

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

TELCOM VENTURES LLC,
Patent Owner

Case No. IPR2025-01237
U.S. Patent No. 11,924,743

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	LEGAL STANDARD.....	5
III.	BACKGROUND	6
	A. THE '743 PATENT	6
	B. <i>CARLSON</i> (EX. 1005)	8
	C. <i>JAZAYERI</i> (EX. 1007)	10
	D. <i>SHERMAN</i> (EX. 1014)	11
	E. <i>ISO-14443</i> (EX. 1016).....	11
	F. <i>DOYLE</i> (EX. 1008).....	11
	G. <i>BIRCH</i> (EX. 1031)	12
	H. <i>MURAKAMI</i> (EX. 1009).....	12
IV.	CLAIM CONSTRUCTION.....	12
V.	LEVEL OF ORDINARY SKILL IN THE ART	14
VI.	THE DIRECTOR SHOULD NOT INSTITUTE <i>INTER PARTES</i> REVIEW.....	14
	A. <i>CARLSON</i> 'S REQUEST FOR PPAI WOULD NOT HAVE RENDERED OBVIOUS "SELECTIVELY REQUESTING AN AUTHORIZATION TO ESTABLISH SAID CAPABILITY."	15
	B. GROUNDS 1-8 WOULD NOT HAVE RENDERED OBVIOUS "RESPONSIVE TO SENSING A VALUE OF A PARAMETER AND RESPONSIVE TO DETERMINING THAT THE VALUE OF THE PARAMETER SENSED SATISFIES A CRITERION, SELECTIVELY ESTABLISHING A MASTER-SLAVE RELATIONSHIP AND SELECTIVELY REQUESTING AN AUTHORIZATION TO ESTABLISH SAID CAPABILITY."	24
	1. <i>Carlson</i> 's Request for PPAI Would Not Have Rendered Obvious "responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion, selectively establishing a master-slave relationship and selectively requesting an authorization to establish said capability." (Grounds 1-8)	26

2.	There Would Not Have Been a Motivation to Combine <i>Carlson</i> 's Device With The Biometric Authentication Device of <i>Murakami</i> to Render Obvious "responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion, selectively establishing a master-slave relationship and selectively requesting an authorization to establish said capability." (Grounds 5-8).....	29
C.	<i>CARLSON</i> 'S PPAI WOULD NOT HAVE RENDERED OBVIOUS "RECEIVING THE AUTHORIZATION TO ESTABLISH THE CAPABILITY RESPONSIVE TO SAID SELECTIVELY REQUESTING AN AUTHORIZATION AND ESTABLISHING THE CAPABILITY AT THE SMARTPHONE RESPONSIVE TO SAID RECEIVING THE AUTHORIZATION." (GROUNDS 1-8)	32
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)	12, 13
<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)	13
<i>Realtime Data, LLC v. Iancu</i> , 912 F.3d 1368 (Fed. Cir. 2019)	13
<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).....	6
<i>Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.</i> , 200 F.3d 795 (Fed. Cir. 1999)	13
STATUTES	
35 U.S.C. § 103	2
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	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 establishing a capability at a smartphone to conduct a financial transaction; the method comprising:
1[a]	responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion; selectively establishing a master-slave relationship, and selectively requesting an authorization to establish said capability; then
1[b]	receiving the authorization to establish the capability, responsive to said selectively requesting an authorization, and establishing the capability at the smartphone responsive to said receiving the authorization;
1[c]	wherein said selectively establishing a master-slave relationship, said selectively requesting an authorization and said receiving the authorization comprises wirelessly transmitting/receiving using a WiFi air interface protocol, an Orthogonal Frequency Division Multiplexing air interface protocol and/or an Orthogonal Frequency Division Multiple Access air interface protocol; and
1[d]	wherein the value of the parameter that is sensed comprises a signal, a number, a word, a code, a velocity, an acceleration, a time-of-day, a position, 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.
Claim 2	
2[pre]	The method of claim 1, further comprising:
2[a]	repeatedly sensing said value of the parameter and repeatedly deciding, based on comparing the value of the parameter to the criterion, whether or not to maintain enabled a first function of the smartphone while maintaining disabled a second function of the smartphone; and
2[b]	maintaining enabled said first function while maintaining disabled said second function responsive to deciding that said value of the parameter continues to satisfy the criterion; or
2[c]	disabling said first function and enabling said second function responsive to deciding that the value of the parameter no longer satisfies the criterion.

