

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

TELCOM VENTURES LLC,
Patent Owner

Case No. IPR2025-01235
U.S. Patent No. 10,674,432

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	LEGAL STANDARD.....	4
III.	BACKGROUND.....	5
	A. THE '432 PATENT	5
	B. CARLSON (EX. 1005).....	8
	C. HOLLOWAY (EX. 1032)	10
	D. JAZAYERI (EX. 1007).....	10
	E. ISO-14443 (EX. 1016)	12
	F. LIN (EX. 1030).....	13
	G. SHERMAN (EX. 1014)	13
	H. MURAKAMI (EX. 1009).....	13
IV.	CLAIM CONSTRUCTION.....	14
V.	LEVEL OF ORDINARY SKILL IN THE ART	15
VI.	THE DIRECTOR SHOULD NOT INSTITUTE <i>INTER PARTES</i> REVIEW.....	16
	A. PETITIONER HAS FAILED TO ESTABLISH A REASONABLE LIKELIHOOD THAT THE CHALLENGED CLAIMS WOULD HAVE BEEN OBVIOUS IN VIEW OF CARLSON IN COMBINATION WITH HOLLOWAY AND/OR MURAKAMI (GROUNDS 1–8).	17
	1. Carlson’s request for PPAI does not disclose and would not have rendered obvious “information requesting an authorization” (Grounds 1-8).....	17
	2. A POSITA would not have been motivated to combine Carlson’s device with Holloway’s fingerprint scanner to render obvious “responsive to at least one physiological parameter . . . enabling a mode to communicate by the smartphone information requesting an authorization” (Grounds 1-4).....	29
	3. A POSITA would not have been motivated to combine Carlson’s device with the biometric authentication device of Murakami to render obvious “responsive to at least one	

physiological parameter . . . enabling a mode to
communicate by the smartphone information requesting
an authorization” (Grounds 5-8).34

VII. CONCLUSION 37

TABLE OF AUTHORITIES

	Page(s)
CASES	
<i>Eon Corp. IP Holdings LLC v. Silver Spring Networks, Inc.</i> , 815 F.3d 1314 (Fed. Cir. 2016)	14
<i>In re Magnum Oil Tools Int’l, Ltd.</i> , 829 F.3d 1364 (Fed. Cir. 2016)	4
<i>Microsoft Corp. v. Secure Web Conf. Corp.</i> , IPR2014-00745, Paper 12 (P.T.A.B. Sept. 29, 2014).....	4
<i>Philips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005) (en banc)	14
<i>Realtime Data, LLC v. Iancu</i> , 912 F.3d 1368 (Fed. Cir. 2019)	15
<i>Sirona Dental Sys. GmbH v. Institut Straumann AH</i> , 892 F.3d 1349 (Fed. Cir. 2018)	5
<i>Synopsys, Inc. v. Mentor Graphics Corp.</i> , IPR2012-00041, Paper 16 (P.T.A.B. Feb. 22, 2013).....	4
<i>Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.</i> , 200 F.3d 795 (Fed. Cir. 1999)	15
STATUTES	
35 U.S.C. § 103	6, 16
35 U.S.C. § 312(a)(3).....	4
OTHER AUTHORITIES	
37 CFR § 42.108(c).....	4

TABLE OF EXHIBITS

Exhibit Number	Description
2001	Interim Processes for PTAB Workload Management, Acting Director Memorandum (March 26, 2025) (https://www.uspto.gov/sites/default/files/documents/InterimProcesses-PTABWorkloadMgmt-20250326.pdf)
2002	Third Amended Docket Control Order
2003	Standing Order for Civil Cases Before Judge Rita F. Lin
2004	Telcom Ventures' Proposed Case Schedule for the Apple Litigation
2005	<i>Telcom Ventures LLC v. Apple, Inc.</i> , No. 3:25-cv-05041-RFL, Dkt. 1 (Oct. 4, 2024)
2006	Declaration of Chuck Easttom
2007	<i>Curriculum Vitae</i> of Chuck Easttom
2008	Chiradeep BasuMallick, "What is NFC (Near Field Communication)? Definition, Working, and Examples" (Sept. 29, 2022), https://www.spiceworks.com/tech/networking/articles/what-is-near-field-communication/
2009	Liu et al., "Near-Field Communications: A Comprehensive Survey," IEEE (June 2025)
2010	"The Creation of the NFC Forum and its Vision" (2011) https://cs.stanford.edu/people/eroberts/courses/cs181/projects/2010-11/NFCChips/nfcforum.html
2011	McHugh & Yarmey, "Near Field Communication: Introduction and Implication," ERIC (2012)
2012	Coskun et al., "The Survey on Near Field Communication," Sensors (June 5, 2015)

TABLE OF CLAIMS

Claim	Limitation
1[pre]	A method of operating a smartphone in performing a plurality of financial transactions, the method comprising:
1[a][i]	responsive to at least one physiological parameter having been sensed by at least one sensor of the smartphone,
1[a][ii]	enabling a mode to communicate by the smartphone information requesting an authorization;
1[b]	while the mode is enabled, transmitting by the smartphone first data to a first device, the first data relating to a plurality of financial transactions to be conducted;
1[c]	receiving by the smartphone second data from the first device responsive to said transmitting by the smartphone the first data, the second data relating to the plurality of financial transactions to be conducted and differing from the first data;
1[d]	performing a first transaction of the plurality of financial transactions by:
1[e]	detecting by the smartphone that a proximity condition is satisfied between the smartphone and a first entity, wherein the first entity is distinct from the first device;
1[f]	establishing, using a first air interface, a wireless short-range communications link between the smartphone and the first entity, in response to the proximity condition having been satisfied between the smartphone and the first entity;
1[g]	receiving, using the first air interface, a short-range signal from the first entity; and
1[h]	responsive to receiving the short-range signal from the first entity, sending by the smartphone to the first entity over the first air interface, information associated with the second data received from the first device; and

Claim	Limitation
1[i]	independent of performing said first transaction, receiving by the smartphone a communications service from a wireless network, using a second air interface that differs from the first air interface,
1[j]	wherein said transmitting by the smartphone first data and said receiving by the smartphone second data are performed over an air interface that differs from the first air interface.
2[pre]	The method of claim 1,
2[a]	wherein establishing the wireless short-range communications link between the smartphone and the first entity is performed responsive to at least one physiological parameter having been sensed by at least one sensor of the smartphone.
3[pre]	The method of claim 1,
3[a]	wherein sending by the smartphone to the first entity, information associated with the second data, is performed responsive to at least one physiological parameter having been sensed by at least one sensor of the smartphone.
4[pre]	The method of claim 1,
4[a]	wherein sending by the smartphone to the first entity, information associated with the second data, is performed responsive to a value of at least one parameter associated with the smartphone.
5[pre]	The method of claim 1, wherein the method further comprises:
5[a]	performing a second transaction of the plurality of financial transactions by:
5[b]	detecting by the smartphone that a proximity condition is satisfied between the smartphone and a second entity, wherein the second entity is distinct from the first entity and is further distinct from the first device;
5[c]	establishing, using the first air interface, a wireless short-range communications link between the smartphone and the second entity, in

Claim	Limitation
	response to the proximity condition having been satisfied between the smartphone and the second entity;
5[d]	receiving, using the first air interface, a short-range signal from the second entity; and
5[e]	responsive to receiving the short-range signal from the second entity, sending by the smartphone to the second entity over the first air interface, information associated with the second data received from the first device.
6[pre]	The method of claim 1,
6[a]	wherein said transmitting by the smartphone first data to a first device includes transmitting by the smartphone data relating to a request to pay for a transaction; and
6[b]	wherein said receiving by the smartphone second data from the first device includes receiving by the smartphone data relating to an acknowledgement and/or authorization of enabling a mode/function to pay for a transaction.
7[pre]	The method of claim 1, comprising:
7[a]	transmitting by the smartphone third data to a second device; the second device being distinct from the first device and further being distinct from the first entity; and
7[b]	receiving by the smartphone fourth data from the second device relating to an acknowledgement and/or authorization of enabling a mode/function to pay for a financial transaction,
7[c]	wherein said transmitting by the smartphone third data to a second device and said receiving by the smartphone fourth data from the second device are performed over the air interface that differs from the first air interface.
8[pre]	The method of claim 1, wherein said operations further comprise:

