

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

TELCOM VENTURES LLC,
Patent Owner

Case No. IPR2025-01236
U.S. Patent No. 11,770,756

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	LEGAL STANDARD	5
III.	BACKGROUND	6
	A. THE '756 PATENT	6
	B. <i>CARLSON</i> (EX. 1005)	9
	C. <i>HOLLOWAY</i> (EX. 1032)	11
	D. <i>JAZAYERI</i> (EX. 1007)	12
	E. <i>ISO-14443</i> (EX. 1016)	13
	F. <i>SHERMAN</i> (EX. 1014)	14
	G. <i>MURAKAMI</i> (EX. 1009)	14
IV.	CLAIM CONSTRUCTION	14
V.	LEVEL OF ORDINARY SKILL IN THE ART	16
VI.	THE DIRECTOR SHOULD NOT INSTITUTE <i>INTER PARTES</i> REVIEW	16
	A. GROUNDS 1-3 WOULD NOT HAVE RENDERED OBVIOUS THE CHALLENGED CLAIMS.	17
	1. <i>Carlson</i> in View of <i>Jazayeri</i> Would Not Have Rendered Obvious “determining” “a value of the parameter that is sensed.”	17
	B. GROUNDS 4-6 WOULD NOT HAVE RENDERED OBVIOUS THE CHALLENGED CLAIMS.	23
	1. <i>Carlson</i> in View of <i>Murakami</i> Would Not Have Rendered Obvious “determining” “a value of the parameter that is sensed.”	23
	C. GROUNDS 1-6 WOULD NOT HAVE RENDERED OBVIOUS CHALLENGED CLAIMS 3-5 AND 8-18.	27
	1. <i>Carlson</i> ’s Request for PPAI Does Not Teach and Would Not Have Rendered Obvious “requesting . . . from a	

second device an authorization to enable a function for
conducting a financial transaction by the device.” 27

VII. CONCLUSION 39

TABLE OF AUTHORITIES

	Page(s)
CASES	
<i>Chevron Oronite Co. v. Infineum USA LP</i> , IPR2018-00923, Paper 9 (P.T.A.B. Nov. 7, 2018).....	5
<i>Deeper, UAB v. Vexilar, Inc.</i> , IPR2018-01310, Paper 7 (P.T.A.B. Jan. 24, 2019)	5
<i>Eon Corp. IP Holdings LLC v. Silver Spring Networks, Inc.</i> , 815 F.3d 1314 (Fed. Cir. 2016)	14, 15
<i>In re Magnum Oil Tools Int’l, Ltd.</i> , 829 F.3d 1364 (Fed. Cir. 2016)	6
<i>Microsoft Corp. v. Secure Web Conf. Corp.</i> , IPR2014-00745, Paper 12 (P.T.A.B. Sept. 29, 2014).....	6
<i>Philips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005) (en banc)	15
<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)	6
<i>Synopsys, Inc. v. Mentor Graphics Corp.</i> , IPR2012-00041, Paper 16 (P.T.A.B. Feb. 22, 2013).....	5
<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	2, 8
35 U.S.C. § 312(a)(3).....	6
OTHER AUTHORITIES	
37 CFR § 42.108(c).....	5

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	Order Granting Joint Stipulation to Dismiss With Prejudice Counts I, II, V, and VIII of Telcom Ventures' Complaint
2003	Third Amended Docket Control Order
2004	Standing Order for Civil Cases Before Judge Rita F. Lin
2005	Telcom Ventures' Proposed Case Schedule for the Apple Litigation
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

Reference	Claim Limitation
Claim 1	
1[pre]	A method of operating a device, the method comprising:
1[a]	sensing by the device, using a device-based sensor, a parameter that is associated with the device, an environment of the device and/or a user of the device;
1[b]	determining by the device a value of the parameter that is sensed; and
1[c]	responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion, enabling by the device a number of functions of the device and disabling by the device a function of the device;
1[d]	wherein the parameter that is sensed using the device-based sensor, comprises a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state; and
1[e]	wherein the device comprises a smartphone.
Claim 2	
2[pre]	The method of claim 1,
2[a]	wherein said enabling by the device a number of functions of the device comprises enabling by the device a number of functions of the device that is greater than or equal to one.
Claim 3	
3[pre]	The method of claim 3, further comprising:
3[a]	while said number of functions is enabled by having sensed by the device the parameter and by having determined by the device that the value of the parameter that is sensed satisfies the threshold criterion, requesting by the device from a second device an authorization to enable a function for conducting a financial transaction by the device;
3[b]	responsive to the requesting, receiving by the device from the second device the authorization to enable the function for conducting the financial transaction; and
3[c]	responsive to receiving the authorization, enabling at the device the function for conducting the financial transaction.
Claim 4	
4[pre]	The method of claim 3,

Reference	Claim Limitation
4[a]	responsive to the device satisfying a proximity condition relative to an entity and responsive to the device sensing the parameter and determining the value that is associated with parameter that is sensed satisfies the threshold criterion, using by the device the function for conducting the financial transaction and conducting by the device the financial transaction by paying for a product.
Claim 5	
5[pre]	The method of claim 3, further comprising:
5[a]	enabling at the second device a function for conducting the financial transaction.
Claim 6	
6[pre]	A device that is configured to perform operations comprising:
6[a]	sensing by the device, using a device-based sensor, a parameter that is associated with the device, an environment of the device and/or a user of the device;
6[b]	determining by the device a value of the parameter that is sensed; and
6[c]	responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion, enabling by the device a number of functions of the device and disabling by the device a function of the device;
6[d]	wherein the parameter that is sensed using the device-based sensor, comprises a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state; and
6[e]	wherein the device comprises a smartphone.
Claim 7	
7[pre]	The method of claim 6,
7[a]	wherein said enabling by the device a number of functions of the device comprises enabling by the device a number of functions of the device that is greater than or equal to one.
Claim 8	
8[pre]	The device of claim 6, wherein the operations further comprise:
8[a]	while said number of functions is enabled by having sensed the parameter and by having determined by the device that the value of the parameter that is sensed satisfies the threshold criterion, requesting by the device from a second device an authorization to enable a function for conducting a financial transaction by the device;