Reference	Claim Limitation
Claim 3	
3[pre]	The method of claim 1, wherein following said establishing the capability at the smartphone, the method further comprises:
3[a]	responsive to satisfying a proximity condition and responsive to sensing the value of the parameter and determining that the value of the parameter sensed satisfies the criterion, using the capability to conduct the financial transaction that has been established at the smartphone and conducting the financial transaction by paying for a product;
3[b]	wherein said paying for a product comprises sensing that the proximity condition is satisfied relative to an access point maintained by a vendor at a point of purchase counter, by detecting a short-range signal that is transmitted by the access point, determining that the value of the parameter that is sensed satisfies the criterion and then, responsive to having sensed that the proximity condition is satisfied relative to the access point and having determined that the value of the parameter sensed satisfies the criterion, paying for the product by selectively sending information to at least one device;
3[c]	wherein said paying for the product by selectively sending information to at least one device comprises selectively and wirelessly transmitting information to the at least one device using unlicensed frequencies; and
3[d]	wherein said paying for the product by selectively sending information to at least one device is further responsive to said selectively requesting an authorization, said receiving the authorization and said establishing the capability at the smartphone.
Claim 4	
4[pre]	The method of claim 3,
4[a]	wherein said paying for a product further comprises deducting/withdrawing an amount of money from an account.
Claim 5	
5[pre]	The method of claim 4,
5[a]	wherein said selectively sending information to at least one device comprises selectively sending information to the access point maintained by the vendor at the point of purchase counter and to at least one other device that is predetermined; and

Reference	Claim Limitation
5[b]	wherein the method further comprises selectively receiving information from the access point maintained by the vendor at the point of purchase counter and from at least one other device that is predetermined.
Claim 6	
6[pre]	The method of claim 4,
6[a]	wherein said using unlicensed frequencies comprises using unlicensed frequencies over a short-range link in a Time Division Duplex operation.
Claim 7	
7[pre]	The method of claim 1, wherein prior to said selectively requesting an authorization the method comprises:
7[a]	enabling a first function of the smartphone while disabling a second function of the smartphone responsive to sensing the parameter and responsive to determining that the parameter sensed satisfies the criterion; then
7[b]	selectively communicating with a device by using a communications capability of the first function, selectively establishing the master-slave relationship with the device and selectively requesting from the device the authorization to establish the capability for conducting the financial transaction.
Claim 8	
8[pre]	A smartphone that is configured to perform operations in order to establish a capability to conduct a financial transaction; the operations comprising:
8[a]	responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion, selectively establishing a master-slave relationship, and selectively requesting an authorization to establish said capability; then
8[b]	receiving the authorization to establish the capability, responsive to said selectively requesting an authorization, and establishing the capability at the smartphone responsive to said receiving the authorization;

Reference	Claim Limitation
8[c]	wherein said selectively establishing a master-slave relationship, said selectively requesting an authorization and said receiving the authorization comprises wirelessly transmitting/receiving using a WiFi air interface protocol, an Orthogonal Frequency Division Multiplexing air interface protocol and/or an Orthogonal Frequency Division Multiple Access air interface protocol; and
8[d]	wherein the value of the parameter that is sensed comprises a signal, a number, a word, a code, a velocity, an acceleration, a time-of-day, a position, 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.
Claim 9	
9[pre]	The smartphone of claim 8, wherein the operations further comprise:
9[a]	repeatedly sensing said value of the parameter and repeatedly deciding, based on comparing the value of the parameter to the criterion, whether or not to maintain enabled a first function of the smartphone while maintaining disabled a second function of the smartphone; and
9[b]	maintaining enabled said first function while maintaining disabled said second function responsive to deciding that said value of the parameter continues to satisfy the criterion; or
9[c]	disabling said first function and enabling said second function responsive to deciding that the value of the parameter no longer satisfies the criterion.
Claim 10	
10[pre]	The smartphone of claim 8, wherein following said establishing the capability at the smartphone, the operations further comprise:
10[a]	responsive to satisfying a proximity condition and responsive to sensing the value of the parameter and determining that the value of the parameter sensed satisfies the criterion, using the capability to conduct the financial transaction that has been established at the smartphone and conducting the financial transaction by paying for a product;

Reference	Claim Limitation
10[b]	wherein said paying for a product comprises sensing that the proximity condition is satisfied relative to an access point maintained by a vendor at a point of purchase counter, by detecting a short-range signal that is transmitted by the access point, determining that the value of the parameter that is sensed satisfies the criterion and then, responsive to having sensed that the proximity condition is satisfied relative to the access point and having determined that the value of the parameter sensed satisfies the criterion, paying for said product by selectively sending information to at least one device;
10[c]	wherein said selectively sending information to at least one device comprises selectively and wirelessly transmitting the information to the at least one device using unlicensed frequencies;
10[d]	wherein said paying for the product by selectively sending information to at least one device comprises selectively and wirelessly transmitting information to the at least one device using unlicensed frequencies; and
10[e]	wherein said paying for the product by selectively sending information to at least one device is further responsive to said selectively requesting an authorization, said receiving the authorization and said establishing the capability at the smartphone.
Claim 11	
11[pre]	The smartphone of claim 10,
11[a]	wherein said paying for a product further comprises deducting/withdrawing an amount of money from an account.
Claim 12	
12[pre]	The smartphone of claim 11,
12[a]	wherein said selectively sending information to at least one device comprises selectively sending information to the access point maintained by the vendor at the point of purchase counter and to at least one other device that is predetermined; and
12[b]	wherein the operations further comprise selectively receiving information from the access point maintained by the vendor at the point of purchase counter and from at least one other device that is predetermined.
Claim 13	
13[pre]	The smartphone of claim 10,