Claim	Limitation
8[a]	responsive to performing a financial transaction, causing data to be transmitted selectively to a plurality of predetermined devices and further causing data to be received selectively from said plurality of predetermined devices.
9[pre]	The method of claim 1,
9[a]	wherein the second air interface comprises an Orthogonal Frequency Division Multiplexed and/or an Orthogonal Frequency Division Multiple Access (OFDM/OFDMA) technology.
10[pre]	A smartphone that is configured to perform operations associated with a plurality of financial transactions; the operations comprising:
10[a]	responsive to at least one physiological parameter having been sensed by at least one sensor of the smartphone, enabling a mode to communicate by the smartphone information requesting an authorization;
10[b]	while the mode is enabled, transmitting first data to a first device as a precursor to performing the plurality of financial transactions; and
10[c]	receiving second data from the first device responsive to said transmitting the first data;
10[d]	performing a first financial transaction of the plurality of financial transactions by:
10[e]	detecting by the smartphone that a proximity condition is satisfied between the smartphone and a first entity, wherein the first entity is distinct from the first device;
10[f]	establishing, using a first air interface, a wireless short-range communications link between the smartphone and the first entity, in response to the proximity condition having been satisfied between the smartphone and the first entity;
10[g]	receiving, using the first air interface, a short-range signal from the first entity; and

Claim	Limitation
10[h]	responsive to receiving the short-range signal from the first entity, sending to the first entity over the first air interface, information based on the second data received from the first device; and
10[i]	independent of performing a transaction to pay for one or more items, receiving by the smartphone a communications service from a wireless network, using a second air interface that differs from the first air interface,
10[j]	wherein said transmitting first data and said receiving second data are performed over an air interface that differs from the first air interface.
11[pre]	The smartphone of claim 10,
11[a]	wherein establishing the wireless short-range communications link between the smartphone and the first entity is performed responsive to at least one physiological parameter having been sensed by at least one sensor of the smartphone.
12[pre]	The smartphone of claim 10,
12[a]	wherein sending by the smartphone to the first entity, information based on the second data, is performed responsive to at least one physiological parameter having been sensed by at least one sensor of the smartphone.
13[pre]	The smartphone of claim 10,
13[a]	wherein sending by the smartphone to the first entity, information based on the second data, is performed responsive to a value of at least one parameter associated with the smartphone.
14[pre]	The smartphone of claim 10, wherein the operations further comprise:
14[a]	performing a second financial transaction of the plurality of financial transactions by:
14[b]	detecting by the smartphone that a proximity condition is satisfied between the smartphone and a second entity; wherein the second entity is distinct from the first entity and is further distinct from the first device;

Claim	Limitation
14[c]	establishing, using the first air interface, a wireless short-range communications link between the smartphone and the second entity, in response to the proximity condition having been satisfied between the smartphone and the second entity;
14[d]	receiving, using the first air interface, a short-range signal from the second entity; and
14[e]	responsive to receiving the short-range signal from the second entity, sending by the smartphone to the second entity over the first air interface; information associated with the second data received from the first device.
15[pre]	The smartphone of claim 10,
15[a]	wherein said transmitting by the smartphone first data to a first device includes transmitting by the smartphone data relating to a request to pay for a transaction; and
15[b]	wherein said receiving by the smartphone second data from the first device includes receiving by the smartphone data relating to an acknowledgement and/or authorization of enabling a mode/function to pay for a transaction.
16[pre]	The smartphone of claim 10, wherein said operations further comprise:
16[a]	transmitting third data to a second device; the second device being distinct from the first device and further being distinct from the first entity; and
16[b]	receiving by the smartphone fourth data from the second device relating to an acknowledgement and/or authorization of enabling a mode/function to pay for a financial transaction;
16[c]	wherein said transmitting by the smartphone third data to a second device and said receiving by the smartphone fourth data from the second device are performed over the air interface that differs from the first air interface.

Claim	Limitation
17[pre]	The smartphone of claim 10, wherein said operations further comprise:
17[a]	responsive to performing a financial transaction, causing data to be transmitted selectively to a plurality of predetermined devices and further causing data to be received selectively from said plurality of predetermined devices.

I. INTRODUCTION

Telcom Ventures LLC (“Telcom Ventures” or “Patent Owner”) respectfully submits this Preliminary Response (“POPR”) requesting that the Director deny institution of the Petition for *inter partes* review (Paper 1, “Petition,” or “Pet.”) filed by Petitioner Apple Inc. (“Apple” or “Petitioner”).

The Petition seeks *inter partes* review (“IPR”) of claims 1-17 (the “Challenged Claims”) of U.S. Patent No. 10,674,432 (the “’432 Patent,” Ex. 1001). While the Petition sets forth eight grounds, Petitioner relies on U.S. Patent No. 8,229,852 to Carlson (“Carlson,” Ex. 1005) in combination with other references in each of these grounds. Indeed, the Petition relies heavily on multi-reference combinations in an attempt to cobble together a system that allegedly meets the claimed inventions of the ’432 Patent.

Petitioner’s combinations fail for several reasons. First, across all eight grounds, the Petition fails to show that “information requesting an authorization” is taught or rendered obvious by the prior art. Petitioner relies only on Carlson’s alleged request for a pseudo primary account identifier (“PPAI”) as information requesting an authorization to perform a particular transaction. Pet. 29-33 (Grounds 1-4), 78 (incorporating analysis of Grounds 1-4 in Grounds 5-8). But Carlson’s request for PPAI is not a request for authorization for a particular transaction, nor would Carlson’s disclosure render this limitation obvious to a person of ordinary

skill in the art (“POSITA”). Instead, Carlson’s request for PPAI is simply a communication, based on already authorized and stored customer account information, for an identifier that is used as a proxy to protect the consumer’s real account information during a transaction. Carlson’s request for PPAI is not and cannot be information requesting an authorization because Carlson’s transaction may go forward without the device requesting or receiving the PPAI at all. Moreover, Carlson itself undercuts Petitioner’s theory because in Carlson’s system, authorization of particular transactions is achieved by a different “authorization request message” that is transmitted by the merchant—not by any part of Carlson’s system.

Second, in Grounds 1-4, Petitioner fails to show that a POSITA would have been motivated to combine Carlson’s device with Holloway’s fingerprint scanner to render obvious “responsive to at least one physiological parameter . . . enabling a mode to communicate by the smartphone information requesting an authorization” because neither Carlson nor Holloway suggest using biometrics to enable a mode to communicate the PPAI request. Specifically, Petitioner’s expert, Mr. Lipoff, fails to demonstrate that a POSITA would have used Holloway’s fingerprint scanner to enable Carlson’s request for PPAI, which, as admitted by Petitioner, is required to meet the claims. Indeed, even in the embodiments relied on by Peititoner, Carlson teaches that the request for a PPAI “need not occur only after” a user has unlocked

the device. *See* Carlson, 7:7-11. Thus, Carlson's device is always capable of requesting and receiving a PPAI, and a mode to communicate a request for PPAI is not necessarily enabled responsive to a physiological parameter. Worse still, Holloway is silent on the use of biometrics for the purposes of requesting account identifiers, especially "fake" ones. Instead, Holloway relates to biometrics and/or user verification before funds can be transferred. Petitioner has not demonstrated and cannot demonstrate that the added burden of the biometrics of Holloway would have benefitted a request for PPAI. Lastly, Carlson teaches away from using slow and complex biometric authentication for its request for PPAI, because Carlson teaches using a request that is transparent to the user and does not cause any delay.

Finally, in Grounds 5-8, like in Grounds 1-4, Petitioner again fails to show that a POSITA would have been motivated to combine Carlson's device with Murakami's biometric authentication device to render obvious "responsive to at least one physiological parameter . . . enabling a mode to communicate by the smartphone information requesting an authorization." As with Grounds 1-4, Carlson itself does not suggest using biometrics to enable a mode to communicate a PPAI request. And like the Holloway combination, the additional biometrics in the form of a heartbeat sensor of Murakami would defy Carlson's stated goal of having the request for PPAI be instantaneous and not result in delays. Murakami itself acknowledges that its own

biometric sensor can be “impractical” because of the time it takes to capture a good sample. *See* Murakami, 33:4-6.

Accordingly, the Petition fails to establish that any ground would have rendered the Challenged Claims obvious. Petitioner has failed to meet its burden to show a reasonable likelihood of unpatentability of any of the Challenged Claims. *See* 37 CFR § 42.108(c). Accordingly, Patent Owner requests that the Director deny institution of *inter partes* review.