Reference	Claim Limitation
8[b]	responsive to the requesting, receiving from the second device the authorization to enable the function for conducting the financial transaction; and
8[c]	responsive to receiving the authorization, enabling the function for conducting the financial transaction.
Claim 9	
9[pre]	The device of claim 8, wherein the operations further comprise:
9[a]	detecting by the device that a proximity condition has been satisfied between the device and an entity;
9[b]	sensing by the device the parameter and determining by the device the value that is associated with the parameter that is sensed satisfies the threshold criterion; and
9[c]	responsive to the value that is associated with the parameter that is sensed satisfying the threshold criterion, using by the device the function for conducting the financial transaction and conducting by the device the financial transaction by paying for a product.
Claim 10	
10[pre]	The device of claim 8, wherein the operations further comprise:
10[a]	causing a function for conducting the financial transaction to be enabled at the second device.
Claim 11	
11[pre]	A method of operating a wireless device, the method comprising:
11[a]	sensing by the wireless device, using a sensor of the wireless device, a parameter that is associated with the wireless device, an environment of the wireless device and/or a user of the wireless device;
11[b]	determining by the wireless device a value of the parameter that is sensed and determining by the wireless device whether or not the value that is sensed satisfies a threshold criterion;
11[c]	responsive to the value that is sensed satisfying the threshold criterion, enabling a number of functions of the wireless device and disabling a function of the wireless device;
11[d]	requesting by the wireless device from a second device an authorization to enable a function for conducting a financial transaction;
11[e]	responsive to the requesting, receiving by the wireless device from the second device the authorization to enable the function for conducting the financial transaction;

Reference	Claim Limitation
11[f]	responsive to receiving the authorization, enabling at the wireless device the function for conducting the financial transaction; and
11[g]	responsive to the wireless device satisfying a proximity condition relative to an entity and responsive to the wireless device sensing the parameter and determining that the value sensed satisfies the threshold criterion, using the function for conducting the financial transaction and conducting the financial transaction by paying for a product;
11[h]	wherein the parameter that is sensed, using the sensor of the wireless device, comprises a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state; and
11[i]	wherein the wireless device comprises a smartphone.
Claim 12	
12[pre]	The method of claim 11,
12[a]	wherein said enabling a number of functions of the wireless device comprises enabling a number of functions of the wireless device that is greater than or equal to one.
Claim 13	
13[pre]	The method of claim 11, further comprising:
13[a]	enabling at the second device a function for conducting the financial transaction.
Claim 14	
14[pre]	A wireless device that is configured to perform operations comprising:
14[a]	using a sensor of the wireless device and sensing a parameter that is associated with the wireless device, an environment of the wireless device and/or a user of the wireless device;
14[b]	determining a value that is associated with the parameter that is sensed and determining whether or not the value satisfies a threshold criterion;
14[c]	responsive to the value satisfying the threshold criterion, enabling a number of functions of the wireless device and disabling a function of the wireless device;
14[d]	requesting from a second device an authorization to enable a function for conducting a financial transaction;

Reference	Claim Limitation
14[e]	responsive to the requesting, receiving from the second device the authorization to enable the function for conducting the financial transaction;
14[f]	responsive to receiving the authorization, enabling the function for conducting the financial transaction; and
14[g]	responsive to the wireless device satisfying a proximity condition relative to an entity and responsive to the wireless device sensing the parameter and determining that the value of the parameter sensed satisfies the threshold criterion, using the function for conducting the financial transaction and conducting the financial transaction by paying for a product;
14[h]	wherein the parameter that is sensed comprises a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state; and
14[i]	wherein the wireless device comprises a smartphone.
Claim 15	
15[pre]	The smartphone of claim 9,
15[a]	wherein said enabling a number of functions of the wireless device comprises enabling a number of functions of the wireless device that is greater than or equal to one.
Claim 16	
16[pre]	The wireless device of claim 14, wherein the operations further comprise:
16[a]	causing a function for conducting the financial transaction to be enabled at the second device.
Claim 17	
17[pre]	The wireless device of claim 14, wherein said conducting the financial transaction by paying for a product comprises:
17[a]	establishing by the wireless device a short-range wireless link with the entity;
17[b]	wirelessly transmitting information to the entity using unlicensed frequencies; and
17[c]	wirelessly receiving information from the entity using unlicensed frequencies;
17[d]	wherein said wirelessly transmitting and said wirelessly receiving comprises using a time domain duplex protocol; and

Reference	Claim Limitation
17[e]	wherein said establishing by the wireless device a short-range wireless link with the entity comprises establishing the short-range wireless link with the entity responsive to the wireless device satisfying the proximity condition relative to the entity and responsive to the wireless device sensing the parameter and determining that the value associated therewith satisfies the threshold criterion.
Claim 18	
18[pre]	The wireless device of claim 14, wherein said requesting from a second device an authorization to enable a function for conducting a financial transaction and/or said receiving from the second device the authorization to enable the function for conducting the financial transaction comprises:
18[a]	establishing by the wireless device a link with the second device, comprising a wireless link that comprises a distance that is greater than a distance associated with the proximity condition;
18[b]	wirelessly transmitting information to the second device over said wireless link using unlicensed and/or licensed frequencies; and
18[c]	wirelessly receiving information from the second device over said wireless link using unlicensed and/or licensed frequencies;
18[d]	wherein said wirelessly transmitting and/or said wirelessly receiving comprises using an orthogonal frequency division multiplexing and/or orthogonal frequency division multiple access protocol; and
18[e]	wherein said establishing by the wireless device a link with the second device comprises establishing the link with the second device responsive to the wireless device sensing the parameter and determining that the value sensed satisfies the threshold criterion.

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 1-18 (the “Challenged Claims”) of U.S. Patent No. 11,770,756 (the “’756 Patent,” Ex. 1001). The Petition sets forth six Grounds. Pet., 19. In all Grounds, Petitioner relies on U.S. Patent No. 8,229,852 to *Carlson* (“*Carlson*,” Ex. 1005) in combination with up to five other secondary references. The Petition relies exclusively on multi-reference combinations in an attempt to cobble together a system that allegedly meets the claimed inventions of the ’756 Patent. The six separate Grounds are summarized in the below chart.

Ground	Claims	Proposed Ground of Unpatentability
1	Claims 1-3, 5-8, and 10	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> ¹ in view of <i>Holloway</i> ² and <i>Jazayeri</i> ³

¹ U.S. Patent No. 8,229,852 (“*Carlson*,” Ex. 1005).

² WIPO International Patent Application Publication No. WO 02/49322 (“*Holloway*,” Ex. 1032).

³ U.S. Patent Application Publication No. 2008/0155268 (“*Jazayeri*,” Ex. 1007).

