

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

TELCOM VENTURES LLC,
Patent Owner

Case No. IPR2025-01234
U.S. Patent No. 10,219,199

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	LEGAL STANDARD.....	4
III.	BACKGROUND.....	5
	A. THE '199 PATENT	5
	B. <i>CARLSON</i> (EX. 1005).....	7
	C. <i>HOLLOWAY</i> (EX. 1032).....	9
	D. <i>JAZAYERI</i> (EX. 1007).....	10
	E. <i>ISO-14443</i> (EX. 1016).....	12
	F. <i>MATSUSHITA</i> (EX. 1013).....	13
	G. <i>SHERMAN</i> (EX. 1014)	13
	H. <i>MURAKAMI</i> (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. GROUNDS 1-4 WOULD NOT HAVE RENDERED OBVIOUS THE CHALLENGED CLAIMS.	16
	1. Ground 1 Would Not Have Rendered Obvious “in response to a physiological parameter, wirelessly providing by the smartphone, using the first air interface, information to the entity and wirelessly receiving by the smartphone, using the first air interface, information from the entity.”	16
	2. Ground 1 Would Not Have Rendered Obvious “wirelessly receiving by the smartphone, using the first air interface, information from the entity.”	27
	B. GROUNDS 5-7 WOULD NOT HAVE RENDERED OBVIOUS THE CHALLENGED CLAIMS.	29
	1. Ground 5 Would Not Have Rendered Obvious “in response to a physiological parameter, wirelessly providing by the smartphone, using the first air interface,	

information to the entity and wirelessly receiving by the smartphone, using the first air interface, information from the entity.”	29
2. Ground 5 Would Not Have Rendered Obvious “wirelessly receiving by the smartphone, using the first air interface, information from the entity.”	31
VII. CONCLUSION	33

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)	5
<i>Microsoft Corp. v. Secure Web Conf. Corp.</i> , IPR2014-00745, Paper 12 (P.T.A.B. Sept. 29, 2014).....	5
<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).....	5
<i>Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.</i> , 200 F.3d 795 (Fed. Cir. 1999)	15
<i>Zhuhai Cosmx Battery Co., Ltd., v. Ningde Ampere Tech. Ltd.</i> , IPR2025-00405, Paper 24 (P.T.A.B. Oct. 15, 2025).....	32
STATUTES	
35 U.S.C. § 103	1, 2
35 U.S.C. § 312(a)(3).....	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	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

Reference	Claim Limitation
Claim 1	
1[pre]	A method of operating a smartphone to wirelessly provide information to an entity using a first air interface, to wirelessly receive information from the entity using the first air interface; and to wirelessly receive a communications service from a wireless network using a second air interface that differs from the first air interface, wherein the communications service is received by the smartphone from the wireless network absent involving the entity and wherein the entity functions independently of the communications service, the method comprising:
1[a]	detecting by the smartphone that a proximity condition is satisfied between the smartphone and the entity;
1[b]	in response to at least the proximity condition having been satisfied between the smartphone and the entity, establishing a wireless short-range communications link between the smartphone and the entity to provide by the smartphone, using the first air interface, information to the entity and to receive by the smartphone information from the entity;
1[c]	in response to at least the proximity condition having been satisfied between the smartphone and the entity and in response to a physiological parameter, wirelessly providing by the smartphone, using the first air interface, information to the entity and wirelessly receiving by the smartphone, using the first air interface, information from the entity independently of, and absent involving the entity in, receiving by the smartphone the communications service from the wireless network using the second air interface; and
1[d]	wirelessly receiving by the smartphone, using the second air interface, the communications service from the wireless network absent involving the entity, absent providing by the smartphone information to the entity, and absent receiving by the smartphone information from the entity,
1[e]	wherein the wireless short-range communications link used by the first air interface is based upon unlicensed frequencies,
1[f]	wherein the second air interface uses a wireless communications link that is based upon licensed frequencies, and

Reference	Claim Limitation
1[g]	wherein the first air interface is not involved in providing the communications service to the smartphone.
Claim 2	
2[pre]	The method of claim 1,
2[a]	wherein said wirelessly providing by the smartphone, using the first air interface, information to the entity and wirelessly receiving by the smartphone, using the first air interface, information from the entity independently of, and absent involving the entity in, receiving by the smartphone the communications service from the wireless network using the second air interface is performed over a first time interval;
2[b]	wherein said wirelessly receiving by the smartphone, using the second air interface, the communications service from the wireless network absent involving the entity, absent providing by the smartphone information to the entity, and absent receiving by the smartphone information from the entity is performed over a second time interval; and
2[c]	wherein the first and second time intervals are non-overlapping with one another.
Claim 3	
3[pre]	The method of claim 1,
3[a]	wherein the wireless short-range communications link that is based upon unlicensed frequencies is further based upon a Time Division Duplex (TDD) protocol, and
3[b]	wherein the second air interface that uses a wireless communications link that is based upon licensed frequencies is further based upon an Orthogonal Frequency Division Multiplexed (OFDM) and/or Orthogonal Frequency Division Multiple Access (OFDMA) protocol.
Claim 4	
4[pre]	The method of claim 1,
4[a]	wherein said detecting by the smartphone that a proximity condition is satisfied between the smartphone and the entity is based, at least in part, on receiving a short-range signal from the entity over the first air interface.
Claim 5	
5[pre]	The method of claim 4,
5[a]	wherein said detecting by the smartphone that a proximity condition is satisfied between the smartphone and the entity is based, at least in part, on a measurement of signal strength of the short-range signal.