II. LEGAL STANDARD

The Petition must both “clearly point out the differences between the claimed invention and [the prior art]” and “explain why a person of ordinary skill in the art would have found the claimed subject matter obvious in spite of those differences.” *Synopsys, Inc. v. Mentor Graphics Corp.*, IPR2012-00041, Paper 16 at 14 (P.T.A.B. Feb. 22, 2013). The Petition must recite where the challenged limitation is found in the reference(s) and explain why a POSITA would have modified the primary reference with the recited limitation from the secondary reference(s). *Microsoft Corp. v. Secure Web Conf. Corp.*, IPR2014-00745, Paper 12 at 11-13 (P.T.A.B. Sept. 29, 2014). The Petition must establish, ***with particularity***, the grounds and evidence that support invalidating the challenged claims. 35 U.S.C. § 312(a)(3). In addition, the Director institutes based on what the Petition ***actually presents*** and not what it could have reasonably contained. *In re Magnum Oil Tools Int’l, Ltd.*, 829

F.3d 1364, 1381 (Fed. Cir. 2016). The Director cannot “deviate from the grounds in the petition and raise its own” theories of invalidity. *Sirona Dental Sys. GmbH v. Institut Straumann AH*, 892 F.3d 1349, 1356 (Fed. Cir. 2018).

III. BACKGROUND

A. The '432 Patent

Applicants filed U.S. Patent Application No. 16/251,834 on January 18, 2019, and the '432 Patent issued on June 2, 2020. Ex. 1002 at 58, 356. The '432 Patent claims the benefit of U.S. Patent Application No. 12/264,711—later issued as U.S. Patent No. 9,462,411—which has a filing date of November 4, 2008. Ex. 1001 at (63).

The '432 Patent describes mobile wireless devices and methods of using a mobile wireless device to perform financial transactions, but only when certain conditions or criteria are met, such as the satisfaction of a proximity condition and a criterion for the value of a parameter, e.g., a physiological parameter. '432 Patent, 1:22-27; 6:14-25; *see also* Ex. 2006 ¶¶61. In the prior art, mobile wireless devices were rigidly configured to perform a predetermined number of functions. '432 Patent, 1:36-41; *see also* Ex. 2006 ¶¶61. To overcome this rigidity, the '432 Patent describes devices and methods that “may be used to enable adaptively one or more modes/functions of a device” based upon satisfying certain criteria. '432 Patent, 1:45-51; *see also* Ex. 2006 ¶¶61. The '432 Patent explains that the invention

advantageously allows “a mobile wireless device [to] act as a ‘wallet’ (over and above other functions) only when it is time to pay for an item and not act as a wallet when there is no need to do so.” ’432 Patent, 1:41-44; *see also* Ex. 2006 ¶61.

The ’432 Patent also describes estimating “a value of at least one other parameter that may be associated with the wireless communications device . . . and/or an entity (living or otherwise) that is associated with and/or is proximate to the wireless communications device.” ’432 Patent, 6:14-20; *see also* Ex. 2006 ¶62. Such parameters include “velocity, acceleration, ToD, ToM, ToY, humidity, temperature, height, level of brightness, level of darkness, a blood pressure, a heart rate, a blood content, a physiological state, a psychological state, etc.” ’432 Patent, 6:20-25; *see also* Ex. 2006 ¶62. These parameters can be estimated using “sensors that may, according to some embodiments, be device-based and/or network assisted/based means and/or sensors.” ’432 Patent, 6:25-31; *see also* Ex. 2006 ¶62. The disclosed wireless communications devices may be “configured to selectively enable the first communications mode/function” responsive to a value of such a parameter. ’432 Patent, 6:41-50; *see also* Ex. 2006 ¶62.

During prosecution, the Examiner rejected proposed Claims 1-19 under 35 U.S.C. § 103 as being unpatentable over Dua in view of Creamer et al. (US 2004/0143550). Ex. 1002 at 169. Applicants filed a request for continued examination along with a response. Ex. 1002 at 233-254. Applicants noted that

“Amended claim 1 recites in pertinent part: responsive to at least one physiological parameter having been sensed by at least one sensor of the smartphone, enabling a mode to communicate by the smartphone information requesting an authorization” Ex. 1002 at 253. Applicants also stated:

The Final Office Action asserted that paragraphs [0026], [0089], and [0495] of Dua taught “the service parameters interaction based on the transaction reads on a physiological parameter”. None of these paragraphs, however, nor anywhere else in Dua or Creamer, teach or suggest “enabling a mode to communicate . . . responsive to at least one physiological parameter . . .” as recited in amended claim 1. Independent claims 5, 9, and 14 include similar language.

Ex. 1002 at 253. A Notice of Allowance issued on April 22, 2020. Ex. 1002 at 269-278. The Examiner stated in the Notice of Allowance that:

Dua alone or in combination fails [to] teach[] or fairly suggest[:] responsive to at least one physiological parameter having been sensed by at least one sensor of the smartphone, enabling a mode to communicate by the smartphone information requesting an authorization; while the mode is enabled, transmitting by the smartphone first data to a first device, the first data relating to a plurality of financial transactions to be conducted; . . . independent of performing said first transaction, receiving by the smartphone a communications service from a wireless network, using a second air interface that differs from the first air interface, wherein said transmitting by the smartphone first data and said receiving by the smartphone second data are performed over an air interface that differs from the first air interface.

Ex. 1002 at 275-276 (emphasis in original).

B. Carlson (Ex. 1005)

U.S. Patent No. 8,229,852 to Carlson is titled “Secure Mobile Payment System.” Carlson describes portable wireless devices that are used to conduct contactless payment transactions in a “secure manner.” Carlson, 1:16-20.

Carlson explains that “[d]ue to the wireless nature of the contactless reader, it is possible that the contactless reader may be used for surreptitious interrogation of the portable wireless device by intercepting the portable wireless device’s communication.” Carlson, 1:64-2:1. Carlson further explains that “it is conceivable that a contactless reader may be developed or modified to enhance its power and sensitivity and thereby increase its ability to interrogate with and intercept signals from the portable wireless device from a greater distance than specified in standards used for contactless readers.” Carlson, 2:1-6.

Carlson describes “[t]heft of sensitive information, such as an account number, using wireless interrogation or interception of communications from portable wireless device” as a “major concern for consumers and businesses alike.” Carlson, 2:7-10. Carlson notes that wireless interrogation can “occur at virtually any time and place,” and “[o]nce the victim of the wireless interrogation discovers that they had sensitive information stolen, it is often too late to discover where the theft took place.” Carlson, 2:10-16. As a result, “[t]he victim must then deal with the

consequences and hassle of correcting the unauthorized access and possible uses of the information.” Carlson, 2:16-18.

Carlson describes other “safeguards for protecting purchases from fraudulent attacks,” including employing encryption technologies to encrypt the payment account number and other data associated with account transactions. Carlson, 2:19-23. Carlson explains that many merchants avoid implementing or upgrading to the latest encryption technology “[d]ue to the cost, time, and risk of potential business interruption (e.g., loss of sales).” Carlson, 2:27-35.

Carlson’s solution describes the use of “pseudo primary account identifiers” or “PPAI.” Carlson, 2:62-63. According to Carlson, “[p]seudo primary account identifiers may include identifiers that are similar in format to a consumer’s real account identifier.” Carlson, 5:30-32. “These account identifiers may include account numbers or any other alphanumeric sequence.” Carlson, 2:66-3:1. Carlson also describes the PPAI as “bogus, fake, decoy, substitute, or the like.” Carlson, 5:42-43.

Carlson describes “a method for conducting a transaction that includes receiving a pseudo account identifier that corresponds to a consumer’s account identifier.” Carlson, 3:3-6. In some embodiments of Carlson, “the pseudo primary account identifier may not be requested at all, but rather is pushed to the portable wireless device at any time, such as when the device is turned on, when the device

is idle, periodically, or through any other such criteria.” Carlson, 7:4-7, 12:67-13:3. Carlson also explains that “the pseudo primary account identifier may not be requested by the portable wireless device at all” and “[t]he portable wireless device may generate the pseudo primary account identifier.” Carlson, 7:15-19.

C. Holloway (Ex. 1032)

International Patent Application Publication No. WO 02/49322 to Holloway is directed to a mobile telephone that “includes a device (15) for checking the identity of a user in connection with various transactions.” Holloway, Abstract.

Holloway proposes using a “means for checking the identity of a user of the unit” to solve the problem of identity verification. Holloway, 2:1-5. Holloway explains that “the means for telephonic communication includes a display, a microphone and a keypad and said means for checking identity is arranged to show a photograph of the user on said display, and/or means for recognizing the voice of the user and/or a password spoken by the user when the user speaks into said microphone, and/or incorporates means for identifying a PIN number entered by a user on said keypad.” Holloway, 2:14-18.

