. *Dec.*, ¶¶171-173. One of *Tuttle*'s communication ports (*See* Claim 11(Pre)) is a wake-up circuit 12 that "senses in-band energy [(an interrogation signal)] and switches from a sleep mode to an operating (waked) mode." *Tuttle*, 4:27-29; *see also id.*, 7:4-10; *Dec.*, ¶¶172-173 A POSITA would have understood that "in-band" energy refers to RF interrogation/handshake signals which constitute an activation cue. *Dec.*, ¶¶172-173; *see* Claim [1(d)].

[11(b)] if an activation cue is received at one of said communication ports, changing the state of said switching element from its default inactive state to an activated state; and

McGregor in view of *Palmer* and *Tuttle* teaches this limitation. *See* Claims [1(e)] and [11(a)]. As explained above, the *McGregor-Palmer-Tuttle* portable electronic device comprises a wake-up circuit 12 that detects the RF handshake signal and causes the modified smartcard chip 408 to be placed in an active state (or operational mode). *See* Claims 3, [1(e)], and [11(a)]; *Dec.*, ¶174. Further, a POSITA would have recognized that the smartcard chip 408 would be by default in an inactive state (or sleep mode) in the absence of an activation cue (*i.e.*, RF handshake signal) to conserve battery power. *Dec.*, ¶174.

[11(c)] selectively triggering said control device to issue an invariable activation command, whereby said method will further comprise one of the two following steps: if said switching element is in its activated state, initiating a data exchange with an external data exchange device through at least one of said communication ports; and

McGregor in view of *Palmer* teaches this limitation. See Claims [1(b), (g)] and [11(a)].

[11(d)] selectively triggering said control device to issue an invariable activation command, whereby said method will further comprise one of the two following steps: . . . if said switching element is in its inactive state, conveying data from said electronic circuit to said user interface device for communicating information to the portable electronic device holder.

McGregor in view of *Palmer* teaches this limitation. See Claims [1(b), 1(h)], and [11(a)].

iii. Claim 12

A method as defined in claim 11, wherein said activation cue is received at one of said communication ports distinct from another one of said communication ports used for data exchange with the external data exchange device.

McGregor in view of *Palmer* and *Tuttle* teaches this limitation. See Claim 11; *Dec.*, ¶177. For example, *Tuttle* discloses an integrated circuit 11 that “is a transceiver including wake-up circuit 12, receiver 13, transmitter 14, control logic 15, and memory 16.” *Tuttle*, 6:14-16. The wake-up circuit 12 receives an activation cue while the receiver 13 and transmitter 14 are used for data exchange. See Claim 3. In the combination, the data exchange occurs between the external data device and the smartcard chip 408, which includes the features of *Tuttle* discussed. See Claim 11; Section III.C.

iv. Claim 13

A method as defined in claim 11, wherein the additional following step occurs after selectively triggering said control device if said switching element is in said activated state: conveying data from said electronic circuit to said user interface device for communicating information to the portable electronic device holder.

McGregor in view of *Palmer* teaches this limitation. *Dec.*, ¶¶178-185.

McGregor in view of *Palmer* discloses selectively triggering a control device when the switching element is in the activated state. *See* Claims [1(g)] and [11(c)]; *Dec.*, ¶179. *McGregor*'s modified device discloses both displaying and wirelessly transmitting data. *See* Claims 1[(g), (h)] and [11(c), (d)]; *Dec.*, ¶179. Additionally, *Palmer* discloses that its electro-luminescent display 412 can display information to the user including a "credit card number to support 'card not present' transactions, a residual balance of an 'electronic purse,' air travel flight and seat assignment information[.]" *Palmer*, [0044]; *Dec.*, ¶180.

A POSITA would have been motivated to apply this functionality to *McGregor*'s modified device, displaying data when the switching element is in the active state *after* a data conveyance with an external data exchange device. A POSITA would have understood that such modification would have improved *McGregor*'s device for numerous reasons. *Dec.*, ¶¶178-181. For example, during a wireless transaction, when *McGregor*'s security key is automatically wirelessly transmitted, it would be obvious to display a confirmation message via display 420. *Id.*, ¶181. In another example, it would be obvious to a POSITA that if a wireless

transaction is ongoing (i.e., when the switching element is in an active state) but a user has insufficient funds, the user would be notified of such insufficient funds via the user interface. *Dec.*, ¶¶181. Additionally, in the event that a wireless transaction fails, information displayed on the screen would be used to complete the transaction. *Id.*; see Claim [1(g)].

It was well known in the art before the priority date of the '333 Patent, that portable electronic devices (*e.g.*, smart card) were capable to convey information to the user following the conveyance of data to an external data exchange device (*e.g.*, card reader/writer device. *Dec.*, ¶¶182-184. The proposed modification would be within the skill of a POSITA because it would be a simple modification using technology taught by both *McGregor* and *Palmer*. *Dec.*, ¶¶185-86; see Section III.A-B.