Reference	Claim Limitation
13[a]	wherein said using unlicensed frequencies comprises using unlicensed frequencies over a short-range link in Time Division Duplex operation.
Claim 14	
14[pre]	The smartphone of claim 8, wherein prior to said selectively requesting an authorization the operations comprise:
14[a]	enabling a first function of the smartphone while disabling a second function of the smartphone responsive to sensing the parameter and responsive to determining that the parameter sensed satisfies the criterion; then
14[b]	selectively communicating with a device by using a communications capability of the first function, selectively establishing the master-slave relationship with the device and selectively requesting from the device the authorization to establish the capability for conducting the financial transaction.

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 1-14 (the “Challenged Claims”) of U.S. Patent No. 11,924,743 (the “’743 Patent,” Ex. 1001). The Petition sets forth eight Grounds. In all Grounds, Petitioner relies on U.S. Patent No. 8,229,852 to *Carlson* (“*Carlson*,” Ex. 1005) in combination with other references in each of these Grounds. Indeed, the Petition relies heavily on multi-reference combinations in an attempt to cobble together a system that allegedly meets the claimed inventions of the ’743 Patent. The eight separate Grounds are summarized in the below chart.

Ground	Claims	Proposed Ground of Unpatentability
1	Claims 1, 7, 8, and 14	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> ¹ in view of <i>Jazayeri</i> ² and <i>Sherman</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 U.S. Patent Application Publication No. 2007/0232358 (“*Sherman*,” Ex. 1014).

Ground	Claims	Proposed Ground of Unpatentability
2	Claims 3-6 and 10-13	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> in view of <i>Jazayeri</i> , <i>Sherman</i> , and <i>ISO-14443</i> ⁴
3	Claims 2 and 9	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> in view of <i>Jazayeri</i> , <i>Sherman</i> , and <i>Doyle</i> ⁵
4	Claim 5	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> in view of <i>Jazayeri</i> , <i>Sherman</i> , <i>ISO-14443</i> , and <i>Birch</i> ⁶
5	Claims 1, 7, 8, and 14	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> in view of <i>Murakami</i> ⁷ , and <i>Sherman</i>
6	Claims 3-6 and 10-13	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> in view of <i>Jazayeri</i> , <i>Sherman</i> , <i>ISO-14443</i> , and <i>Murakami</i>
7	Claims 2 and 9	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> in view of <i>Sherman</i> , <i>Doyle</i> , and <i>Murakami</i>
8	Claim 5	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> in view of <i>Jazayeri</i> , <i>Sherman</i> , <i>ISO-14443</i> , <i>Birch</i> , and <i>Murakami</i>

Petitioner’s combinations fail for several reasons. First, across all eight Grounds, the Petition fails to show that “selectively requesting an authorization to establish said capability” is taught or rendered obvious by the prior art. Petitioner

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

⁵ U.S. Patent Application Publication No. 2002/0095586 (“*Doyle*,” Ex. 1008).

⁶ U.S. Patent No. 7,213,742 (“*Birch*,” Ex. 1031).

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

relies on *Carlson*'s alleged request for a pseudo primary account identifier ("PPAI") as the claimed "selectively requesting an authorization to establish said capability." Pet., 28 (Grounds 1-4), 72-74 (incorporating analysis of Grounds 1-4 into Grounds 5-8). But *Carlson*'s request for a PPAI is not the claimed "selectively requesting an authorization to establish said capability," nor would *Carlson*'s disclosure render this limitation obvious to a person of ordinary skill in the art ("POSITA"). Instead, *Carlson*'s request for a 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 the claimed "authorization to establish said capability" 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 and not dependent on whether a function is enabled in *Carlson*'s wireless device.

Second, across all eight Grounds, Petitioner fails to show that "responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion . . . selectively requesting an authorization to establish said capability" is taught or rendered obvious by the prior art. Again, for

all eight Grounds, Petitioner relies only on *Carlson*'s alleged request for a pseudo primary account identifier ("PPAI") as the claimed "requesting an authorization to establish said capability." Pet. 28 (Grounds 1-4), 72-74 (incorporating analysis of Grounds 1-4 into Grounds 5-8). But *Carlson*'s PPAI can be received or generated without unlocking the wireless device via biometric authentication. Accordingly, Petitioner's mapped "requesting an authorization to establish said capability" is not "responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion."