D. Jazayeri (Ex. 1007)

U.S. Patent Application Publication No. 2008/0155268 to Jazayeri is directed to “[a]n architecture . . . that controls access to secure data via biometric verification.” Jazayeri, Abstract. Jazayeri discloses a “memory module that

communicates with biometric data to establish a heightened level of security for controlling access to data stored in the non-volatile memory.” *Id.* “Specifically, biometric data is input and communicated to the security processor, then compared against the existing biometric templates stored in the non-volatile memory. If the data matches, verification is sent to the external processor and the user is granted access to the secure assets.” *Id.*

Jazayeri requires a security processor. Jazayeri, ¶[0006] (“As the security processor controls access to the entire non-volatile memory space and monitors all traffic to and from the non-volatile memory components, the security processor is able to manage access to the secure assets stored in the non-volatile memory.”); *see also* Jazayeri, ¶¶[0024], [0025], [0027], [0028], [0030], Figs. 1, 2; Ex. 2006, ¶79. Jazayeri explains that “[o]nly the security processor 104 accesses the security software from the nonvolatile memory 102 and performs security functions based on the specific security software being executed.” Jazayeri, ¶[0027].

Figure 3 of Jazayeri illustrates a block diagram of the Jazayeri’s security processor.

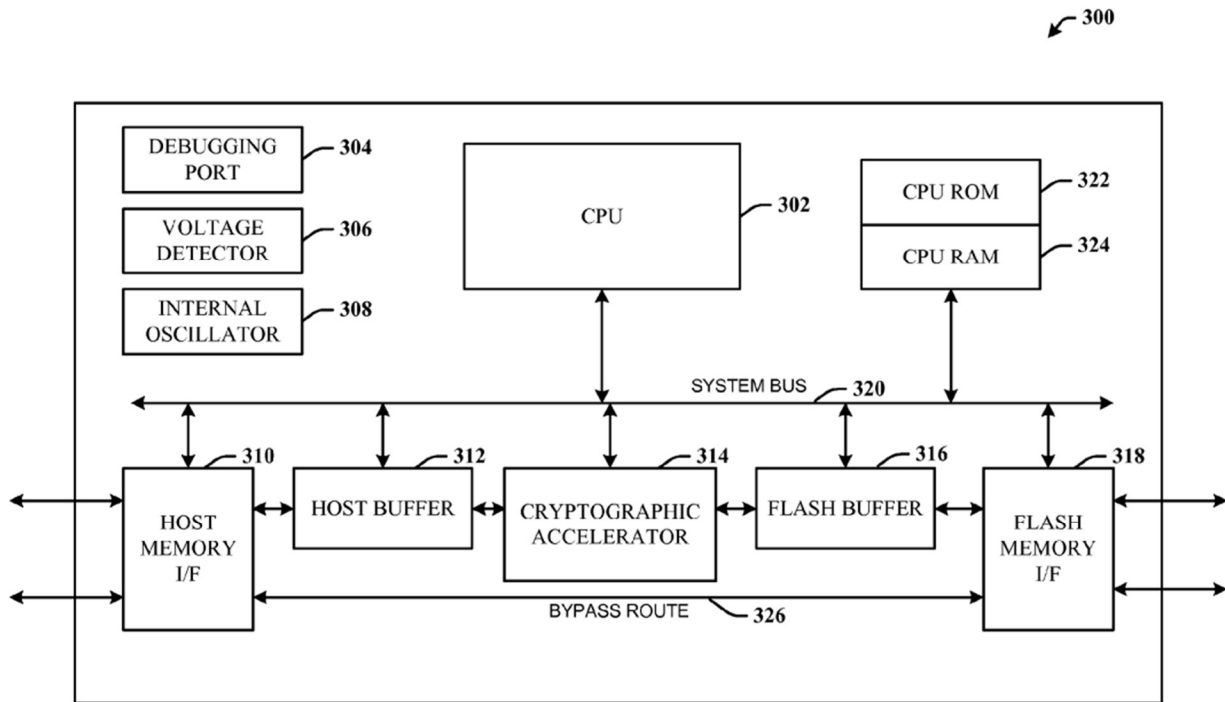


FIG. 3

Jazayeri, Fig. 3

Jazayeri’s security processor comprises sophisticated hardware. Jazayeri explains that “[a] cryptographic accelerator 314 . . . performs all the cryptographic algorithms, symmetric and a-symmetric needed by the system.” Jazayeri, ¶[0033].

E. ISO-14443 (Ex. 1016)

Petitioner relies on the first edition of ISO-14443 that Petitioner alleges was published in 2000 and 2001. Pet., 13 (citing Ex. 1033, Munford Declaration). The ISO/IEC 14443 standard has four parts. Ex. 2006 ¶81. ISO-14443 “is one of a series of International Standards describing the parameters for identification cards as defined in ISO/IEC 7810 and the use of such cards for international interchange.” ISO-14443, 4; Ex. 2006 ¶82.

F. Lin (Ex. 1030)

United States Patent No. 10,380,573 to Lin is directed to a method for “carrying out peer-to-peer financial transactions using one or more electronic devices.” Lin, Abstract. “In one embodiment, the group transaction members may include an initiator operating the electronic device. The initiator may initiate a primary transaction to pay the entirety of a group invoice containing amounts owed by each of the group transaction members. Thereafter, the initiator may perform one or more secondary transactions with each of the remaining group transaction members to collect the respective amounts owed.” Lin, 3:11-18.

G. Sherman (Ex. 1014)

U.S. Patent Application Publication No. 2007/0232358 to Sherman is directed to an “apparatus for and method of Bluetooth and WiMAX coexistence.” Sherman, Abstract. Sherman explains that WiMAX is “a long range system that uses licensed spectrum to deliver a point-to-point connection to the Internet from an ISP to an end user.” Sherman, ¶[0009].

H. Murakami (Ex. 1009)

International Patent Application Publication No. WO 01/95246 to Murakami is directed to “a method and device for biometric authentication using a signal transmitter (20), a signal receiver (22), a memory module, and a processing module.” Murakami, Abstract. Specifically, Murakami “employ[s] histological and physiological biometric markers that are substantially unique to an individual in

order to permit an individual to activate a device, participate in a transaction, or identify him or herself.” Murakami, 1:10-13.

IV. CLAIM CONSTRUCTION

Claim terms should be given their plain and ordinary meaning to a POSITA as of the earliest effective filing date. *See, e.g., Eon Corp. IP Holdings LLC v. Silver Spring Networks, Inc.*, 815 F.3d 1314, 1320 (Fed. Cir. 2016). “The ordinary meaning of a claim term is not ‘the meaning of the term in the abstract.’ Instead, ‘the “ordinary meaning” of a claim term is its meaning to the ordinary artisan after reading the entire patent.’” *Id.* (quoting *Philips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc)). With the sole exception described below, Petitioner contends that “no constructions are necessary to resolve the proposed grounds.” Pet., 4. Patent Owner agrees that the Board should apply the plain and ordinary meaning of the terms in the Challenged Claims. Patent Owner does not waive its right to raise additional issues of claim construction in any litigation, nor does it waive any argument that claim terms are not indefinite or are otherwise valid. The failure of the Petition to render obvious the Challenged Claims is clear in view of the arguments below without construing any specific claim term.

In Grounds 1-4, the Petition relies on a fingerprint to satisfy the claimed “physiological parameter” limitation. Pet., 6. The Petition then relies on Murakami’s biometric sensor for the “physiological parameter” limitation in Grounds 5-8. Pet., 6.

Because the Grounds fail regardless of the physiological parameter that the Petition relies on, a construction is not necessary for the purposes of institution. *Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (“The Board is required to construe ‘only those terms that . . . are in controversy only, and only to the extent necessary to resolve the controversy.’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))). Patent Owner reserves the right to address “physiological parameter” if this case is instituted.

V. LEVEL OF ORDINARY SKILL IN THE ART

Each of the arguments below is considered from the standpoint of a POSITA in the field of the '432 Patent at the time of the invention. Patent Owner contends that a POSITA would have had at least a bachelor's degree in electrical engineering, computer engineering, or a related field, with about two years of experience in wireless communications. Ex. 2006 ¶47. This is different from Petitioner's proposal, which calls for “a bachelor's degree in computer science, electrical engineering, computer engineering or equivalent from an accredited academic program with a year of work experience with mobile payment systems or wireless communication systems.” Pet., 6; Ex. 1003 ¶51. Petitioner also requires “a working knowledge of short-range communication technologies in portable wireless devices.” Pet. 6. Patent Owner disagrees that “a working knowledge of short-range communication

technologies” is necessary. Regardless, Petitioner fails to meet its burden under either POSITA definition.