Ground	Claims	Proposed Ground of Unpatentability
2	Claims 4, 9, and 11-17	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> in view of <i>Holloway</i> , <i>Jazayeri</i> , and <i>ISO-14443</i> ⁴
3	Claim 18	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> in view of <i>Holloway</i> , <i>Jazayeri</i> , <i>ISO-14443</i> , and <i>Sherman</i> ⁵
4	Claims 1-3, 5-8, and 10	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> in view of <i>Murakami</i> ⁶
5	Claims 4, 9, and 11-17	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> in view of <i>Jazayeri</i> , <i>ISO-14443</i> , and <i>Murakami</i>
6	Claim 18	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> in view of <i>Jazayeri</i> , <i>ISO-14443</i> , <i>Sherman</i> , and <i>Murakami</i> .

Petitioner divides the Grounds into two groups. Grounds 1-3 combine *Carlson* with *Holloway*, *Jazayeri*, and other references. Pet., 18. In Grounds 4-6, Petitioner replaces *Holloway*'s biometric sensor and *Jazayeri*'s authentication process with *Murakami*'s teachings. Pet., 72. Petitioner states that "Grounds 4-6 differ from Grounds 1-3 only in the proposed modifications to *Carlson* pertaining to the biometric sensor and authentication process" and "[i]n Grounds 4-6, in place of

⁴ ISO/IEC 14443 ("*ISO-14443*," Ex. 1016).

⁵ U.S. Patent Application Publication No. 2007/0232358 ("*Sherman*," Ex. 1014).

⁶ WIPO International Application Publication No. WO 01/95246 ("*Murakami*," Ex. 1009).

Holloway-Jazayeri, the proposed combination involves modifying *Carlson* pursuant to *Murakami*'s biometric sensor and authentication process." Pet., 72.

Petitioner's Grounds 1-3 would not have rendered obvious the Challenged Claims. **First**, Ground 1 would not have rendered obvious "determining . . . a value of the parameter that is sensed" of independent claim limitations 1[b], 6[b], and 11[b] nor the similar language of independent claim limitation 14[b]. Petitioner alleges that a POSITA would have modified *Carlson* "to unlock its device pursuant to the biometric authentication process described by *Jazayeri*." Pet., 24-25. However, a POSITA would not have been motivated to combine *Carlson* and *Jazayeri*. Petitioner underestimates the difficulties of combining the devices from the two references and fails to establish a motivation to modify *Carlson*'s device with the authentication system of *Jazayeri*.

Second, Petitioner's Grounds 4-6 similarly fail. Petitioner again fails to establish that a POSITA would have been motivated to combine *Carlson* with *Murakami* to render obvious claim limitations 1[b], 6[b], and 11[b] nor the similar language of claim limitation 14[b]. *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. A POSITA would not have been motivated to implement *Murakami*'s time-delayed biometric sensor to unlock *Carlson*'s device.

Third, across all six Grounds, with respect to independent claims 11 and 14 (and certain dependent claims that depend from independent claims 1 and 6) the Petition fails to show that “an authorization to enable a function for conducting a financial transaction by the device” is taught or rendered obvious by the prior art. *Carlson*’s pseudo primary account number (“PPAI”) is not an 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 requesting an authorization to perform a particular transaction 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.

Petitioner relies only on *Carlson*’s request for PPAI as the claimed authorization to perform a particular transaction in all six Grounds, implicating fourteen of the eighteen Challenged Claims. Pet. 30-32 (Ground 1, addressing dependent claim limitation 3[a]), 37 (incorporating analysis of claim limitation 3[a]

into dependent claim limitation 8[a]), 54 (incorporating analysis of claim limitation 3[a] into independent claim limitation 11[d]), 55 (incorporating analysis of claim limitation 3[a] into independent claim limitation 14[d]), 72 (incorporating analysis of Grounds 1-3 into Grounds 4-6). As applies here, the Board regularly denies institution under § 314(a) when instituting trial would not be an efficient use of the Board's time and resources—for example, where Petitioner fails to present a reasonable likelihood of prevailing with respect to a subset of grounds or challenged claims. *See, e.g., Chevron Oronite Co. v. Infineum USA LP*, IPR2018-00923, Paper 9, 9-11 (P.T.A.B. Nov. 7, 2018) (informative); *Deeper, UAB v. Vexilar, Inc.*, IPR2018-01310, Paper 7, 41-43 (P.T.A.B. Jan. 24, 2019) (informative).

Accordingly, the Petition fails to establish that any Ground would have rendered the Challenged Claims obvious, and 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 ’756 Patent

Applicants filed U.S. Patent Application No. 17/653,748 on March 7, 2022, which issued as U.S. Patent No. 11,770,756 on September 26, 2023. ’756 Patent at 1. The ’756 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. *Id.* at 2.

The ’756 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. '756 Patent, 1:25-30, 6:13-23; *see also* Ex. 2006, ¶61. In the prior art, mobile wireless devices were rigidly configured to perform a predetermined number of functions. '756 Patent, 1:39-44; *see also* Ex. 2006, ¶61. To overcome this rigidity, the '756 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. '756 Patent, 1:49-54; *see also* Ex. 2006, ¶61. The '756 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.” '756 Patent, 1:44-57; *see also* Ex. 2006, ¶61.

The '756 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.” '756 Patent, 6:15-19; *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.” '756 Patent, 6:20-23; *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.” ’756 Patent, 6:28-30; *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. ’756 Patent, 6:40-44; *see also* Ex. 2006, ¶62.

During prosecution, the Examiner issued a non-final rejection that rejected the claims as unpatentable under 35 U.S.C. § 103 over U.S. Patent Application Publication No. 2009/0058637 to Kuo et al. (“Kuo”) in view of U.S. Patent Application Publication No. 2003/0172028 to Abell et al. (“Abell”), and for double patenting over claims 1, 7, and 17 of U.S. Patent No. 11,304,118. Ex. 1002 at 104, 106. Following an amendment of the independent claims to include “responsive to the value that is determined . . . enabling . . . a number of functions . . . and disabling a function” and the filing of a terminal disclaimer, the Examiner allowed the claims. *Id.* at 206-07. In the Notice of Allowance, the Examiner explained that Kuo, as the closest prior art of record, alone or in combination failed to teach or suggest “responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion, enabling by the device a number of functions of the device and disabling by the device a function of the device.” *Id.* at 207.