VI. DISCRETIONARY CONSIDERATIONS

A. The Board Should Not Deny Institution Under *Fintiv*

The parallel litigation was recently transferred from the Western District of Texas to the Northern District of California. There is currently no schedule in place for the transferred case, so there is no jury trial date to guide a *Fintiv* analysis. Further, the parties have agreed to request a stay of the litigation pending resolution of *Inter Partes* Review and are currently finalizing a stipulation to memorialize this agreement. Ex. 1019, 3 (noting in a joint statement that DH will not object to Apple's

planned Stipulation to Stay the parallel proceeding pending IPR). Accordingly, there is no basis on which to deny institution under *Fintiv*.

B. The *General Plastics* Factors Favor Institution

The Board set forth seven factors it considers in determining whether to exercise discretion to deny a petition under § 314(a). *General Plastic Industrial Co., Ltd. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19 at 15-19 (September 6, 2017) (precedential). Here, these factors weigh heavily in favor of institution.

There are two prior PTAB challenges to the '333 Patent— *Samsung Electronics Co., Ltd. v. G. Holdings, Ltd*, IPR2021-00885 (“the Samsung IPR”) and *Google LLC v. DH International Ltd.*, IPR2024-01321 (“the Google IPR”). With respect to the first five *General Plastic* factors, it weighs against a discretionary denial that Apple is not a party to any prior IPR, that this is Apple’s first IPR challenge to the '333 Patent, and that Apple did not coordinate with Samsung or Google in any way. *See Unified Patents, Inc. v. Certified Measurement, LLC*, IPR2018-00548, Paper No. 7, 7-8 (Sep. 5, 2018) (finding that it “weighs especially heavily against a discretionary denial” when the Petitioner is not a party to any prior proceeding, and it is Petitioner’s first challenge to the challenged Patent); *see also Foursquare Labs, Inc. v. Mimzi LLC*, IPR2019-01287, Paper 11 (Jan. 14, 2020) (petitioners individually sued with no evidence of coordination weighed against denying institution); *see Alcatel-Lucent USA Inc. v. Oyster Optics, LLC*, Case

IPR2017-02146, slip op. at 12 (PTAB Feb. 28, 2018) (Paper 12) (“Once resolution of factor 1 indicates that Petitioner had not previously filed a petition against the same patent, factors 2–5 bear little relevance.”).

Relevant to factor (3), the Board in *General Plastic* discussed the “potential for abuse” due to “[m]ultiple, staggered petitions challenging the same patent and same claims[.]” *Gen. Plastic*, IPR2016-01357, Paper 19 at 17. The Board explained, “[t]he absence of any restrictions on follow-on petitions would allow petitioners the opportunity to strategically stage their prior art and arguments in multiple petitions, using our decisions as a roadmap, until a ground is found that results in the grant of review.” *Id.* Such roadmap concerns do not exist here. Importantly, the Samsung IPR was not denied institution. Instead, it was terminated pre-institution pursuant to settlement. Further, the Preliminary Response filed in the Samsung IPR addressed only *Fintiv*. There was no discussion of the merits, so Apple could not have used the Samsung POPR as a guide to reframe the Samsung prior art. There has not been an institution decision on the Google IPR, so it cannot be used as a roadmap.

As to the sixth factor, the instant petition respects the finite resources of the Board. The Samsung IPR was terminated pursuant to settlement prior to institution. To the extent the Board assigned to the Samsung IPR had already begun reviewing the challenge pre-termination, the instant Petition provides it an opportunity to pick up where it left off. Although the grounds are not identical, at least the *Palmer*

reference was presented by both Samsung and Petitioner here. The Google IPR advances entirely different prior art than the current petition and the grounds are not duplicative.

Regarding the seventh factor, there is no readily identifiable roadblock for the Board to issue a final determination within the statutory one-year limit.

Accordingly, the Board should reach the merits of this petition, and institute review of all Challenged Claims.

VII. CONCLUSION

For the foregoing reasons, Petitioner respectfully requests *inter partes* review of Claims 1-13 of the '333 Patent.

Respectfully submitted,

By: /s/ Paul R. Hart

Paul R. Hart, Reg. No. 59,646

Adam P. Seitz, Reg. No. 52,206

COUNSEL FOR PETITIONER

VIII. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(A)(1)

A. Real Party-In-Interest

Petitioner is the real party-in-interest. 37 C.F.R. § 42.8(b)(1).

B. Related Matters

Pursuant to 37 C.F.R. § 42.8(b)(2), Petitioner is aware of the following matters involving the '333 Patent or related patents:

- *DH International Ltd v. Apple Inc.*, No. 1:23-cv-01114 (W.D. Tex.), transferred to Northern District of California (3:24-cv-06185)
- *DH International Ltd v. Google LLC*, No. 1:23-cv-01116 (W.D. Tex.), dismissed
- *Google LLC v. DH International Ltd.*, IPR2024-01321 (PTAB)
- *Samsung Electronics Co., Ltd. v. G. Holdings, Ltd.*, IPR2021-00885 (PTAB), terminated pre-institution pursuant to settlement
- *Google LLC v. DH International Ltd.*, IPR2024-01322 (PTAB), challenging related U.S. Patent No. 9,022,294
- *Samsung Electronics Co., Ltd. v. G. Holdings, Ltd.*, IPR2021-00884 (PTAB), challenging related U.S. Patent No. 9,022,294, terminated pre-institution pursuant to settlement
- *G. Holdings Ltd. v. Samsung Electronics Co., Ltd. et al*, No. 2:20-cv-00342 (E.D. Tex.), dismissed

C. Lead and Back-Up Counsel

Petitioner provides the following designation and service information for lead and back-up counsel. 37 C.F.R. § 42.8(b)(3) and (b)(4).