VI. THE DIRECTOR SHOULD NOT INSTITUTE *INTER PARTES* REVIEW

All of Petitioner’s grounds fail. As described below, Petitioner’s combinations fail to render obvious all elements of any of the Challenged Claims. Petitioner’s proposed combinations are as follows:

Ground	Claims	Proposed Ground of Unpatentability
1	1-3, 5-6, and 10-15	Obvious under pre-AIA 35 U.S.C. § 103 over Carlson in view of Holloway and ISO-14443
2	7-8 and 16-17	Obvious under pre-AIA 35 U.S.C. § 103 over Carlson in view of Holloway, ISO-14443, and Lin
3	9	Obvious under pre-AIA 35 U.S.C. § 103 over Carlson in view of Holloway, ISO-14443, and Sherman
4	2-4 and 11-13	Obvious under pre-AIA 35 U.S.C. § 103 over Carlson in view of Holloway, ISO-14443, and Jazayeri
5	1-3, 5-6, and 10-15	Obvious under pre-AIA 35 U.S.C. § 103 over Carlson in view of Murakami and ISO-14443
6	7-8 and 16-17	Obvious under pre-AIA 35 U.S.C. § 103 over Carlson in view of Murakami, ISO-14443, and Lin
7	9	Obvious under pre-AIA 35 U.S.C. § 103 over Carlson in view of Murakami, ISO-14443, and Sherman
8	2-4 and 11-13	Obvious under pre-AIA 35 U.S.C. § 103 over Carlson in view of Murakami, ISO-14443, and Jazayeri

A. Petitioner Has Failed to Establish a Reasonable Likelihood that the Challenged Claims Would Have Been Obvious in View of Carlson in Combination with Holloway and/or Murakami (Grounds 1–8).

In Ground 1, Petitioner asserts that certain of the Challenged Claims, including independent claims 1 and 10, would have been obvious over Carlson in view of Holloway. Pet., 24-25. In Grounds 2-4, Petitioner adds additional secondary references in an attempt to show that certain dependent claims would have been obvious. Pet., 57, 68, 70. In Grounds 5-8, Petitioner replaces Holloway with Murakami. Pet., 78. In view of the deficiencies discussed below, Petitioner has failed to demonstrate a reasonable likelihood of prevailing on any of Grounds 1-8.

1. Carlson’s request for PPAI does not disclose and would not have rendered obvious “information requesting an authorization” (Grounds 1-8).

Carlson does not disclose and would not have rendered obvious “enabling a mode to communicate by the smartphone information requesting an authorization” of independent claims 1[a][ii] and 10[a]. *See* Ex. 2006 ¶¶91-105. All dependent claims depend from one of these two independent claims and thus include this same requirement.

Petitioner’s only argument as to this limitation is that Carlson’s request for PPAI is “information requesting an authorization to perform [a] particular transaction or particular limited set of transactions in Carlson’s system.” Pet., 29-33 (grounds 1-4); *see also* Pet., 78-79 (incorporating analysis of Carlson into grounds

5-8).¹ That is, Petitioner equates a PPAI to an authorization to perform a particular transaction or particular limited set of transactions.² However, for at least three key reasons, a POSITA would not have understood Carlson’s request for PPAI to be the claimed “information requesting an authorization” to perform a particular transaction.

First, the request for PPAI in Carlson is not “information requesting an authorization” to perform a particular transaction, as the Petition alleges, and Carlson’s disclosure of a request for PPAI would not have rendered this limitation obvious to a POSITA. Ex. 2006, ¶93. Carlson’s request for PPAI is not “information requesting an authorization”—or any type of authorization of a transaction—as it is simply a request for an identifier that can be used as a proxy for the consumer’s account identifier during a transaction. In fact, Carlson never describes or even suggests that the PPAI is an authorization to perform a transaction. Ex. 2006, ¶93.

¹ The Petition solely relies on Carlson and, thus, does not rely on Holloway in grounds 1-4 nor Murakami in grounds 5-8 for this part of the limitation.

² For the purposes of this IPR, Petitioner interprets the “authorization” of claims 1[a][ii] and 10[a] to be an authorization for a transaction or a set of transactions. *See* Pet., 29-33 (grounds 1-4); *see also* Pet., 78-79 (incorporating analysis of Carlson into grounds 5-8).

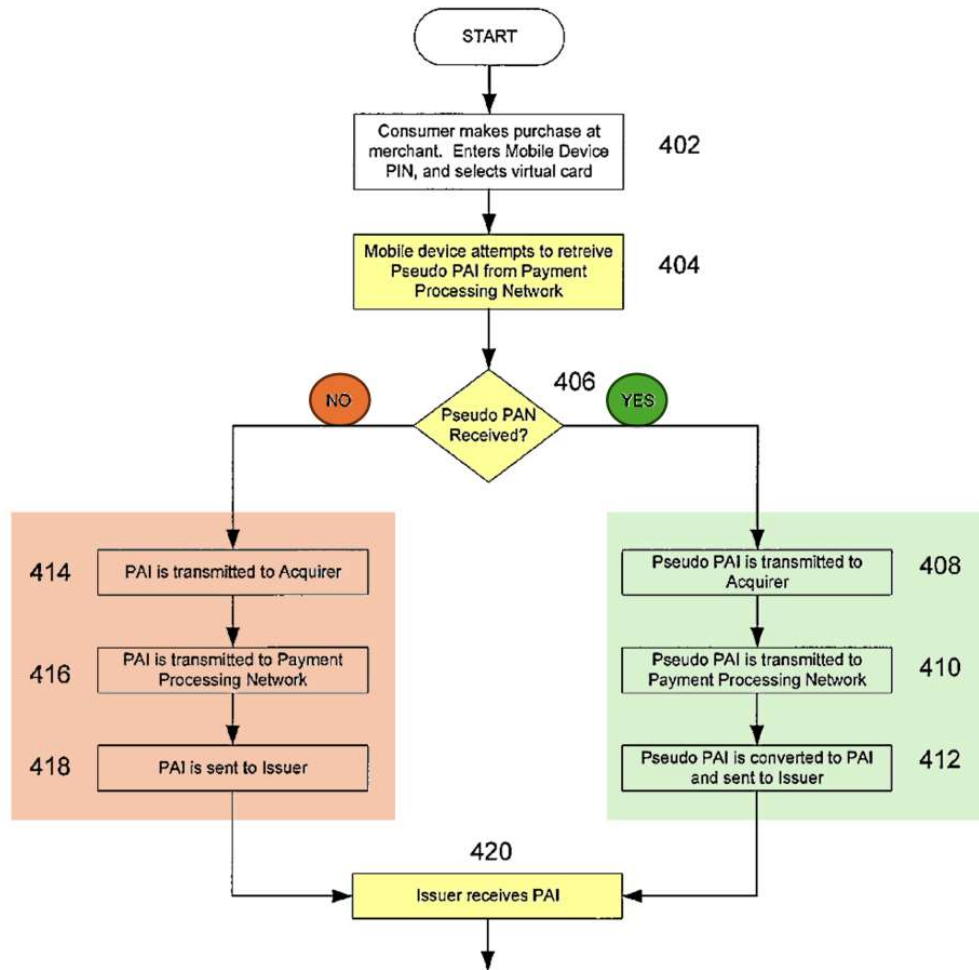
Instead, Carlson explains that a PPAI is used during a financial transaction, instead of the user's real account identifier, to protect the user from "[t]heft of sensitive information . . . using wireless interrogation or interception of communications from portable wireless device." Carlson, 2:7-10. According to Carlson, "[p]seudo primary account identifiers may include identifiers that are similar in format to a consumer's real account identifier." Carlson, 5:30-32, 2:66-3:1. Carlson also describes the PPAI as "bogus, fake, decoy, substitute, or the like." Carlson, 5:42-43. Just like a real account number that can be denied by a merchant, the PPAI can likewise be denied when used during a particular transaction. As a result, the PPAI is not and cannot be "an authorization" to perform a transaction, as the Petition alleges. Ex. 2006, ¶94.

Second, it follows that because the PPAI of Carlson is not an authorization, a *request* for PPAI is not information requesting an authorization. Ex. 2006, ¶95. Petitioner is relying on an embodiment of Carlson wherein the wireless device requests PPAI from the payment processing network. Pet. 29-30. According to the Petition, because Carlson's financial transaction "*requires* requesting and receiving the PPAI before the process may proceed" (Pet., 30 (emphasis added)), then the request for PPAI is necessarily information requesting an authorization for a particular transaction. But Petitioner is wrong. The mere fact that this embodiment

discloses *requesting* the PPAI does not transform the request for PPAI into information requesting *an authorization*. Ex. 2006, ¶95.