Similarly in Grounds 5-8, Petitioner fails to show that a POSITA would have been motivated to combine *Carlson*'s device with *Murakami*'s biometric authentication device to render obvious "responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion . . . selectively requesting an authorization to establish said capability." As with Grounds 1-4, *Carlson* itself does not suggest using biometrics to request an authorization. And the additional biometrics in the form of a heartbeat sensor of *Murakami* would defy *Carlson*'s stated goal of having the request for PPAI be instantaneous and not result in delays. *Murakami* itself acknowledges that its own biometric sensor can be "impractical" because of the time it takes to capture a good sample. See *Murakami*, 33:4-6.

Finally, across all eight Grounds, Petitioner fails to show that “receiving the authorization to establish the capability responsive to said selectively requesting an authorization and establishing the capability at the smartphone responsive to said receiving the authorization” is disclosed or would have been rendered obvious by the prior art. As discussed above, *Carlson*’s request for a PPAI does not disclose or render obvious “requesting an authorization.” Because that limitation provides the antecedent basis for the limitation “receiving the authorization to establish the capability responsive to said selectively requesting an authorization and establishing the capability at the smartphone responsive to said receiving the authorization,” the Petition’s identified Grounds necessarily fail to disclose or render obvious these limitations.

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

II. LEGAL STANDARD

The Petition must both “clearly point out the differences between the claimed invention and [the prior art]” and “explain why a person of ordinary skill in the art would have found the claimed subject matter obvious in spite of those differences.”

Synopsys, Inc. v. Mentor Graphics Corp., IPR2012-00041, Paper 16 at 14 (P.T.A.B. Feb. 22, 2013). The Petition must recite where the challenged limitation is found in the reference(s) and explain why a POSITA would have modified the primary reference with the recited limitation from the secondary reference(s). *Microsoft Corp. v. Secure Web Conf. Corp.*, IPR2014-00745, Paper 12 at 11-13 (P.T.A.B. Sept. 29, 2014). The Petition must establish, **with particularity**, the grounds and evidence that support invalidating the challenged claims. 35 U.S.C. § 312(a)(3). In addition, the Director institutes based on what the Petition **actually presents** and not what it could have reasonably contained. *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1381 (Fed. Cir. 2016). The Director cannot “deviate from the grounds in the petition and raise its own” theories of invalidity. *Sirona Dental Sys. GmbH v. Institut Straumann AH*, 892 F.3d 1349, 1356 (Fed. Cir. 2018).

III. BACKGROUND

A. The ’743 Patent

Applicants filed U.S. Patent Application No. 18/489,517 on October 18, 2023, which issued as U.S. Patent No. 11,924,743 on March 5, 2024. ’743 Patent at 1. The ’743 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 '743 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. '743 Patent, 1:28-33, 6:17-27; *see also* Ex. 2006, ¶61. In the prior art, mobile wireless devices were rigidly configured to perform a predetermined number of functions. '743 Patent, 1:42-47; *see also* Ex. 2006, ¶61. To overcome this rigidity, the '743 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. '743 Patent, 1:52-57; *see also* Ex. 2006, ¶61. The '743 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.” '743 Patent, 1:47-50; *see also* Ex. 2006, ¶61.

The '743 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.” '743 Patent, 6:19-23; *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.” ’743 Patent, 6:25-28; *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.” ’743 Patent, 6:32-34; *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. ’743 Patent, 6:45-49; *see also* Ex. 2006, ¶62.

The Examiner issued only one rejection, rejecting the application for double patenting over claims 1, 6, 11, and 14 of U.S. Patent No. 11,770,756. Ex. 1002 at 243. The Examiner allowed the claims of the ’743 Patent following the Applicants’ submission of a terminal disclaimer. *Id.* at 350; Ex. 2006, ¶65.

B. *Carlson* (Ex. 1005)

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

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

from the portable wireless device from a greater distance than specified in standards used for contactless readers.” *Carlson*, 2:1-6.

Carlson describes “[t]heft of sensitive information, such as an account number, using wireless interrogation or interception of communications from portable wireless device” as a “major concern for consumers and businesses alike.” *Carlson*, 2:7-10. *Carlson* notes that wireless interrogation can “occur at virtually any time and place,” and “[o]nce the victim of the wireless interrogation discovers that they had sensitive information stolen, it is often too late to discover where the theft took place.” *Carlson*, 2:10-16. As a result, “[t]he victim must then deal with the consequences and hassle of correcting the unauthorized access and possible uses of the information.” *Carlson*, 2:16-18.