Reference	Claim Limitation
Claim 6	
6[pre]	The method of claim 1,
6[a]	wherein a value of the physiological parameter is provided by using a sensor of the smartphone.
Claim 7	
7[pre]	The method of claim 1, wherein said wirelessly providing by the smartphone, using the first air interface, information to the entity comprises:
7[a]	being proximate to a specific location within a store, then detecting a short-range signal being transmitted from said specific location within the store, and then performing a transaction to pay for one or more items
Claim 8	
8[pre]	The method of claim 1,
8[a]	wherein the entity comprises a check-out counter in a store, and
8[b]	wherein said wirelessly providing by the smartphone, using the first air interface, information to the entity comprises:
8[c]	performing a financial transaction to pay for one or more items.
Claim 9	
9[pre]	The method of claim 1,
9[a]	wherein establishing the wireless short-range communications link between the smartphone and the entity is performed in response to the physiological parameter.
Claim 10	
10[pre]	A system comprising:
10[a]	a smartphone that is configured to perform operations comprising:
10[b]	detecting by the smartphone that a proximity condition is satisfied between the smartphone and an entity;
10[c]	in response to at least the proximity condition having been satisfied between the smartphone and the entity, establishing a wireless short-range communications link between the smartphone and the entity to provide by the smartphone, using a first air interface, information to the entity and to receive by the smartphone information from the entity;

Reference	Claim Limitation
10[d]	in response to at least the proximity condition having been satisfied between the smartphone and the entity and in response to a physiological parameter, wirelessly providing, using the first air interface, information to the entity and wirelessly receiving, using the first air interface, information from the entity independently of, and absent involving the entity in, receiving a communications service from a wireless network using a second air interface that differs from the first air interface; and
10[e]	wirelessly receiving, using the second air interface, the communications service from the wireless network absent involving the entity, absent providing information to the entity, and absent receiving information from the entity,
10[f]	wherein the wireless short-range communications link used by the first air interface is based upon unlicensed frequencies,
10[g]	wherein the second air interface uses a wireless communications link that is based upon licensed frequencies, and
10[h]	wherein the first air interface is not involved in providing the communications service to the smartphone.
Claim 11	
11[pre]	The system according to claim 10
11[a]	further comprising the entity.
Claim 12	
12[pre]	The system of claim 10,
12[a]	wherein said wirelessly providing, using a first air interface, information to an entity and wirelessly receiving, using the first air interface, information from the entity independently of, and absent involving the entity in, receiving a communications service from a wireless network using a second air interface that differs from the first air interface is performed over a first time interval;
12[b]	wherein said wirelessly receiving, using the second air interface, the communications service from the wireless network absent involving the entity, absent providing information to the entity, and absent receiving information from the entity is performed over a second time interval; and
12[c]	wherein the first and second time intervals are non-overlapping with one another.
Claim 13	
13[pre]	The system of claim 10,

Reference	Claim Limitation
13[a]	wherein the second air interface is based upon an Orthogonal Frequency Division Multiplexed (OFDM) and/or Orthogonal Frequency Division Multiple Access (OFDMA) protocol.
Claim 14	
14[pre]	The system of claim 10,
14[a]	wherein said detecting by the smartphone that a proximity condition is satisfied between the smartphone and an entity is based, at least in part, on receiving a short-range signal from the entity over the first air interface.
Claim 15	
15[pre]	The system of claim 14,
15[a]	wherein said detecting by the smartphone that a proximity condition is satisfied between the smartphone and an entity is based, at least in part, on a measurement of signal strength of the short-range signal.
Claim 16	
16[pre]	The system of claim 10,
16[a]	wherein a value of the physiological parameter is provided by using a sensor of the smartphone.
Claim 17	
17[pre]	The system of claim 10,
17[a]	wherein said wirelessly providing, using the first air interface, information to the entity comprises:
17[b]	being proximate to a specific location within a store, then detecting a short-range signal being transmitted from said specific location within the store, and then performing a transaction to pay for one or more items.
Claim 18	
18[pre]	The system of claim 10,
18[a]	wherein the entity comprises a check-out counter in a store, and
18[b]	wherein said wirelessly providing, using the first air interface, information to the entity comprises:
18[c]	performing a financial transaction to pay for one or more items.
Claim 19	
19[pre]	The system of claim 10,
19[a]	wherein establishing the wireless short-range communications link between the smartphone and the entity is performed in response to the physiological parameter.