The purpose of requesting a PPAI in Carlson is so that Carlson's wireless device and the payment processing network can both associate the same PPAI with a user's real account information. See Carlson, 3:3-6, 6:48-50, 7:21-24. The user's authorized real account information is already on Carlson's wireless device at the time of requesting a PPAI. Carlson, 12:25-37 ("The user then may select which virtual card they wish to use to conduct the transaction 214. A virtual card corresponds to an account that the user has with an issuer and may be identified by the issuer through the use of a primary account identifier. . . . In this exemplary embodiment, the portable wireless device 202 may then request a pseudo primary account identifier that corresponds with a primary account identifier from the payment processing network 210."). Indeed, a financial transaction will proceed in Carlson regardless of whether a PPAI is received in response to a request for PPAI. For example, if a PPAI is *not* received in response to Carlson's request for PPAI, the particular transaction will *still* proceed using, for example, the primary account identifier—because a PPAI is not a necessary part of any particular financial transaction. Ex. 2006, ¶96. In Carlson's Figure 4, when the PPAI is not received in response to Carlson's request for PPAI, the transaction still continues with the user's

real account identifier (orange, below), instead of proceeding with a received PPAI (green, below). Carlson, 14:24-33; Ex. 2006, ¶96.



Carlson, Fig. 4 (cropped and annotated); Ex. 2006, ¶96.

Additionally, Carlson is clear that the PPAI “*may not be requested at all.*” Carlson, 7:4 (emphasis added). This further undercuts Petitioner’s argument that the request for PPAI is required for a particular transaction because there is no embodiment in Carlson that *requires* a request for PPAI prior to a particular transaction. Ex. 2006, ¶97. For example, the PPAI may be “pushed to the portable

wireless device at any time, such as when the device is turned on, when the device is idle, periodically, or through any other such criteria.” Carlson, 7:4-7, 12:67-13:3. As another example, Carlson discloses that “[t]he portable wireless device may generate the pseudo primary account identifier.” Carlson, 7:15-19. In embodiments where the PPAI is pushed or generated, the PPAI cannot act as an authorization for a particular transaction because the PPAI is unrelated to any particular transaction. Ex. 2006, ¶97.

Third, Carlson itself undercuts Petitioner’s theory that a request for a PPAI by Carlson’s device is “information requesting an authorization” sent by a smartphone. Carlson discloses a different message, an “authorization request message” sent by the merchant rather than Carlson’s wireless device, as a function for requesting an authorization of a particular transaction. Thus, the authorization of a transaction in Carlson depends on the “authorization request message” and not the call-and-response of an optional request for PPAI. As a result, a transaction authorization is agnostic to whether the PPAI is received, or if the PPAI request is even made. Ex. 2006, ¶98. Carlson discloses that, “[a]fter receiving the [PPAI] from the contactless device, the merchant may then use that identifier, as well as additional information to form an authorization request message.” Carlson, 8:10-13. “An authorization request message can include a request for authorization to conduct an electronic payment transaction or some other type of activity.” Carlson, 8:130-13.

“The payment processing network may then process the authorization message and return a response that indicates if the transaction is authorized or not.” Carlson, Abstract. As a result, it is the “authorization request message” sent by the merchant, not the request for PPAI sent by Carlson’s device, that drives authorization in the Carlson system. Ex. 2006, ¶98.

To be sure, even if the Petition had identified Carlson’s “authorization request message” instead of Carlson’s request for PPAI as the claimed “information requesting an authorization,” the mapping would still fail. Ex. 2006, ¶99. The claims require “enabling a mode to communicate *by the smartphone* information requesting an authorization.” Because Carlson’s “authorization request message” is sent *by the merchant*, the “authorization request message” cannot be the claimed “information requesting an authorization.” Carlson explains that the “authorization request message” is sent by the merchant—not by Carlson’s device—over a different logical network than the one used by Carlson’s device to request a PPAI. Carlson, 13:18-20, 13:23-27; *see also* Pet., 25 (arguing that Carlson’s device is the smartphone of the claims). Carlson further discloses that having the merchant send the authorization request message is an advantage because the PPAI is able to be sent over a different communication network than the one used to conduct the authorization for the transaction. Carlson, 15:50-53, 11:17-34, Fig. 1.

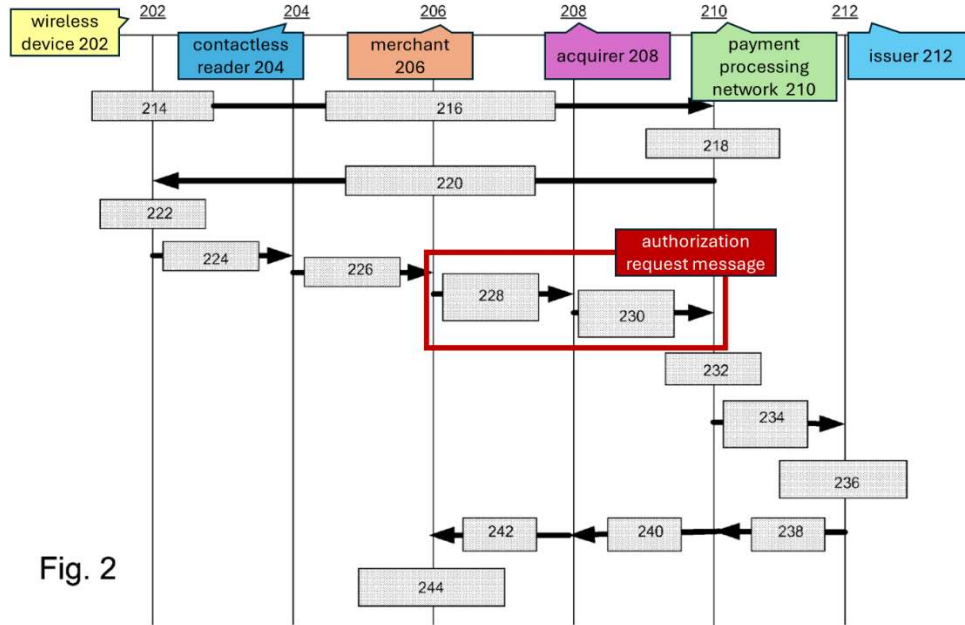


Fig. 2

Carlson, Fig. 2 (annotated); Ex. 2006, ¶199.

Having the “authorization request message” sent by the merchant instead of by Carlson’s device is also consistent with Carlson’s Figure 4, which shows an authorization step (purple, below) separate from Carlson’s device requesting and potentially receiving the PPAI (yellow).³

³ Notably, the Petition excerpts Carlson’s Figure 4 in a way that excludes the authorization step in purple below. *See* Pet., 60.