Lead Counsel	Back-Up Counsel
Paul R. Hart (Reg. No. 59,646) <u>Paul.Hart@eriseip.com</u> PTAB@eriseip.com	Adam P. Seitz (Reg. No. 52,206) <u>Adam.Seitz@eriseip.com</u> PTAB@eriseip.com
<u>Postal and Hand-Delivery Address:</u> Erise IP, P.A. 717 17 th Street Suite 1400 Denver, Colorado 80202 Telephone: (913) 777-5600 Fax: (913) 777-5601	<u>Postal and Hand-Delivery Address:</u> Erise IP, P.A. 7015 College Blvd., Ste. 700 Overland Park, Kansas 66211 Telephone: (913) 777-5600 Fax: (913) 777-5601

APPENDIX OF EXHIBITS

Exhibit 1001	U.S. Patent No. 7,628,333 (“the ’333 Patent”)
Exhibit 1002	File History for U.S. Patent No. 7,628,333
Exhibit 1003	Declaration of Dr. Michael Buehrer
Exhibit 1004	U.S. Patent Publication No. 2002/0180584 to McGregor et al. (“ <i>McGregor</i> ”)
Exhibit 1005	U.S. Patent Publication No. 2003/0226041 to Palmer et al. (“ <i>Palmer</i> ”)
Exhibit 1006	U.S. Patent No. 6,078,791 to Tuttle & Lake (“ <i>Tuttle</i> ”)
Exhibit 1007	File History for U.S. Patent No. 9,022,294
Exhibit 1008	U.S. Patent Publication No. 2002/0116330 to Hed & Pavelle (“ <i>Hed</i> ”)
Exhibit 1009	U.S. Patent No. 5,690,773 to Fidalgo & Oi (“ <i>Fidalgo</i> ”)
Exhibit 1010	U.S. Patent No. 5,767,503 to Gloton (“ <i>Gloton</i> ”)
Exhibit 1011	U.S. Patent No. 6,097,292 to Kelly et al. (“ <i>Kelly</i> ”)
Exhibit 1012	U.S. Patent No. 6,375,082 to Kobayashi et al. (“ <i>Kobayashi</i> ”)
Exhibit 1013	U.S. Patent No. 5,748,737 to Daggar (“ <i>Daggar</i> ”)
Exhibit 1014	U.S. Patent No. 6,704,608 to Azuma (“ <i>Azuma</i> ”)
Exhibit 1015	U.S. Patent No. 5,280,527 to Gullman et al. (“ <i>Gullman</i> ”)
Exhibit 1016	U.S. Patent No. 6,631,849 to Blossom (“ <i>Blossom</i> ”)
Exhibit 1017	U.S. Patent Publication No. 2002/0095587 to Doyle et al. (“ <i>Doyle</i> ”)
Exhibit 1018	U.S. Patent Publication No. 2002/0038369 to Sung & Lee (“ <i>Sung</i> ”)
Exhibit 1019	<i>DH International Ltd. v. Apple Inc.</i> , 3:24-cv-06185 (N.D. Cal.), Dkt. 83, Joint Initial Case Management Statement

CERTIFICATION OF WORD COUNT

The undersigned certifies pursuant to 37 C.F.R. § 42.24 that the foregoing Petition for *Inter Partes* Review, excluding any table of contents, mandatory notices under 37 C.F.R. § 42.8, certificates of service or word count, or appendix of exhibits, contains 13,133 words according to the word-processing program used to prepare this document (Microsoft Word).

Dated: December 3, 2024

By: /s/ Paul R. Hart
Paul R. Hart, Reg. No. 59,646

COUNSEL FOR PETITIONER

CERTIFICATE OF SERVICE ON PATENT OWNER
UNDER 37 C.F.R. § 42.105

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105, the undersigned certifies that on December 3, 2024, a complete and entire copy of this Petition for *Inter Partes* Review including exhibits was provided via Federal Express to the Patent Owner by serving the correspondence address of record for the '333 Patent as listed on PAIR:

SHUMAKER, LOOP & KENDRICK, LLP
1000 JACKSON STREET
TOLEDO, OH 43604

Further, a courtesy copy of this Petition for *Inter Partes* Review was sent via email to Patent Owner's litigation counsel:

Robert P. Hart (robert@addyhart.com)
Meredith Martin (meredith@addyhart.com)
Charles A. Pannell, III (cpannell@addyhart.com)
Benjamin M. Cappel (benjamin@addyhart.com)
Paul Tauger (ptauger@addyhart.com)

By: /s/ Paul R. Hart
Paul R. Hart, Reg. No. 59,646

COUNSEL FOR PETITIONER