B. *Carlson* (Ex. 1005)

U.S. Patent No. 8,229,852 to *Carlson* is titled “Secure Mobile Payment System.” *Carlson* is directed to 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 [a] 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 purchase 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 pseudo primary account identifier 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; *see also id.*, 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* describes “fingerprint scanning means, voice or password recognition means (e.g. using a microphone of the telephone), photograph display means (e.g. using a display (12) of the telephone) or retina recognition means.” *Id.*

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, ¶75. *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 *Jazayeri*’s security processor.

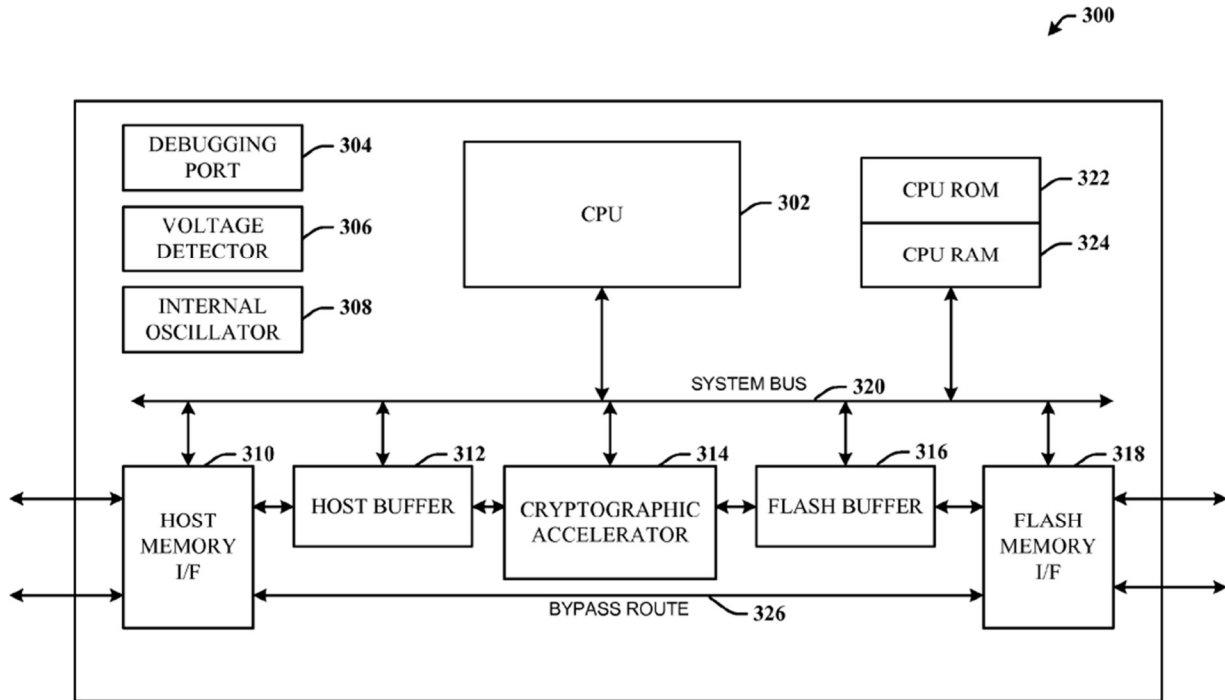


FIG. 3

Jazayeri, Fig. 3

Jazayeri's security processor comprises sophisticated hardware. Ex. 2006, ¶77. *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 2002. Pet., 13 (citing Ex. 1033, Munford Declaration). The ISO/IEC 14443 standard has four parts. Ex. 2006, ¶78. *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, ¶79.

F. *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].

G. *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 1-3, the Petition relies on a fingerprint to satisfy the claimed “physiological state” limitation. Pet., 6. The Petition then relies on *Murakami*’s biometric sensor for the “physiological state” limitation in Grounds 4-6. Pet., 6, 72. Because the Grounds fail regardless of the physiological state 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 state” 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 '756 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., 7; Ex. 1003, ¶51. Petitioner also requires “a working knowledge of short-range communication technologies in portable wireless devices.” Pet., 7. 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.

A. Grounds 1-3 Would Not Have Rendered Obvious the Challenged Claims.

In Ground 1, Petitioner asserts that independent Challenged Claims 1 and 6 and certain dependent Challenged Claims would have been obvious over *Carlson* in view of *Holloway* and *Jazayeri*. Pet., 18. In Ground 2, Petitioner asserts that independent Challenged Claims 11 and 14 and certain dependent Challenged Claims would have been obvious over *Carlson* in view of *Holloway*, *Jazayeri*, and *ISO-14443*. Pet., 18. In Ground 3, Petitioner asserts that an additional dependent Challenged Claim, which depends from claim 14, would have been obvious over *Carlson* in view of *Holloway*, *Jazayeri*, *ISO-14443*, and *Sherman*. Pet., 18. For the reasons set forth below, Grounds 1-3 all fail.

1. *Carlson* in View of *Jazayeri* Would Not Have Rendered Obvious “determining” “a value of the parameter that is sensed.”

Claim limitations 1[b], 6[b], and 11[b] state “determining . . . a value of the parameter that is sensed.” Claim limitation 14[b] similarly states “determining a value that is associated with the parameter that is sensed.” The Petition states that “*Carlson-Holloway-Jazayeri* teaches Claim 1(b).” Pet., 23; *see also* Pet., 37 (addressing limitation 6[b] with “[s]ee *supra* Claim 1(b)”), 54 (addressing limitation

11[b] with “[s]ee *supra* Claims 1(b)-(c)”), 55 (addressing limitation 14[b] with “[s]ee *supra* Claims 1(b)-(c)”).⁷ Petitioner’s Grounds 1-3 all fail. Ex. 2006, ¶¶88-97.

Petitioner states that “[l]ike *Carlson* and *Holloway*, *Jazayeri* discloses providing access to secure data on a device using biometric data such as ‘***fingerprint data*** . . . for identification and authentication purposes.” Pet., 23 (citing *Jazayeri*, ¶[0029]). The Petition does not identify any disclosures in *Carlson* or *Holloway* that disclose or render obvious limitation 1[b], nor does the Petition identify how *Carlson* or *Holloway* allegedly similarly disclose “providing access to secure data on a device using biometric data.” Based only on this disclosure in *Jazayeri*, the Petition concludes that a POSITA would have been motivated to “unlock” the *Carlson-Holloway* device “pursuant to the biometric authentication process described by

⁷ Claim limitation 1[c] states “responsive to the value . . . satisfying a threshold criterion” The Petition’s analysis of claim limitation 1[c] addresses “satisfying a threshold criterion” (Pet., 27-28), which is also required in claim limitations 11[b] and 14[b]. Given the difference in claim language, the Petition’s analysis and incorporation of 1[c] is not relevant to the analysis of whether *Carlson-Holloway-Jazayeri* teaches the “determining by the device a value of the parameter that is sensed” requirement in 11[b] and 14[b]. If this Petition is instituted, Patent Owner reserves the right to address the analysis of limitation 1[c].