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 1-19 (the “Challenged Claims”) of U.S. Patent No. 10,219,199 (the “’199 Patent,” Ex. 1001). The Petition sets forth seven Grounds. Pet. at 19. In all, Petitioner relies on U.S. Patent No. 8,229,852 to Carlson (“*Carlson*,” Ex. 1005) in combination with up to four 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 ’199 Patent. The seven separate Grounds are summarized in the below chart.

Ground	Claims	Proposed Ground of Unpatentability
1	Claims 1, 4-5, 7-11, and 14-19	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> ¹ in view of <i>Jazayeri</i> ² and <i>ISO-14443</i> . ³

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

² U.S. Patent Application Publication No. 2008/0155268 (“*Jazayeri*,” Ex. 1007).

³ ISO/IEC 14443 (“*ISO-14443*,” Ex. 1016).

Ground	Claims	Proposed Ground of Unpatentability
2	Claims 2 and 12	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>Matsushita</i> . ⁴
3	Claims 3 and 13	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>Sherman</i> . ⁵
4	Claim 6	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> in view of <i>Holloway</i> , ⁶ <i>Jazayeri</i> , and <i>ISO-14443</i> .
5	Claims 1, 4-11, and 14-19	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> . ⁷
6	Claims 2 and 12	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> in view of <i>Jazayeri</i> , <i>ISO-14443</i> , <i>Matsushita</i> , and <i>Murakami</i> .
7	Claims 3 and 13	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> in view of <i>ISO-14443</i> , <i>Sherman</i> , and <i>Murakami</i> .

⁴ U.S. Patent Application Publication No. 2006/0234778 (“*Matsushita*” Ex. 1013).

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

⁶ WIPO International Patent Application Publication No. WO 02/49322 (“*Holloway*” Ex. 1032).

⁷ WIPO International Application Publication No. WO 01/95246 (“*Murakami*,” Ex. 1009).

Petitioner divides the Grounds into two groups. Grounds 1-4 combine *Carlson*, *Jazayeri*, and other references. Pet., 19. Grounds 5-7 combine *Carlson*, *Jazayeri*, *Murakami*, and other references. Pet., 70. Petitioner states that “Grounds 5-7 differ from Grounds 1-4 only in the proposed modifications to *Carlson* pertaining to the biometric sensor and authentication process.” Pet., 71.

Petitioner’s Grounds 1-4 would not have rendered obvious the Challenged Claims. *First*, Ground 1 would not have rendered obvious “in response to a physiological parameter, wirelessly providing by the smartphone, using the first air interface, information to the entity and wirelessly receiving by the smartphone, using the first air interface, information from the entity” of claim limitation 1[c] nor the similar language of claim limitation 10[d]. Petitioner alleges that a POSITA would modify *Carlson* “to unlock its device pursuant to the biometric authentication process described by *Jazayeri*.” Pet., 33. 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 that if combined, the proposed combination device would have rendered obvious providing *Carlson*’s “bogus, fake, decoy, substitute” (*Carlson*, 5:42-43) pseudo primary account identifier (“PPAI”) to the near field communication (“NFC”) access device “in response to a physiological parameter.”

Second, Ground 1 would also not have rendered obvious “wirelessly receiving

[by the smartphone], using the first air interface, information from the entity” of claim limitation 1[c] and 10[d]. Petitioner alleges that a POSITA would “modify *Carlson*’s device to receive a digital receipt via NFC” to meet this limitation. Pet., 41. But *Carlson* teaches away from systems that do not integrate “easily with existing payment processing networks.” *Carlson*, 2:49-51. A stated benefit of *Carlson* is the use of “currently installed equipment” such that “no change is required at the merchant in order to process transactions. . . .” *Carlson*, 5:44-46. Thus, a POSITA would not have been motivated to modify *Carlson* such that it received a digital receipt.

Petitioner’s Grounds 5-7 similarly fail. Petitioner again fails to establish that a POSITA would have been motivated to combine *Carlson* with other references to render obvious claim limitations 1[c] and 10[d], even including the disclosures from *Murakami*. With respect to the claim limitation “wirelessly receiving [by the smartphone], using the first air interface, information from the entity” the introduction of *Murakami* fails to alter the fact that a POSITA would not have been motivated to modify the system of *Carlson* to include receiving a digital receipt.

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 patented 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 AG*, 892 F.3d 1349, 1356 (Fed. Cir. 2018).