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

Carlson’s solution describes the use of “pseudo primary account identifiers” or “PPAI.” *Carlson*, 2:62-63. According to *Carlson*, “[p]seudo primary account identifiers may include identifiers that are similar in format to a consumer’s real

account identifier.” *Carlson*, 5:30-32. “These account identifiers may include account numbers or any other alphanumeric sequence.” *Carlson*, 2:66-3:1. *Carlson* also describes the PPAI as “bogus, fake, decoy, substitute, or the like.” *Carlson*, 5:42-43.

Carlson describes “a method for conducting a transaction that includes receiving a pseudo account identifier that corresponds to a consumer’s account identifier.” *Carlson*, 3:3-6. In some embodiments of *Carlson*, “the pseudo primary account identifier may not be requested at all, but rather is pushed to the portable wireless device at any time, such as when the device is turned on, when the device is idle, periodically, or through any other such criteria.” *Carlson*, 7:4-7; *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. 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.*

D. *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].

E. *ISO-14443* (Ex. 1016)

Petitioner relies on the first edition of *ISO-14443* that Petitioner alleges was published in 2000 and 2002. Pet., 14 (citing Ex. 1033, Munford Declaration). The *ISO-14443* standard has four parts. Ex. 2006, ¶77. *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, ¶78.

F. *Doyle* (Ex. 1008)

U.S. Patent Application Publication No. 2002/0095586 to Doyle describes a method and system for continuously authenticating a user of a portable device via biometrics to improve the security of transactions or operations. *Doyle*, Abstract.

G. *Birch* (Ex. 1031)

U.S. Patent. No. 7,213,742 to Birch et al. describes a system that includes a mobile device comprising a wireless communications technology that enables the device to communicate with a back-end system. *Birch*, Abstract. This communication with the back-end system enables the device to obtain coupons and discounts for the transaction and e-receipts post-transaction. *Id.*, 7:55-60; *see also id.*, 13:19-35.

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 state” limitation. Pet., 6. The Petition then relies on *Murakami*’s biometric sensor for the “physiological state” limitation in Grounds 5-8. Pet., 6. 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 '743 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, ¶52. 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 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. *Carlson’s Request for PPAI Would Not Have Rendered Obvious “selectively requesting an authorization to establish said capability.”*

Petitioner’s proposed combinations, which rely on *Carlson’s* request for a PPAI, would not have rendered obvious “selectively requesting an authorization to establish said capability [to conduct a financial transaction].” Ex. 2006, ¶¶82-83. Claim limitation 1[a] states “responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion, selectively establishing a master-slave relationship, and selectively ***requesting an authorization to establish said capability.***” (emphasis added). “Said capability” derives its basis from “a capability at a smartphone to conduct a financial transaction” of claim limitation 1[pre]. Claim limitation 8[a] similarly states “responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion, selectively establishing a master-slave relationship and selectively ***requesting an authorization to establish said capability.***” (emphasis added). Again, “said capability” derives its basis from “a capability to conduct a financial transaction” of claim limitation 8[pre]. All dependent claims depend from one of the two independent claims that include these limitations. For Grounds 1-4, Petitioner alleges that states that “*Carlson-Jazayeri* teaches Claim 1(a).” Pet., 21; *see also* Pet., 36 (discussing claim limitation 8[a] and stating “[s]ee *supra* Claim 1(a)”). For Grounds 5-8, Petitioner modifies “*Carlson*

pursuant to *Murakami*'s biometric sensor and authentication process" (Pet., 73) and incorporates by reference "[a]ll arguments and evidence from Grounds 1-4." Pet., 74.

While Petitioner identifies *Carlson-Jazayeri* as disclosing this claim limitation, the Petition relies exclusively on *Carlson*'s request for a PPAI for "requesting an authorization to establish said capability," stating that "because the financial transaction requires requesting and receiving the PPAI before the transaction may proceed for that particular transaction or a particular limited set of transactions, the PPAI is an authorization to conduct that particular transaction or a particular limited set of transactions in *Carlson*'s system." Pet., 28. *see also* Pet., 74 (incorporating analysis of *Carlson* into Grounds 5-8).⁸ That is, Petitioner equates a PPAI to an authorization to perform a particular transaction or particular limited set of transactions. However, for at least three key reasons, a POSITA would not have understood *Carlson*'s request for PPAI to be the claimed "requesting an authorization to establish said capability."

First, the request for PPAI in *Carlson* is not "requesting an authorization" to perform a particular transaction, as the Petition alleges, and *Carlson*'s disclosure of

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

a request for PPAI would not have rendered this limitation obvious to a POSITA. Ex. 2006, ¶84. *Carlson*'s request for PPAI is not “an authorization to establish [a capability to conduct a financial transaction]”—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, ¶84.