Jazayeri.” Pet., 24-25. For the reasons explained below, Petitioner is incorrect. Ex. 2006, ¶89.

a. A POSITA Would Not Have Had a Reasonable Expectation of Success in Modifying Carlson with Jazayeri.

Petitioner’s proposed combination underestimates the difficulties that the POSITA, as defined by either expert, would have had in combining *Carlson* and *Jazayeri*, based on the system architecture of *Jazayeri*. Ex. 2006, ¶90. Specifically, *Jazayeri* depends on a security processor (Figure 1, Figure 2, ¶¶[0005]-[0006], [0023]-[0025], [0027]) and a cryptographic accelerator (Figure 3, ¶[0034]). *Jazayeri* ¶[0027] confirms the essential nature of the security processor as it states: “[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]; *see also* Ex. 2006, ¶90.

Here, Petitioner and Patent Owner agree that the proper definition of a POSITA would not include knowledge of security processor design or cryptography, but such knowledge is essential to understand the architecture of *Jazayeri*. *See supra*, § V. As such, a POSITA, as defined by Petitioner or Patent Owner, would not have been able to combine *Jazayeri* with any other prior art based at least on its complex architecture, which includes the security processor. Ex. 2006, ¶91.

The technical sophistication of the necessary security processor of *Jazayeri* that Petitioner proposes to add to the disclosures of *Carlson* undercuts Petitioner's theory that "a POSITA would have had a reasonable expectation of success when modifying *Carlson* according to *Jazayeri's* teachings." Pet., 26. Petitioner incorrectly asserts that "*Jazayeri's* biometric authentication technique requires simple components" and that "*Carlson's* wireless device already includes the necessary elements for *Jazayeri's* biometric authentication such as a memory and processor." Pet., 26 (citing *Carlson*, 14:47-59); *see also* Ex. 2006, ¶92. This is a misstatement of *Jazayeri*. Rather than rely on common elements, *Jazayeri* highlights that its security processor is specially designed for processing biometric data, and it is this security processor that passes verification data to another external processor. *Jazayeri*, ¶[0030]. That is, the security processor is necessary for any biometric authentication process disclosed in *Jazayeri*. Ex. 2006, ¶¶93-94. In fact, it is the "security processor 204 [that] will capture the user's biometric data via the biometric sensor 214 the compare the biometric data against biometric templates stored in the non-volatile memory 206 for verification." *Jazayeri*, ¶[0030]; *see also* Ex. 2006, ¶¶93-94. But Petitioner ignores the necessity of the security processor, failing to mention it at all in the Petition. Without this processor, *Jazayeri* has no mechanism for performing the disclosed verification process. Ex. 2006, ¶93.

Jazayeri discloses that “[t]he security processor provides for concurrent processing of security protocols, provides a secure execution environment within the memory module to evaluate and store biometric data, communicates either directly or indirectly with the biometric data sensors to fetch the biometric data, and analyzes the biometric data to control access to data or applications stored in the non-volatile memory.” *Jazayeri*, ¶[0005]. *Jazayeri* discloses that its specific security processor possesses specific features:

The security processor 300 includes a central processing unit (CPU) 302 or any other type of low power application processor. The CPU 302 within the security processor 300 can manage the flash memory storage (not shown) and provide a secure environment to implement authentication algorithms and security software. The security processor 300 also includes a Joint Test Action Group (JTAG) port 304 for debugging the system with a mechanism to prevent tampering, a voltage detector 306 that indicates the voltage level of the security processor 300 and stops the memory module from functioning when voltage levels are outside of the acceptable range in order to prevent side channel attacks, and an internal oscillator 308 that provides a clock for the security processor 300. This clock may be exported in its present form or it may be divided to provide the clock signal for other components such as a separate NFC RF chip or a fingerprint sensor. However, other mechanisms (not shown) can be provided that help prevent tampering. For example, temperature detecting, metal overlay (to hide signals), and scrambling of signals are additional methods that

can be utilized in the security processor 300. A host memory interface (I/F) 310 handles all the flash memory transactions with a host processor (not shown). Specifically the host memory I/F 310 manages signaling, thus complying with the interface definitions of the flash memory. The host memory I/F 310 also manages interpretation or differentiating between a secure and non-secure request, and monitors requests to the non-volatile memory to enforce access rights and permissions.

Jazayeri, ¶[0033]; *see also id.* at ¶¶[0034]-[0036], [0039], [0043]-[0044]; Ex. 2006, ¶94.

Jazayeri did not intend its security processor to be “common hardware elements,” as alleged by Petitioner. Instead, as disclosed in the detailed description and shown in the block diagram, *Jazayeri* disclosed a custom security processor to provide “a secure environment to implement authentication algorithms and security software.” *Jazayeri* ¶[0033]; *see also* Ex. 2006, ¶95. Because of the complexity introduced by *Jazayeri*’s implementation, a POSITA would not have had a reasonable expectation of success in combining *Carlson*’s device with *Jazayeri*’s complex security processor and authentication process. Ex. 2006, ¶95.

b. A POSITA Would Not Have Been Motivated to Combine Carlson with Jazayeri.

Furthermore, even if the combination were possible, there would have been no motivation to modify *Carlson*’s system with the biometric authentication process of *Jazayeri*. Petitioner combines *Carlson* with *Jazayeri* to “unlock its device

pursuant to the biometric authentication process described by *Jazayeri*.” Pet., 24. A POSITA would not have been motivated to combine *Carlson*’s device with *Jazayeri*’s authentication for the purposes of unlocking the device.