III. BACKGROUND

A. The ’199 Patent

Applicants filed U.S. Patent Application No. 15/800,885, on November 1, 2017, which issued as U.S. Patent No. 10,219,199 on February 26, 2019. Ex. 1001, 1.

The ’199 Patent describes mobile wireless devices and methods of using a mobile wireless device to engage in one or more communications modes, but only

when certain conditions or criteria are met, such as the satisfaction of a proximity condition and a value of a parameter, e.g., a physiological parameter, satisfying a criterion. Ex.1001, 1:18-22; 6:10-27. The specification recognizes that the devices in the art were rigidly configured to perform a predetermined number of functions. *Id.*, 1:32-37. The '199 Patent addresses this rigidity problem by providing devices and methods that “may be used to enable adaptively one or more modes/functions of a device” based upon the satisfaction of certain criteria. *Id.*, 1:44-46. The specification 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.” *Id.*, 1:37-40.

The '199 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.” *Id.*, 6:12-17. 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.” *Id.*, 6:16-21. 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.” *Id.*, 6:22-27. The disclosed wireless communications devices may be “configured to selectively enable

a first communications mode/function” responsive to a value of such a parameter.
Id., 6:37-46.

The ’199 Patent issued after a single rejection during prosecution. Ex. 1002 at 102. The Examiner issued a non-final rejection of initial proposed claims 1-8 and 24 for double patenting in light of claims 1, 11, 16, and 18 of U.S. Patent No. 9,832,708 and as obvious in light of U.S. Patent Application 2007/0260710 to Dowling, and U.S. Patent Application 2007/0129077 to Iguchi et al. Ex. 1002 at 108, 110. Applicant filed a terminal disclaimer over the ’708 Patent. Ex. 1002 at 157, 161.

Applicant filed amended claims in response to the rejection. Ex. 1002 at 174-182. Applicant argued that the identified prior art did not “disclose or suggest detecting by a smartphone that a proximity condition is satisfied between the smartphone and an entity.” Ex. 1002 at 185. Applicant also argued that the identified prior art did not disclose “wirelessly providing by the smartphone information to the entity in response to . . . a physiological parameter.” Ex. 1002 at 185.

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* 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, ¶76. *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.

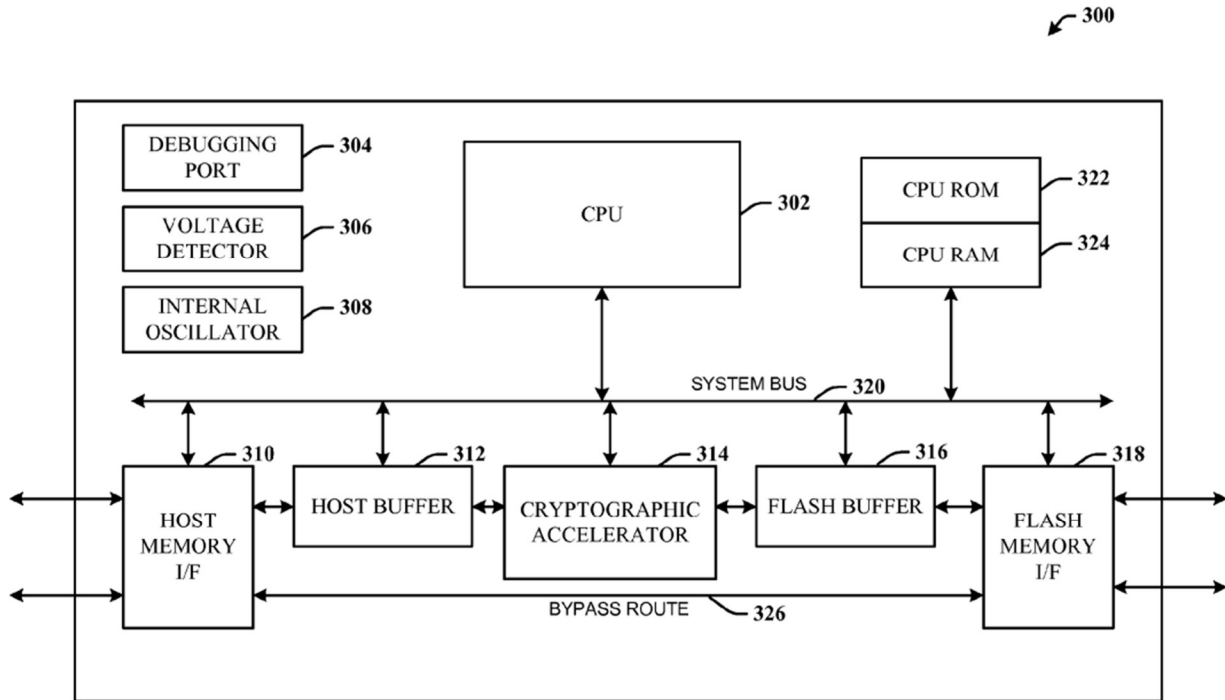


FIG. 3

Jazayeri, Fig. 3

Jazayeri's security processor comprises sophisticated hardware. Ex. 2006 ¶78. *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., 12 (citing Ex. 1033, Munford Declaration). The *ISO/IEC 14443* standard has four parts. Ex. 2006 ¶79. *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 ¶80.