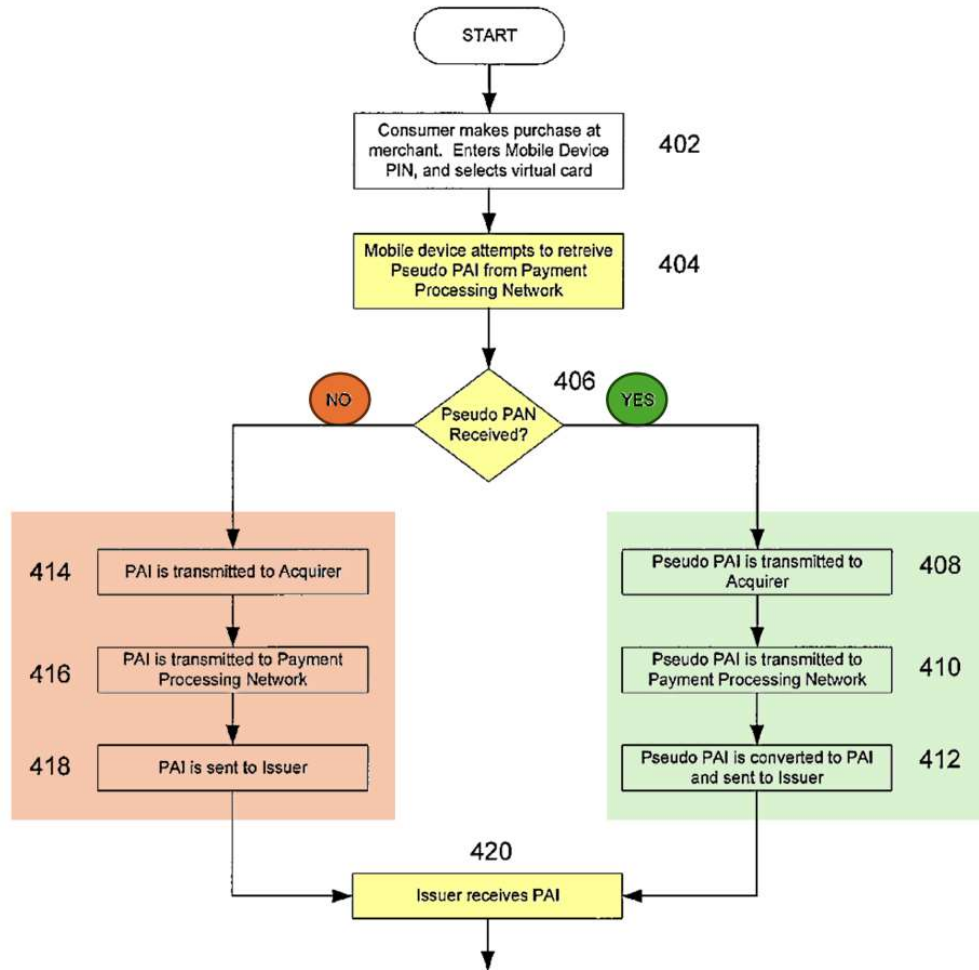
Instead, *Carlson* explains that a PPAI is used during a financial transaction, instead of the user's real account identifier, to protect the user from “[t]heft of sensitive information . . . using wireless interrogation or interception of communications from [a] portable wireless device.” *Carlson*, 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; *see also id.*, 2:66-3:1. *Carlson* also describes the PPAI as “bogus, fake, decoy, substitute, or the like.” *Carlson*, 5:42-43. *Carlson* describes that “[i]n the simplest case, this request message [for a PPAI] may include the primary account identifier.” *Carlson*, 6:40-41. Accordingly, a POSITA would understand that a request for a PPAI that only requires the primary account number and no other identifying information to secure the request is simply a request for a proxy for the primary account identifier and not a request for an authorization. Ex. 2006, ¶85. 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 Petitioner alleges. Ex. 2006, ¶85.

Second, it follows that because the PPAI of *Carlson* is not an authorization, a **request** for PPAI is not information requesting an authorization. Ex. 2006, ¶86. Petitioner is relying on an embodiment of *Carlson* wherein the wireless device requests a PPAI from the payment processing network. Pet. 26-27. According to the Petition, because *Carlson*’s financial transaction “**requires** requesting and receiving the PPAI before the process may proceed” (Pet., 28 (emphasis added)), then the request for PPAI is necessarily the authorization to establish a function to conduct a financial transaction. But Petitioner is wrong. The mere fact that this embodiment discloses **requesting** the PPAI does not transform the PPAI into information requesting **an authorization**. Ex. 2006, ¶86.