A POSITA would have readily understood that using biometrics of *Jazayeri* is contrary to the teachings of *Carlson*. Ex. 2006, ¶¶96-97. *Carlson* is solely concerned with the lack of security in any short-range wireless communication concerning sensitive financial information. *Carlson*, 2:10-18. *Carlson* proposes the use of a “pseudo primary account identifier” (PPAI) to overcome the deficiencies of all other security measures. *Carlson*, 2:63-66, 3:3-22, 4:26-38, 5:19-29. In *Carlson*’s view, biometrics would not improve the security of the account number once it is in transmission, which is the goal of *Carlson*. *Carlson*, 2:39-48. Thus, a POSITA would not have been motivated to combine the secure authentication process of *Jazayeri* with *Carlson* at the point of unlocking the device. Indeed, additional security would have undercut the usability of *Carlson*, further undercutting Petitioner’s identified motivation. Ex. 2006, ¶97.

B. Grounds 4-6 Would Not Have Rendered Obvious the Challenged Claims.

1. *Carlson* in View of *Murakami* Would Not Have Rendered Obvious “determining” “a value of the parameter that is sensed.”

With respect to Grounds 4-6, Petitioner states that “[i]n Grounds 4-6, in place of *Holloway-Jazayeri*, the proposed combination involves modifying *Carlson*

pursuant to *Murakami*'s biometric sensor and authentication process." Pet., 72. Petitioner goes on to incorporate by reference "[a]ll arguments and evidence from Grounds 1-3." Pet. 72. However, Grounds 4 and 5 do not rely on *Jazayeri* for the "determining" "a value of the parameter that is sensed" in limitations 1[b], 6[b], 11[b], and 14[b]. Pet., 18, 72.⁸ Petitioner's Grounds 4-6 fail. Ex. 2006, ¶¶98-102.

Petitioner states that "*Carlson* modified to unlock its device pursuant to the biometric authentication process described by *Murakami* teaches the claimed limitation of a parameter comprising a heart rate and/or a physiological state." Pet.,

⁸ The Petition states that "Jazayeri is maintained in Grounds [sic] 6 for the purpose of alternatively mapping an additional biometric authentication step prior to conducting the financial transaction or establishing a wireless link for Claims 4, 9, 11, 14, and 17-18." Pet., 72. Ground 6 is only directed to claim 18, and therefore the Petition is not clear how it is relying on *Jazayeri* in Ground 5 for claims 4, 9, 11, 14, or 17. Moreover, nowhere does the Petition describe "an additional biometric authentication step" or "establishing a wireless link" for any limitation of independent claims 11 or 14. Indeed, this is the only mention of "an additional biometric authentication step" in the Petition. *See generally* Pet. The Petition therefore does not rely on *Jazayeri* at all for at least claim limitations 1[b], 6[b], 11[b], and 14[b] in Grounds 4-6.

74 (citing Ex. 1003, ¶218). The Petition relies on *Murakami*'s sensor "used to measure a heartbeat waveform, a dynamic variable determined by measuring a user's heartbeat." Pet., 71 (citing *Murakami*, 32:30-33:6). Specifically, Petitioner relies on an embodiment wherein "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*, 23:20-22. *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, ¶99. A POSITA would not have been motivated to implement *Murakami*'s biometric sensor for functionalities, such as those disclosed in *Carlson*, which require little or no delay. *Id.*

Specifically, a POSITA would not have been motivated to implement *Murakami*'s biometric sensor for unlocking a consumer's wireless device because a

consumer would not use a lock that takes 30–100 heartbeats to use. Ex. 2006, ¶100. For example, such delay would be extremely disadvantageous in an emergency situation, where quick access to the device’s functions is preferred. *Id.* Indeed, *Murakami* expressly discloses that “[w]hen the signal is not valid, the biometrically activated switch will remain off or the device will remain disabled.” *Murakami*, 20:9-10.

Further, the Petition fails to identify any disclosure in *Murakami* that resolves the issues a POSITA would have had combining *Carlson* and *Jazayeri*. Ex. 2006, ¶101. Although *Carlson* discusses, in its Background section, the use of PIN authentication as an inadequate security measure which “still does not resolve the situation where the sensitive information is intercepted while the user is making a legitimate purchase and has thus already entered the PIN” (*Carlson*, 2:46-48), this does not establish that a POSITA would have been motivated to combine *Carlson*’s device with the authentication or authorization disclosures of *Jazayeri* or the exceedingly complicated, time consuming, and untemplated authentication procedures of *Murakami* such that *Carlson*’s device “determin[es]” “a value of the parameter that is sensed” and unlocks the device. Ex. 2006, ¶101.

For at least these reasons, a POSITA would not have been motivated to use *Murakami*’s biometric sensor to unlock *Carlson*’s device. Ex. 2006, ¶102. As such, Grounds 4-6 fail to disclose or render obvious “determining” “a value of the

parameter that is sensed” of independent claims 1[b] 6[b], 11[b], and 14[b], and thus all dependent claims as well. *Id.*

C. Grounds 1-6 Would Not Have Rendered Obvious Challenged Claims 3-5 and 8-18.

1. *Carlson’s* Request for PPAI Does Not Teach and Would Not Have Rendered Obvious “requesting . . . from a second device an authorization to enable a function for conducting a financial transaction by the device.”

Independent claim limitations 11[d] and 14[d] and dependent claim limitations 3[a] and 8[a] state “requesting by the device from a second device an authorization to enable a function for conducting a financial transaction by the device.” All claims that depend from independent claims 11 and 14 and dependent claims 3 and 8 also include this limitation.⁹ Petitioner’s Grounds 1-6 all fail with respect to claims 3-5 and 8-18. Ex. 2006, ¶¶103-117. Petitioner sets forth its position with respect to “requesting by the device from a second device an authorization to

⁹ The Petition’s analysis for this limitation is in dependent claim limitation 3[a]. Pet., 30-32. For independent claim limitations 11[d] and 14[d] and dependent claim limitation 8[a], the Petition merely incorporates the discussion of dependent claim limitation 3[a]. Pet., 37, 54, 55 (“*See supra* Claim 3(a).”). All citations herein are to the Petition’s analysis of dependent claim limitation 3[a].

enable a function for conducting a financial transaction by the device” in discussion of dependent claim limitation 3[a]. Pet., 30-32.

Petitioner’s only argument as to this limitation is that *Carlson*’s PPAI is “an authorization to conduct [a] particular transaction or particular limited set of transactions in *Carlson*’s system.” Pet., 30-32 (Grounds 1-3); *see also* Pet., 72 (incorporating analysis of *Carlson* into Grounds 4-6).¹⁰ That is, Petitioner equates a PPAI to an authorization to perform a particular transaction or particular limited set of transactions.¹¹ However, for at least two key reasons, a POSITA would not have understood *Carlson*’s PPAI to be the claimed “authorization to enable a function for conducting a financial transaction by the device.”