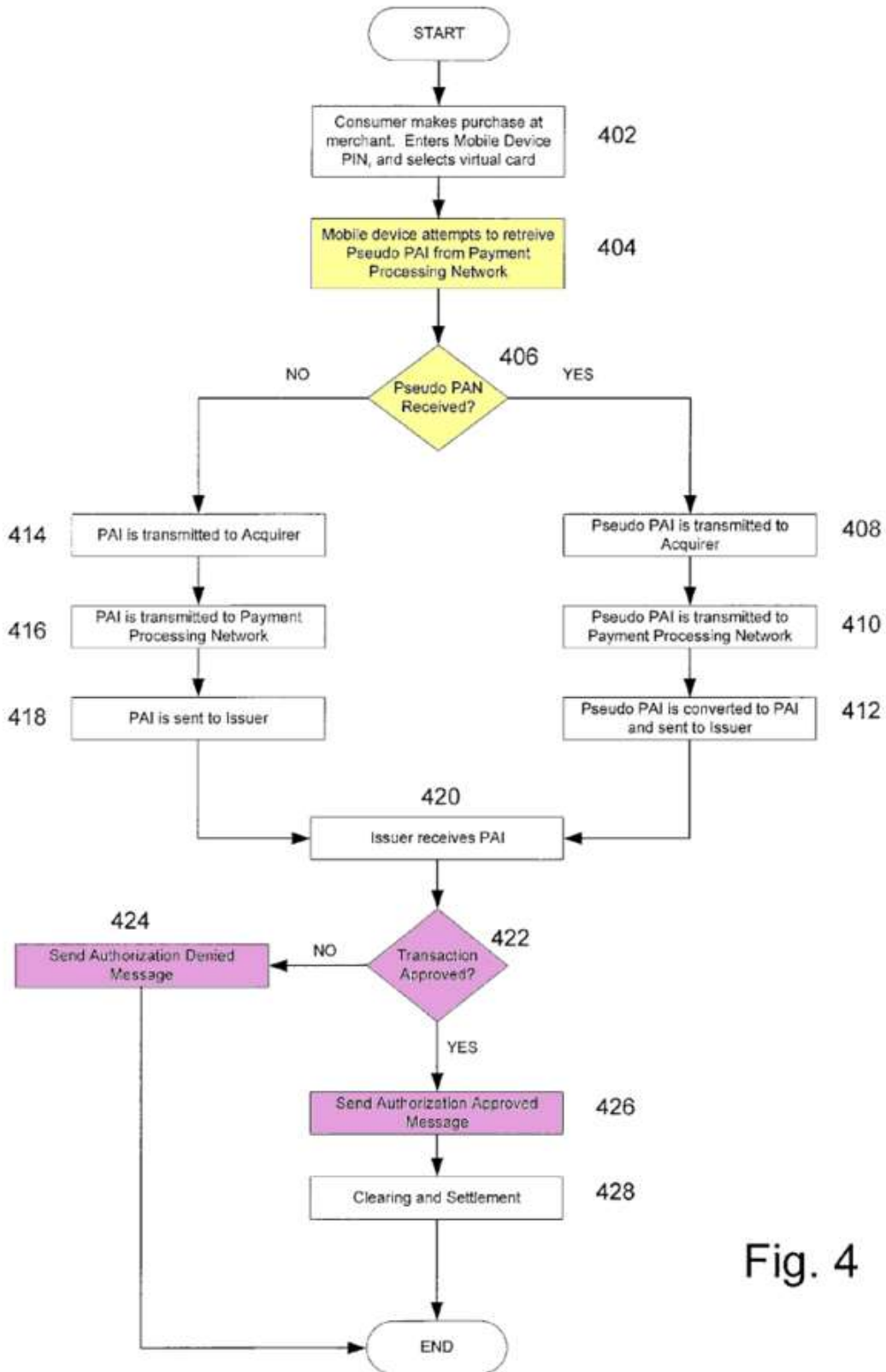


Fig. 4

Carlson, Fig. 4 (annotated); Ex. 2006, ¶100. Carlson then discloses that “the issuer receives the transaction request that contains the primary account identifier,” and that “[u]sing any number of criteria, such as the account specified by the primary account identifier being in good standing, having sufficient funds available, having sufficient credit available, etc., the issuer makes a decision at step 422 to either approve or deny the transaction.” Carlson, 14:34-40.

Petitioner does not dispute that Carlson does not actually require receiving a PPAI to conduct a financial transaction. Instead, the Petition acknowledges this major shortcoming in Carlson in a footnote. Petitioner’s footnote states that, because “[t]he proposed grounds rely on the PPAI-based financial transaction,” then “in the context of the proposed grounds, [the failure to receive the PPAI] serves as an indication that the function to conduct the PPAI-based financial transaction has *not* been established.” Pet., 33 n.6 (emphasis in original). The Petition then states that “[w]hile it may still be possible in Carlson’s system to conduct a different financial transaction (e.g., a less secure process that uses a PAN, rather than PPAI), the function relied upon in the Proposed Grounds is not established absent a PPAI.” *Id.* However, the Petition invents these two distinct secure and less secure transactions. Carlson contemplates just one exchange—one where, regardless of whether a PPAI is received in response to a request for the PPAI, the exact same financial account is debited for the exact same amount for the exact same purchase. Carlson, 14:34-46

(referring to Figure 4 showing that, regardless of whether a PPAI is received, “settlement and clearing processes occur at step 428 to actually transfer funds from the account held at the issuer to the merchant”); Ex. 2006, ¶101. Further, Petitioner continues to fail to appreciate that a PPAI-based financial transaction is still possible in Carlson without a response to a request for PPAI.⁴ Ex. 2006, ¶101. Because a PPAI-based financial transaction in such situations is still possible in Carlson, a request for PPAI is not information requesting an authorization to perform a PPAI-based financial transaction.

Even if Petitioner were correct that Carlson could be limited to a PPAI-based transaction, as described above, it is not true that a PPAI-based transaction requires *requesting and receiving* a PPAI before a PPAI-based transaction may proceed. Ex. 2006, ¶102. For example, the particular transaction may still (1) go forward without a response to the device’s request for PPAI, as set forth in Figure 4; or (2) go forward without any request at all, either because the PPAI was (i) pushed to the device independent of any request (Carlson, 7:3-15) or (ii) generated by the device itself (Carlson, 7:16-19). There is no embodiment in Carlson where the “particular transaction or particular limited set of transactions” “requires requesting and receiving the PPAI” as the Petition suggests. *See* Pet., 30. The request for PPAI

⁴ Petitioner’s error stems from its erroneous belief that the PPAI must be requested.

therefore does not disclose “information requesting an authorization” to perform a particular financial transaction. Ex. 2006, ¶102.

Additionally, a specific PPAI-based transaction may be authorized or unauthorized regardless of any use of the PPAI because Carlson’s “authorization request message”—sent by the merchant—is the functionality that actually authorizes a particular transaction. Carlson, 13:18-20. Carlson explains that authorization for a particular transaction in response to the “authorization request message” can be based on whether “the consumer conducting the transaction has sufficient funds or credit to conduct the transaction.” Carlson, 9:11-25. Therefore, a POSITA would not have understood Carlson’s request for PPAI to be “information requesting an authorization.” Ex. 2006, ¶103.

For at least these reasons, both Carlson in view of Holloway and Carlson in view of Murakami fail to disclose or render obvious “responsive to at least one physiological parameter . . . enabling a mode to communicate by the smartphone information requesting an authorization” of independent claims 1 and 10, and thus all dependent claims as well. Ex. 2006, ¶¶104-105.

2. **A POSITA would not have been motivated to combine Carlson’s device with Holloway’s fingerprint scanner to render obvious “responsive to at least one physiological parameter . . . enabling a mode to communicate by the smartphone information requesting an authorization” (Grounds 1-4).**

Claim limitations 1[a] and 10[a] require that “enabling a mode to communicate by the smartphone information requesting an authorization” is done “responsive to at least one physiological parameter having been sensed by at least one sensor of the smartphone.” The Petition’s only mapping for “information requesting an authorization” is Carlson’s request for a PPAI. Pet., 29-33. The Petition also argues that Holloway teaches using a fingerprint scanner to “initiate” and “complete” a transaction. Pet., 26-27. However, the Petition fails to show that a POSITA would have been motivated to combine Carlson and Holloway such that Holloway’s fingerprint scanner would be used to enable a mode to communicate Carlson’s PPAI request, because neither Holloway nor Carlson suggest using biometrics to enable a mode to communicate the PPAI request. Ex. 2006, ¶¶106-114.

The claims require that the mode to communicate information requesting an authorization is enabled “responsive to at least one physiological parameter.” The Petition argues that when the device is unlocked, a user is “allowed to proceed with a financial transaction.” Pet., 58 (citing Carlson, 12:18-24). At the same time, the Petition relies on a single embodiment in Carlson where the PPAI is requested by Carlson’s device, and the Petition identifies Carlson’s request for PPAI as the

“information requesting an authorization.” The Petition fails to show that Carlson’s mode to communicate a request for PPAI is enabled responsive to unlocking the device. Ex. 2006, ¶107.

In the very embodiment on which Petitioner relies, Carlson emphasizes that the device does not need to be unlocked for Carlson’s device to request a PPAI. Carlson, 7:7-11 (“[A] request for a [PPAI] need not occur only after a user has enabled the device and selected an account.”). Specifically, Carlson explains that “[a] request for a [PPAI] may occur *at any time*, such as when the device is turned on, when the device is idle, periodically, or through any other such criteria.” Carlson, 7:10-14 (emphasis added); *see also* Carlson, 6:59-61 (explaining that a PPAI can “expire after a certain number of transactions or after a certain time period”). A POSITA would therefore understand that Carlson’s device is always capable of requesting or receiving a PPAI—or at the very least, capable without Carlson’s device being unlocked. Thus, Carlson’s request for PPAI is *not* necessarily enabled responsive to unlocking the device. Ex. 2006, ¶108. This furthers Carlson’s stated objective of creating a “transparent” user experience such that the user “need not know that the pseudo account identifier is ever retrieved.” Carlson, 15:63-16:3; *see also* Ex. 2006, ¶108.

Additionally, and as described above, there are many other ways a PPAI could be received or generated without any request from the device itself, and thus without

unlocking the device. Specifically, Carlson teaches that the PPAI may never be requested but instead may be either pushed to the device by the network (Carlson, 7:3-6), or even generated by the device itself (Carlson, 7:17-18). These alternative embodiments do not require unlocking the device, nor do they require enabling a mode to communicate a request for PPAI. *See* Carlson, 7:3-6 (“The pseudo account identifier may not be requested at all, but rather is pushed to the portable wireless device *at any time*, such as when the device is turned on, when the device is idle, periodically, or through other such criteria.” (emphasis added)). Carlson therefore does not disclose, nor would it have rendered obvious, the use of a security measure such as a physiological parameter to enable a mode to communicate a PPAI request. Ex. 2006, ¶109.