F. *Matsushita* (Ex. 1013)

U.S. Patent Application Publication No. 2006/0234778 to *Matsushita* is directed to “a wireless communications terminal capable of preventing radio interferences from being caused by other wireless communications concurrent with a contactless communications.” *Matsushita*, Abstract. *Matsushita* discloses a “wireless communications control section” capable of “restricting a wireless communications performed by the first wireless communications section in response to an initiation of a contactless communications.” *Matsushita*, ¶[0008].

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 5-7. Pet.,

6, 71. 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 ’199 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., 6-7. 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 1-4 Would Not Have Rendered Obvious the Challenged Claims.

In Ground 1, Petitioner asserts that both independent Challenged Claims 1 and 10 and certain dependent Challenged Claims would have been obvious over *Carlson* in view of *Jazayeri* and *ISO-14443*. Pet., 19. In Grounds 2-4 Petitioner asserts that additional dependent Challenged Claims, which depend from claims 1 or 10, would have been obvious over *Carlson* in view of *Jazayeri*, *ISO-14443*, and additional references. Pet., 19. For the reasons set forth below, Ground 1, and thus, Grounds 2-4, fail.

1. Ground 1 Would Not Have Rendered Obvious “in response to a physiological parameter, wirelessly providing by the smartphone, using the first air interface, information to the entity and wirelessly receiving by the smartphone, using the first air interface, information from the entity.”

Claim limitation 1[c] states “in response to at least the proximity condition having been satisfied between the smartphone and the entity and *in response to a physiological parameter*, wirelessly providing by the smartphone, using the first air interface, information to the entity and wirelessly receiving by the smartphone, using

the first air interface, information from the entity.” (emphasis added). Limitation 10[d] similarly states “in response to at least the proximity condition having been satisfied between the smartphone and the entity and *in response to a physiological parameter*, wirelessly providing, using the first air interface, information to the entity and wirelessly receiving, using the first air interface, information from the entity.” (emphasis added). Petitioner alleges that “*Carlson-ISO-14443-Jazayeri* teaches Claim 1(c).” Pet., 32, *see also* Pet., 53 (addressing limitation 10[d] with “[s]ee *supra* Claims 1(Pre) and 1(c)”). Petitioner’s Grounds all fail.

With respect to the “in response to a physiological parameter” portion of this limitation, Petitioner states that “*Carlson* modified to unlock its device pursuant to the biometric authentication process described by *Jazayeri* teaches sensing a physiological parameter.” Pet., 33 (citing Ex. 1003 ¶125). Petitioner states that a POSITA would have been motivated to modify *Carlson* to implement *Jazayeri*’s process because “*Carlson* explicitly contemplates unlocking the device with a fingerprint.” Pet., 34. However, *Carlson* mentions biometrics or fingerprints only once and does so only with respect to unlocking the device the device. *Carlson*, 12:18-24; Ex. 2006 ¶85. Because *Carlson* alone fails to teach the limitation, Petitioner alleges that “a POSITA would have been motivated to look to *Jazayeri* as a guide for implementing biometric authentication in *Carlson*’s device.” Pet., 34. Petitioner is incorrect. Ex. 2006 ¶85.

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 ¶86. 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 ¶86.

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 ¶87.

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., 35. 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., 35 (citing *Carlson*, 14:47-49); *see also* Ex. 2006 ¶88. 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 ¶¶ 88-89. 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 ¶¶ 88-89. But Petitioner ignores the necessity of the security processor, failing to mention it at all in the Petition. Without this processor, *Jazayeri* has no process for performing the disclosed verification process. Ex. 2006 ¶88.

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 ¶90.

Jazayeri did not intend its security processor to be “common hardware elements,” as alleged by Petitioner. Instead, as shown by the detailed description and 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 ¶91. 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 ¶91.

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

Furthermore, even if possible by a POSITA, there is no motivation to modify *Carlson*’s system with the biometric authentication process of *Jazayeri*. Petitioner proposes two mappings for this limitation. First, Petitioner combines *Carlson* with *Jazayeri* to “unlock its device pursuant to the biometric authentication process described by *Jazayeri*.” Pet., 33. Second, Petitioner states that “*Jazayeri* discloses authenticating a user via biometric data immediately prior to exchanging account information to make a purchase.” Pet., 35. A POSITA would not have been

motivated to combine *Carlson*'s device with *Jazayeri*'s authentication in either scenario.