First, the PPAI in *Carlson* is not “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, ¶105.

¹⁰ The Petition solely relies on *Carlson* and, thus, does not rely on *Holloway* or *Jazayeri* in Grounds 1-3 nor *Murakami* in Grounds 4-6 for this part of the limitation.

¹¹ For the purposes of this IPR, Petitioner interprets the “authorization” of claims 3[a], 8[a], 11[d], and 14[d] to be an authorization for a transaction or a set of transactions. *See* Pet., 30-32 (Grounds 1-3); *see also* Pet., 72 (incorporating analysis of *Carlson* into Grounds 4-6).

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, ¶105.

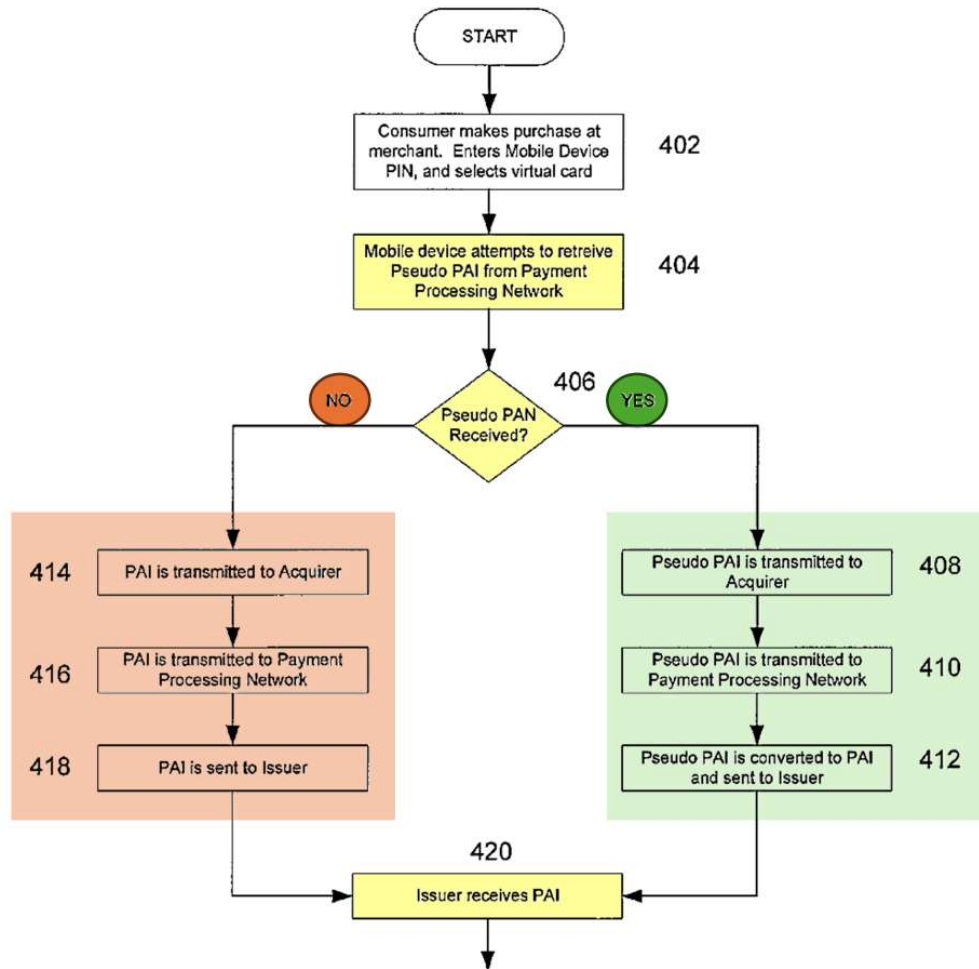
Instead, *Carlson* explains that a PPAI is used during a financial transaction, instead of the user's real account identifier, to protect the user from “[t]heft of sensitive information . . . using wireless interrogation or interception of communications from portable wireless device.” *Carlson*, 2:7-10. 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, ¶106.

Petitioner is relying on an embodiment of *Carlson* wherein the wireless device requests PPAI from the payment processing network. Pet. 30-32. According to the Petition, because *Carlson*'s financial transaction “**requires** requesting and receiving the PPAI before the process may proceed” (Pet., 32 (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, ¶107.

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, ¶108. 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, ¶108.



Carlson, Fig. 4 (cropped and annotated); Ex. 2006, ¶108.

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

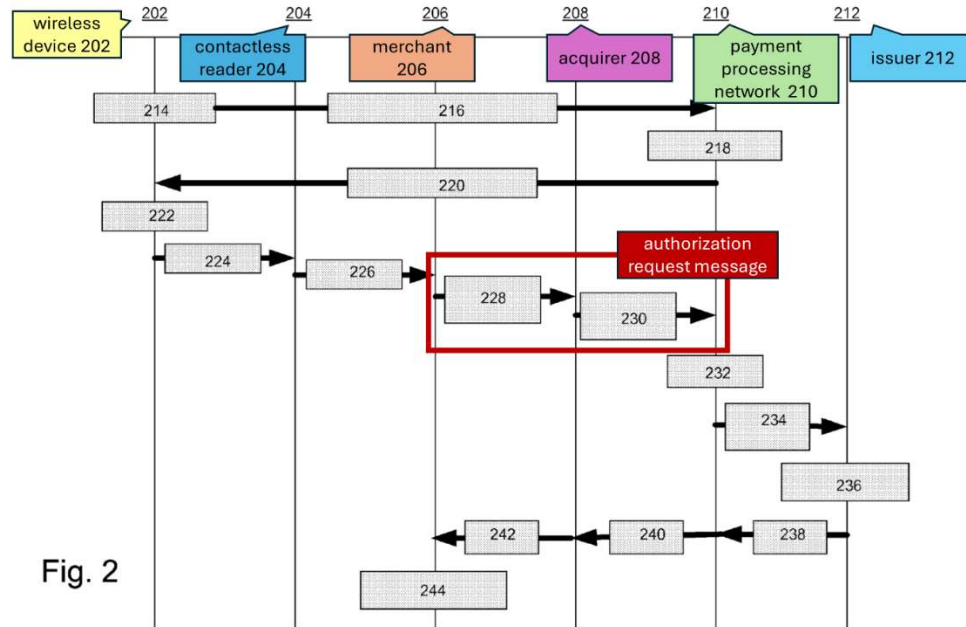
transaction. Ex. 2006, ¶109. For example, the PPAI may be “pushed to the portable wireless device at any time, such as when the device is turned on, when the device is idle, periodically, or through any other such criteria.” *Carlson*, 7:4-7, 12:67-13:3. As another example, *Carlson* discloses that “[t]he 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, ¶109.