The purpose of requesting a PPAI in *Carlson* is so that both *Carlson*’s wireless device and the payment processing network can 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. Ex. 2006, ¶87. 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, ¶87. 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, ¶87.



Carlson, Fig. 4 (cropped and annotated); Ex. 2006, ¶87.

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 response to a request for PPAI. Ex. 2006, ¶88. 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; *see also id.*, 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 non-existent request for a PPAI cannot act as a request for “authorization to establish [the capability to to conduct a financial transaction].” Ex. 2006, ¶88.

Third, *Carlson* itself undercuts Petitioner’s theory that a request for a PPAI by *Carlson*’s device is “requesting an authorization.” *Carlson* discloses a different message, an “authorization request message” that is independent of *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, ¶89. *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*, 8:13-15. “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, ¶89.

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., 31 n.8 (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 PAI [primary account identifier], rather than PPAI), the function relied upon in the Proposed Grounds has not been established absent a PPAI.” *Id.* However, Petitioner invents these two distinct secure and less secure transactions. *Carlson* contemplates just one exchange—one where, regardless of whether a PPAI is received in response to a request for the PPAI, the exact same financial account is debited for the exact same amount for the exact same purchase. *Carlson*, 14:34-46 (referring to Figure 4 showing that, regardless of whether a PPAI is received, “settlement and clearing processes occur at step 428 to actually transfer funds from the account held at the issuer to the merchant”); Ex. 2006, ¶90. 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.⁹ Ex. 2006, ¶¶90-91. Because a PPAI-based financial transaction is still possible in *Carlson*, a request for PPAI is not “requesting an authorization to establish said capability” 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, ¶91. 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 disclosed in *Carlson* where the “particular transaction or particular limited set of transactions” “requires requesting and receiving the PPAI” as the Petition suggests. *See* Pet., 28. The request for PPAI therefore does not disclose and would not have rendered obvious “information requesting an authorization” to perform a particular financial transaction. Ex. 2006, ¶92.

⁹ Petitioner’s error stems from its erroneous belief that the PPAI must be requested.

For at least these reasons, *Carlson*'s request for PPAI fails to disclose and would not have rendered obvious "requesting an authorization to establish said capability" of independent claims 1 and 8, and thus all dependent claims as well. Ex. 2006, ¶¶92-93. With respect to Grounds 1-4, Petitioner identifies nothing in the proposed combination outside of *Carlson*'s request for PPAI, and thus Grounds 1-4 all fail. Ex. 2006, ¶92. With respect to Grounds 5-8, Petitioner fails to provide element by element mapping, but "modifying *Carlson* pursuant to *Murakami*'s biometric sensor and authentication process" (Pet., 73) does not change the shortcomings of *Carlson*'s PPAI process with respect to this claim element. Ex. 2006, ¶93. Grounds 5-8 all fail. Ex. 2006, ¶93.

B. Grounds 1-8 Would Not Have Rendered Obvious "responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion, selectively establishing a master-slave relationship and selectively requesting an authorization to establish said capability."

Even if Petitioner had established that the Grounds render "selectively requesting an authorization to establish said capability" obvious, Petitioner fails to establish that "selectively requesting an authorization to establish said capability" is preformed "*responsive to* sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion."

Claim limitation 1[a] states "responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a

criterion . . . selectively requesting an authorization to establish said capability.” “[S]aid capability” refers to “a capability at a smartphone to conduct a financial transaction” of claim limitation 1[pre]. Similarly, claim limitation 8[a] states “responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion . . . selectively requesting an authorization to establish said capability.” Again, “said capability” refers to “a capability to conduct a financial transaction” of claim limitation 8[pre]. All dependent claims depend from one of the two independent claims that include these limitations.

Petitioner alleges that “because the PPAI is requested only after unlocking the device following biometric authentication, the establishment of the master-slave relationship and the request for authentication are responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion.” Pet., 28-29 (addressing Grounds 1-4); *see also id.*, at 73-74 (addressing Grounds 5-8 by “modifying *Carlson* pursuant to *Murakami*’s biometric sensor and authentication process”). Accordingly, Petitioner identifies *Carlson*’s request for PPAI as the alleged “requesting an authorization.” But Petitioner fails to establish that *Carlson*’s request for PPAI is “responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion,” or, with respect to Grounds 5-8, that a POSITA would have

been motivated to combine *Carlson* with *Murakami* to render obvious this limitation.

As set forth in detail below, for these reasons, Grounds 1-8 fail. Ex. 2006, ¶96.