With respect to both scenarios, a POSITA would readily understand that using biometrics of *Jazayeri* such that “in response to a physiological parameter” the smartphone “wirelessly provid[es] . . . using the first air interface, information to the entity” and receives “using the first air interface, information from the entity” is contrary to the teachings of *Carlson*. Ex. 2006 ¶¶92-93. *Carlson* is solely concerned with the lack of security in 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*, either at the point of unlocking the device or at the point of transferring the PPAI. Indeed, additional security would have undercut the usability of *Carlson*, further undercutting Petitioner's identified motivation. Ex. 2006 ¶93.

Further confirming the lack of motivation to combine, and with respect to the “second biometric authentication step,” Petitioner admits that “*Carlson*'s native process allows access to the financial transaction function regardless of the amount

of time passed between unlocking the wireless device and selecting a virtual card.” Pet., 37. But *Carlson* not only does not disclose the use of a second biometric authentication, it disparages the use of authentication in connection with transactions as a whole, stating in the Background section of the specification that the use of authentication like a PIN is inadequate because it “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*, 2:46-49; *see also* Ex. 2006 ¶94. A POSITA would not have been motivated to combine *Carlson*’s device with *Jazayeri*’s authentication processes to unlock the device, or prior to exchanging account information.

c. A POSITA Would Not Have Been Motivated to Store Carlson’s PPAI in Jazayeri’s Secure Non-Volatile Memory

With respect to the second proposal, modifying *Carlson*’s device with *Jazayeri* to authenticate “a user via biometric data immediately prior to exchanging account information to make a purchase” (Pet., 35), Petitioner also fails to establish that a POSITA would have been motivated to make the proposed modification to *Carlson*. In discussing the “wirelessly providing information” portion of this claim limitation, Petitioner states that “the wireless device provides the PPAI (information) to the access device via NFC (first air interface).” Pet., 38 (emphasis in original). But Petitioner fails to establish that there was any reason that the PPAI, the

“information” provided by *Carlson*’s device to the NFC access device, would have been protected by *Jazayeri*’s biometric authentication process. Ex. 2006 ¶95.

When discussing the “second biometric authentication step,” Petitioner points to *Jazayeri* ¶¶[0049]-[0052] and Figure 7. Pet., 35-36. *Jazayeri* ¶[0049] states that “[r]eferring to FIG. 7, a method of controlling access to use account information via biometric data is illustrated. At 700, a user selects a payment application on a mobile device to make a purchase. The menu prompts the user to specify the account, amounts, etc. for the purchase. At 702, the user selects an account to use, wherein the account details are stored in non-volatile memory.” *Jazayeri*, ¶[0049]. It is thus the “account details” that are stored in non-volatile memory. Ex. 2006 ¶96. But Petitioner does not point to the transmission of “account details” in *Carlson* as the claimed “information” transferred to the access device via the first air interface. Instead, Petitioner states that “the wireless device provides the PPAI (*information*) to the access device via NFC (*first air interface*).” Pet., 38. (emphasis in original). But Petitioner fails to establish that a POSITA would have been motivated to combine *Carlson* such that its PPAI was stored in *Jazayeri*’s secure non-volatile memory, and thus protected by *Jazayeri*’s biometric authentication and process.

In *Carlson*, the PPAI is not account information at all. Ex. 2006 ¶97. In fact, the PPAI is specifically designed because it does not require security because, if accessed or intercepted, *Carlson* states that it cannot be used. *Carlson*, 8:23-31.

Carlson also does not treat the PPAI with particular emphasis on security. *Carlson* is explicit that the PPAI “may also be described using terms such as bogus, fake, decoy, substitute, or the like.” *Carlson*, 5:42-43. *Carlson* further discloses obtaining the PPAI immediately prior to a transaction, stating that “[u]pon gaining access to the communications network, in this exemplary embodiment, the portable wireless device may send a request through the communications network to a payment processing network in order to retrieve a pseudo primary account identifier that corresponds to the primary account identifier that was previously selected.” *Carlson*, 6:32-37. *Carlson* further states that “[t]he payment processing network can respond to the request from the portable wireless device with a response message that contains a pseudo primary account identifier. The response can be sent over the communications network back to the portable wireless device.” *Carlson*, 6:50-55. The PPAI is thus transmitted to *Carlson* over potentially unsecure networks, often immediately prior to a transaction and thus is specifically designed to not require a secure location. Ex. 2006 ¶98.

Further, *Carlson* discloses that the PPAI “may be set to expire after a certain number of transactions or after a certain time period.” *Carlson*, 6:60-61. *Carlson* also contemplates the wireless device itself generating the PPAI and “[t]he generated pseudo primary account identifier may then be sent to the payment processing network over the communications network.” *Carlson*, 7:19-21. And, as discussed

above, the entire point of *Carlson* is to provide “transmission of a pseudo primary account identifier, *in lieu of a user’s real account identifier such as a primary account identifier (PAI) or a user’s real primary account number (PAN).*” *Carlson*, 5:24-27 (emphasis added); *see also* Ex. 2006 ¶99.