Second, *Carlson* itself undercuts Petitioner’s theory that *Carlson*’s PPAI is “an authorization” received by *Carlson*’s device. *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, ¶110. *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*, 8:10-13. “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, ¶110.

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, ¶111. The claims require “requesting *by the device*” or “requesting *by the wireless device*.” Ex. 1001, cls. 3, 8, 11 (emphasis added); *see also id.* cl. 14 (claiming “[a] wireless device that is configured to perform operations comprising” the request for authorization). Because *Carlson*’s “authorization request message” is sent *by the merchant*, the “authorization request message” cannot be the claimed “request[]” for “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.



Carlson, Fig. 2 (annotated); Ex. 2006, ¶111.

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).¹²

¹² Notably, the Petition excerpts *Carlson*’s Figure 4 in a way that excludes the authorization step in purple below. *See* Pet., 33 (discussing claim limitation 3[c]); *but see* Ex. 1003, ¶149 (annotating Figure 4 and highlighting the authorization step).

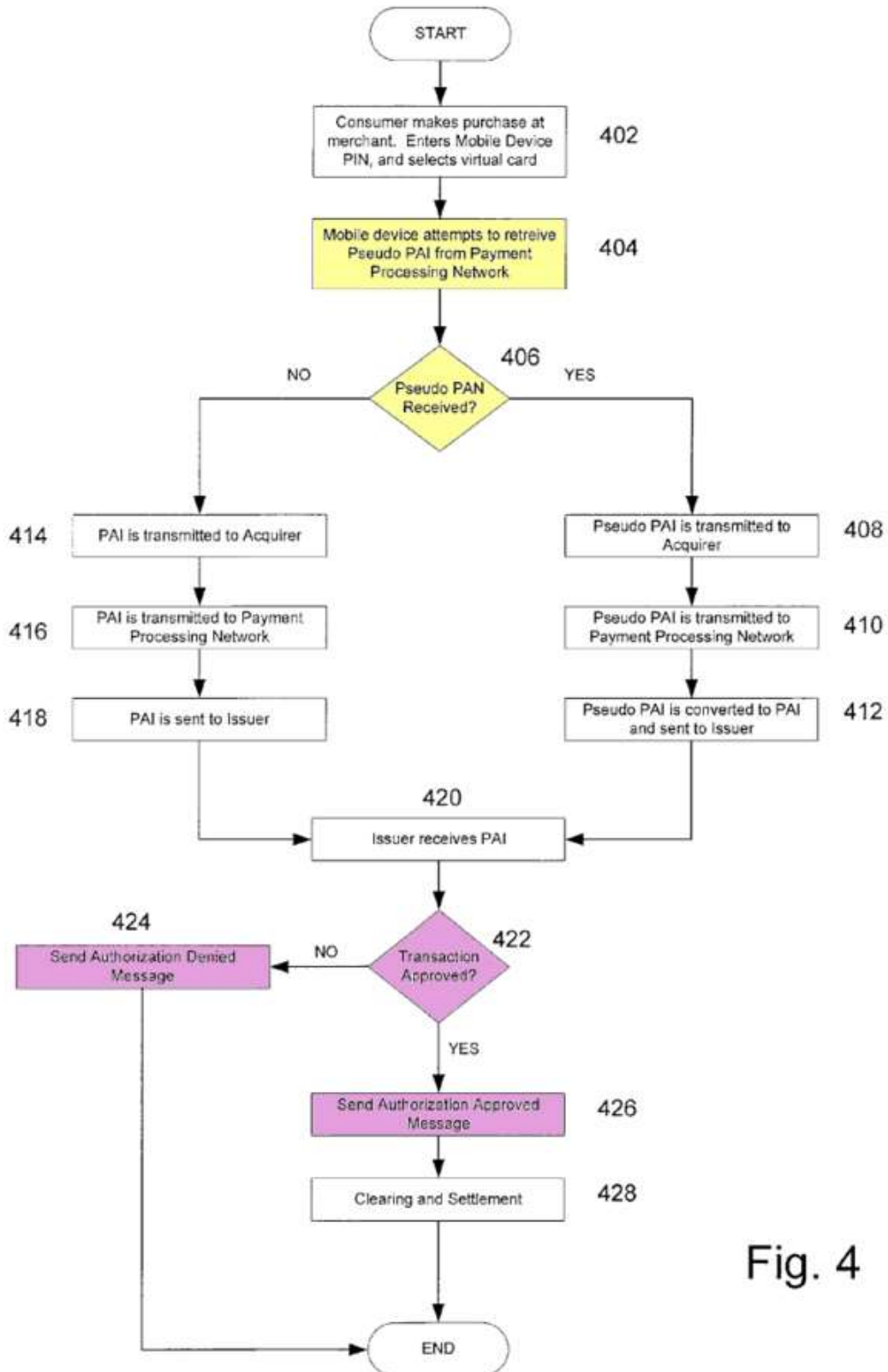


Fig. 4

Carlson, Fig. 4 (annotated); Ex. 2006, ¶112. *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 acknowledges that *Carlson* does not actually require receiving a PPAI to conduct a financial transaction but then only addresses this major flaw in its argument 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., 34 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 or not, 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, ¶113. 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.¹³ Ex. 2006, ¶113. Because a PPAI-based financial transaction is still possible in *Carlson*, a PPAI is not 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, ¶114. 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

¹³ 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, ¶114.

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 PPAI to be “an authorization.” Ex. 2006, ¶115.

For at least these reasons, both *Carlson* in view of *Holloway* and/or *Jazayeri* and *Carlson* in view of *Murakami* fail to disclose or render obvious “requesting by the device from a second device an authorization to enable a function for conducting a financial transaction by the device” of independent claims 11 and 14 and dependent claims 3 and 8, and thus all claims that depend therefrom as well. Ex. 2006, ¶¶116-117.

VII. CONCLUSION

For the foregoing reasons, institution should be denied.

Dated: November 7, 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 7,900 which is less than the 14,000 allowed under 37 CFR § 42.24(b)(1).

Dated: November 7, 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 7, 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 7, 2025

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