Further, a POSITA would not have been motivated to combine Holloway and Carlson to render obvious “enabling a mode to communicate information requesting an authorization” “responsive to at least one physiological parameter.” Holloway itself is silent on the use of biometrics for the purpose of requesting an account identifier, especially fake ones used to avoid the transmission of sensitive information. Instead, Holloway is directed to using biometrics for loading funds directly into a device so that the device may then be used like an RFID smart card. Holloway, 6:13-17, 6:22-26. It is the transfer of actual funds to the device that calls for the additional security measures by the operator of Holloway’s device during the

transaction. Ex. 2006, ¶110. Once transferred, a user cannot claw back the funds, and the user has no remedial action. *Id.*

On the other hand, Carlson’s request for PPAI does not require “increased security” (Pet., 28) because Carlson’s request for PPAI does not involve the immediate and irreversible transfer of funds. Ex. 2006, ¶111. First, Carlson teaches that transmitting the PPAI over a communications network (e.g., during the request for PPAI) is relatively safer than transmitting sensitive information using short range communication because of the ability to use “highly effective” encryption techniques. Carlson, 2:19-27, 9:45-50. Indeed, even if intercepted, Carlson notes that the PPAI will likely be expired before it could be used by a bad actor. *See* Carlson, 6:59-65. Therefore, a POSITA would not have been motivated to implement a slow, complex biometric authentication method. Ex. 2006, ¶111.

Second, Carlson fully embraces that sensitive information may be “intercepted while the user is making a legitimate purchase.” Carlson, 2:1-6, 2:46-48. Carlson is directed to *minimizing the impacts* of having a signal intercepted by a bad actor—not to *preventing* theft of information. Ex. 2006, ¶112. Carlson solves this problem by using the PPAI to avoid sending sensitive information in the first place. Carlson, 2:49-53, 2:59-61. To further this objective, Carlson explains that “the pseudo primary account number may be set to expire after a certain number of transactions or after a certain time period” and “[d]oing so can help to ensure that if

for some reason a pseudo primary account number is revealed to anyone other than an authorized user, the amount of damage that can be done is limited due to the limited lifetime of the pseudo primary account number.” Carlson, 6:59-65. Thus, Carlson teaches that even if the PPAI is intercepted, the effects are limited. Carlson further teaches that its “authorization request message” is intended to protect the user in the event the user’s information is reported as stolen. Carlson, 9:13-17. A POSITA therefore would not have been motivated to implement additional security techniques that delay the financial transaction in Carlson, which would be contrary to Carlson’s stated objectives. Carlson, 16:63-67 (stating that the user should not “experience any delay in conducting the purchase” due to requesting the PPAI); *see also* Ex. 2006, ¶112.

The disclosure in Carlson of a request for a temporary, replaceable, and limited-use PPAI is in sharp contrast to Holloway’s direct transfer of funds at a device over the internet. While the transfer of funds in Holloway might have called for user verification, that is because the very interception of that information is necessarily dangerous because it results in immediate and irreversible transfer of electronic funds. Ex. 2006, ¶113. That is not so for Carlson’s request for PPAI, because (1) the request for PPAI can be protected using encryption, (2) Carlson’s PPAI is set to expire to minimize the effects of the interception of the PPAI, and (3) Carlson’s financial transactions include other safeguards, like the “authorization

request message.” Therefore, a POSITA would not have been motivated to implement Holloway’s fingerprint sensor to “enabl[e] a mode to communicate by the smartphone” a request for PPAI. *Id.*

For at least these reasons, a POSITA would not have been motivated to combine Carlson and Holloway to render obvious “responsive to at least one physiological parameter . . . enabling a mode to communicate by the smartphone information requesting an authorization.” Therefore, claim limitation 1[a] and 10[a] of independent claims 1 and 10 are not disclosed in or rendered obvious by the asserted prior art, and thus all dependent claims are also not disclosed in or rendered obvious by the asserted art. Ex. 2006, ¶114.

3. A POSITA would not have been motivated to combine Carlson’s device with the biometric authentication device of Murakami to render obvious “responsive to at least one physiological parameter . . . enabling a mode to communicate by the smartphone information requesting an authorization” (Grounds 5-8).

The Petition states that “[i]n Grounds 5-8, in place of Holloway, the proposed combination involves modifying Carlson pursuant to Murakami’s biometric sensor and authentication process.” Pet., 79. For the same reasons a POSITA would not have combined Carlson with Holloway, a POSITA would not have been motivated to combine Carlson with Murakami to render obvious “responsive to at least one physiological parameter . . . enabling a mode to communicate by the smartphone

information requesting an authorization.” *See supra* Section VI.A.2; Ex. 2006, ¶¶115-120.

The Petition argues that “Carlson modified to unlock its device pursuant to the biometric authentication process described by Murakami teaches the claimed physiological parameter limitations.” Pet., 81. However, as discussed above, Carlson does not require that its device be unlocked to enable its request for PPAI. Carlson, 7:7-11 (“[A] request for a [PPAI] need not occur only after a user has enabled the device and selected an account.”). Because Carlson’s wireless device is always capable of requesting a PPAI, Carlson’s request for a PPAI is *not* necessarily enabled responsively to unlocking the device. Thus, unlocking the device using the biometric authentication process described by Murakami does not render obvious “enabling a mode to communicate” “responsive to at least one physiological parameter.” Ex. 2006, ¶117.

Additionally, Murakami (in place of Holloway) does not overcome the deficiencies of the Carlson-Holloway combination. Ex. 2006, ¶118. Petitioner relies on Murakami’s sensor “used to measure a heartbeat waveform, a dynamic variable determined by measuring a user’s heartbeat.” Pet., 78-79 (citing Murakami 32:30-33:6). Specifically, the Petition relies on an embodiment wherein a waveform is monitored, and “25 features are extracted out of a waveform to create a list of 25 parameters, each parameter requesting a different unique feature for a particular

person's heartbeat waveform." Murakami, 32:20-22. Murakami teaches "tak[ing] more than one reading of the biometric for purposes of individualization." Murakami, 32:31-33:1. "In one preferred embodiment 30 heartbeats were taken and monitored to do the individualization for each person being identified. In another preferred embodiment, a hundred heartbeats were used. In capturing a good sample, it is preferred to take as many samples as is possible." Murakami, 33:1-4. Murakami even acknowledges that "taking a large number of sample waveforms takes time and using an extended period of time to individualize the waveform may be impractical." Murakami, 33:4-6. As a result, a POSITA would have understood that Murakami's biometric sensor provides updated security but at the expense of a significant amount of the user's time. Ex. 2006, ¶118. A POSITA would not have been motivated to implement Murakami's biometric sensor for everyday use or for functionalities that require little or no delay. Ex. 2006, ¶118.

The PPAI request in Carlson is supposed to be "transparent" to the user. Carlson, 15:67-16:3. Therefore, a POSITA would have understood that Carlson teaches away from using Murakami's biometric sensor for its PPAI request because the Murakami sensor would be inconvenient and cause unwanted delay. Ex. 2006, ¶119. A POSITA would have understood that the added security from the heartbeat sensor of Murakami would not be beneficial in Carlson's system because Carlson emphasizes that the user should not "experience any delay in conducting [a]

purchase.” Carlson, 15:63-67. Therefore, a POSITA would not have been motivated to implement Murakami’s biometric sensor in Carlson’s device because of the delay introduced. Ex. 2006, ¶119.

For at least these reasons, a POSITA would not have been motivated to combine Carlson with Murakami, and this claim limitation is not disclosed in or rendered obvious by the asserted prior art. Ex. 2006, ¶120.

VII. CONCLUSION

For the foregoing reasons, institution should be denied.

Dated: November 6, 2025

Respectfully submitted,

By: / Christopher TL Douglas /
Christopher TL Douglas
Reg. No. 56,950

CERTIFICATION UNDER 37 C.F.R. §42.24(d)

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Patent Owner's Preliminary Response to Petition totals 7,698 which is less than the 14,000 allowed under 37 CFR § 42.24(b)(1).

Dated: November 6, 2025

By: / Christopher TL Douglas /
Christopher TL Douglas

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §42.6(e), the undersigned hereby certifies that true and correct copies of the above-captioned **PATENT OWNER'S PRELIMINARY RESPONSE and Exhibits 2006 – 2012** were served in their entirety on November 6, 2025 via filing through the Patent Trial and Appeal Case Tracking System (P-TACTS) and electronic mail on the following counsel of record for Petitioner:

Paul R. Hart
Paul.Hart@eriseip.com

Adam P. Seitz
Adam.Seitz@eriseip.com

Christina N. Canino
Christina.Canino@eriseip.com

Sten Larson
Sten.Larson@eriseip.com

Eric Brueckner
Eric.Brueckner@eriseip.com

Khoa Vu
Khoa.Vu@eriseip.com

Graeme Gillespie
Graeme.Gillespie@eriseip.com

Service email
PTAB@eriseip.com

Date: November 6, 2025

/Christopher TL Douglas/
Christopher Douglas
Reg. No. 56,950