A POSITA would not have understood the PPAI—which is (1) generated immediately prior to a transaction; (2) transmitted over unsecure networks; (3) set to expire and, thus, useless if intercepted; and (4) used “in lieu” of the user’s actual account information—to be equivalent to the account details stored in non-volatile memory in *Jazayeri*. Ex. 2006 ¶100. Thus, even if a POSITA were able to utilize *Jazayeri*’s complicated security protocols and components, they would not have been motivated to place *Carlson*’s temporary, “bogus, fake, decoy, substitute” PPAI in *Jazayeri*’s non-volatile memory during the window between receipt or generation of that PPAI, and the use of the PPAI during a transaction. Ex. 2006 ¶100. Given the PPAI s short term and will be transmitted over an insecure network, no benefit is gained by storing it in *Jazayeri*’s secure non-volatile memory. Ex. 2006 ¶99.

For at least these reasons, a POSITA would not have been motivated to combine *Carlson* with *Jazayeri*. *Carlson-ISO-1443-Jazayeri* of Petitioner’s Ground 1 would therefore not have rendered obvious “in response to at least the proximity condition having been satisfied between the smartphone and the entity and *in response to a physiological parameter*, wirelessly providing by the smartphone,

using the first air interface, information to the entity and wirelessly receiving by the smartphone, using the first air interface, information from the entity” of claim limitation 1[c] nor “in response to at least the proximity condition having been satisfied between the smartphone and the entity and *in response to a physiological parameter*, wirelessly providing, using the first air interface, information to the entity and wirelessly receiving, using the first air interface, information from the entity” of claim limitation 10[d]. Ground 1 thus fails for both independent claims, and all dependent claims. Ground 1, and as a result, Grounds 2-4, fail. Ex. 2006 ¶101.

2. Ground 1 Would Not Have Rendered Obvious “wirelessly receiving by the smartphone, using the first air interface, information from the entity.”

Claim limitation 1[c] states, in part, “wirelessly receiving by the smartphone, using the first air interface, information from the entity.” Claim limitation 10[d] similarly states, in part, “wirelessly receiving, using the first air interface, information from the entity.” Petitioner states that “*Carlson-ISO-14443-Jazayeri* further teaches the wireless device receiving information in the form of a digital receipt from the contactless reader using NFC.” Pet., 38; *see also id.*, 53 (addressing limitation 10[d] with “[s]ee *supra* Claims 1(Pre) and 1(c)”). That is, Petitioner alleges that a digital receipt is “information from the entity.” Petitioner’s argument fails. Ex. 2006 ¶102.

Carlson does not provide a digital receipt and cannot do so because it only discloses providing the user with a receipt displayed by the merchant or printed. *Carlson*, 9:26-30; *see also* Ex. 2006 ¶¶103-104. Petitioner alleges that a POSITA would have been motivated to combine *Carlson*'s system with *Jazayeri* and would have had a reasonable expectation of success in doing so, to incorporate the transmission of a receipt to the mobile device. Pet., 41. This misstates *Carlson*.

Carlson teaches away from receiving data on the mobile device, because sending such data to the mobile device would require modification not just of *Carlson*'s device, but of the equipment at the merchant such that the equipment can send such a receipt. Ex. 2006 ¶105. *Carlson* is clear that its system is meant to be a “cost effective device and method that integrates easily with **existing payment processing** networks” (2:49-50 (emphasis added)) because “many merchants, for example, resist making necessary upgrades to their procedures and systems.” *Id.* at. 2:32-35. *Carlson* emphasizes that “[f]rom a merchant’s perspective, transaction processing using a pseudo primary account identifier is completely transparent. That is to say that a merchant processing a transaction using a pseudo primary account identifier can process the transaction in exactly the same manner as if the transaction was occurring with a real primary account identifier. . . . As such, a merchant can continue to process transactions **with currently installed equipment** and no change is required at the merchant in order to process transactions using pseudo primary

account identifiers.” *Carlson*, 5:44-56 (emphasis added). The disclosure of *Carlson* is meant to work with existing payment processing networks and merchant equipment, and a POSITA would not have been motivated to combine or have had a reasonable expectation of success in combining *Carlson* with *Jazayeri* such that a receipt was received via NFC by the device in *Carlson*. Ex. 2006 ¶105.

For at least these reasons, a POSITA would not have been motivated to combine *Carlson* with *Jazayeri* to disclose this limitation. *Carlson-ISO-14443-Jazayeri* of Petitioner’s Ground 1 would not have rendered obvious “wirelessly receiving [by the smartphone], using the first air interface, information from the entity” of claim limitations 1[c] and 10[d]. Ground 1 thus fails for both independent claims, and all dependent claims. Ground 1, and as a result, Grounds 2-4, fail. Ex. 2006 ¶106.

B. Grounds 5-7 Would Not Have Rendered Obvious the Challenged Claims.

1. Ground 5 Would Not Have Rendered Obvious “in response to a physiological parameter, wirelessly providing by the smartphone, using the first air interface, information to the entity and wirelessly receiving by the smartphone, using the first air interface, information from the entity.”

With respect to Grounds 5-7, Petitioner states that “[i]n Grounds 5-7, in place of *Jazayeri*, the proposed combination involves modifying *Carlson* pursuant to *Murakami*’s biometric sensor and authentication process.” Pet., 71. Petitioner goes

on to incorporate by reference “[a]ll arguments and evidence from Grounds 1-4.”
Pet. 71.

Patent Owner incorporates by reference all arguments and evidence set forth above regarding Grounds 1-4. Further, Petitioner’s discussion of *Murakami* fails to cure the deficiencies set forth above in Section VI.A.1. Petitioner identifies no disclosures in *Murakami* that resolve the issues a POSITA would have had combining *Carlson* and *Jazayeri*. Ex. 2006 ¶108. Petitioner states that *Murakami* teaches the use of waveforms reflecting anatomical structure and physiological processes, and by comparing stored waveforms to measured waveforms, “the system may ‘grant or deny access to a device or [provide] authorization for transaction.’” Pet., 72-73 (quoting *Murakami*, 16:35-17:3). But Petitioner fails to point to, and *Murakami* fails to provide, any details regarding the identified “authorization for transaction.” Ex. 2006 ¶108. Petitioner’s citation to a single-line disclosure in *Carlson* of a fingerprint sensor (Pet., 74) does not provide motivation to combine *Carlson* with *Murakami*’s complicated and untemplated biometric authentication processes. Ex. 2006 ¶109. This is especially true in light of *Carlson*’s skepticism of device-based authentication as such a measure “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; *see also* Ex. 2006 ¶109.

For the reasons set forth here and above in Section VI.A.1, the *Carlson-Jazayeri-ISO-14443-Murakami* device of Petitioner’s Ground 5 would therefore not have rendered obvious “in response to at least the proximity condition having been satisfied between the smartphone and the entity and *in response to a physiological parameter*, wirelessly providing by the smartphone, using the first air interface, information to the entity and wirelessly receiving by the smartphone, using the first air interface, information from the entity” of claim limitation 1[c] nor “in response to at least the proximity condition having been satisfied between the smartphone and the entity and *in response to a physiological parameter*, wirelessly providing, using the first air interface, information to the entity and wirelessly receiving, using the first air interface, information from the entity” of claim limitation 10[d]. Ground 5 thus fails for both independent claims, and all dependent claims. Ground 5, and thus Grounds 6-7, fail. Ex. 2006 ¶110.

**2. Ground 5 Would Not Have Rendered Obvious
“wirelessly receiving by the smartphone, using the first
air interface, information from the entity.”**

With respect to Grounds 5-7, Petitioner fails to point out with particularity its theory with respect to the “receiving by the smartphone” argument. Petitioner states that “[i]n Grounds 5-7, in place of *Jazayeri*, the proposed combination involves modifying *Carlson* pursuant to *Murakami*’s biometric sensor and authentication process.” Pet., 71. While Petitioner incorporates its arguments and evidence from

Grounds 1-4, it does not specifically map the claim elements, or state whether the digital receipt from *Jazayeri* is retained in the proposed combination of Ground 5. Petitioner has thus failed to point out with particularity where this claim element is met in Ground 5. This lack of clarity warrants the Director denying institution, as sorting out the vagaries of Petitioner's theories for Grounds 5-7 would not be "an efficient use of Office resources." *See Zhuhai Cosmx Battery Co., Ltd., v. Ningde Amperex Tech. Ltd.*, IPR2025-00405, Paper 24 at 2 (P.T.A.B. Oct. 15, 2025) (vacating decision granting institution and denying institution of *inter partes* review).

To the extent Petitioner maintains that this element of *Jazayeri* is somehow part of this ground, despite replacing *Jazayeri* with *Murakami*, Patent Owner incorporates by reference its argument and evidence above in Section VI.A.2. Petitioner provides no discussion of any disclosure in *Murakami* that would have motivated a POSITA to modify *Carlson* such that a digital receipt is "receiv[ed] by the smartphone." Ex. 2006 ¶111. The *Carlson-Jazayeri-ISO-14443-Murakami* device of Ground 5 would not have rendered obvious "wirelessly receiving [by the smartphone], using the first air interface, information from the entity" of claim limitations 1[c] and 10[d]. Ground 5 thus fails for both independent claims, and all dependent claims. Ground 5, and thus Grounds 6-7, fail. Ex. 2006 ¶111.

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 7,019 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