1. *Carlson’s Request for PPAI Would Not Have Rendered Obvious “responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion, selectively establishing a master-slave relationship and selectively requesting an authorization to establish said capability.” (Grounds 1-8)*

The claims require that “selectively requesting an authorization to establish said capability” is performed “responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion.” The Petition argues that when the device is unlocked, “the portable wireless device 202 may then *request a pseudo primary account identifier [(‘PPAI’)]*.” Pet., 26 (quoting *Carlson*, 12:34-37) (emphasis in original); *see also* Pet., 28. At the same time, the Petition relies on a single embodiment in *Carlson* where the PPAI is requested by *Carlson’s* device, and the Petition identifies *Carlson’s* request for PPAI as the “requesting an authorization.”¹⁰ Pet., 28. The

¹⁰ While the Petition relies on *Jazayeri* for the purposes of biometrics, the Petition relies solely on the alleged disclosures of *Carlson* for “responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed

Petition fails to show that *Carlson*'s requesting of a PPAI is performed responsive to unlocking the device. Ex. 2006, ¶97.

In the very embodiment on which Petitioner relies, *Carlson* emphasizes that the device does not need to be unlocked for *Carlson*'s device to request a PPAI. *Carlson*, 7:7-11 (“[A] request for a [PPAI] need not occur only after a user has enabled the device and selected an account.”). Specifically, *Carlson* explains that “[a] request for a [PPAI] may occur ***at any time***, such as when the device is turned on, when the device is idle, periodically, or through any other such criteria.” *Carlson*, 7:10-14 (emphasis added); *see also Carlson*, 6:59-61 (explaining that a PPAI can “expire after a certain number of transactions or after a certain time period”). A POSITA would therefore understand that *Carlson*'s wireless device is ***always*** capable of requesting a PPAI—or at the very least, the request for a PPAI is independent of *Carlson*'s device being unlocked. Thus, *Carlson*'s request for PPAI is ***not*** necessarily performed responsive to unlocking the device. Ex. 2006, ¶97. This furthers *Carlson*'s stated objective of creating a “transparent” user experience such

satisfies a criterion.” Pet., 28 (“[B]ecause the PPAI is requested only after unlocking the device . . . the request for authentication [is] responsive to sensing a value of a parameter.”).

that the user “need not know that the pseudo account identifier is ever retrieved.”
Carlson, 15:63-16:3.

Additionally, and as described above, there are many other ways a PPAI could be received or generated without any request from the device itself, and thus without unlocking the device. Ex. 2006, ¶98. Specifically, *Carlson* teaches that the PPAI may never be requested but instead may be either pushed to the device by the network (*Carlson*, 7:3-6) or even generated by the device itself (*Carlson*, 7:17-18). These alternative embodiments do not require unlocking the device, nor do they require requesting a PPAI. *See Carlson*, 7:3-6 (“The pseudo account identifier may not be requested at all, but rather is pushed to the portable wireless device ***at any time***, such as when the device is turned on, when the device is idle, periodically, or through other such criteria.” (emphasis added)).

Carlson therefore does not disclose, nor would it have rendered obvious, the use of a security measure such as a physiological parameter to request a PPAI. Ex. 2006, ¶¶98-99. Accordingly, a POSITA would not understand that the combination of *Carlson* and *Jazayeri* would have rendered obvious “responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion, . . . selectively requesting an authorization to establish said capability.” Ex. 2006, ¶99. Grounds 1-4 thus fail. Furthermore, for these reasons,

and those additional reasons set forth in detail below, Grounds 5-8 also fail. Ex. 2006, ¶100.

2. There Would Not Have Been a Motivation to Combine *Carlson*'s Device With The Biometric Authentication Device of *Murakami* to Render Obvious “responsive to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion, selectively establishing a master-slave relationship and selectively requesting an authorization to establish said capability.” (Grounds 5-8)

The Petition states that “[i]n Grounds 5-8, in place of *Jazayeri*, the proposed combination involves modifying *Carlson* pursuant to *Murakami*'s biometric sensor and authentication process.” Pet., 73. Grounds 5-8 fail for the additional reason that a POSITA would not have been motivated to combine *Carlson* with *Murakami* to render obvious claim limitations 1[a] and 8[a]. Ex. 2006, ¶102.

The Petition argues that “*Carlson* modified to unlock its device pursuant to the biometric authentication process described by *Murakami* teaches the claimed limitation of a parameter” Pet., 75. However, as discussed above, *Carlson* does not require that its device be unlocked to enable its request for PPAI. *Carlson*, 7:7-11 (“[A] request for a [PPAI] need not occur only after a user has enabled the device and selected an account.”). Because *Carlson*'s wireless device is always capable of requesting a PPAI, *Carlson*'s request for a PPAI is not necessarily enabled responsively to unlocking the device. Thus, unlocking the device using the biometric authentication process described by *Murakami* does not render obvious “responsive

to sensing a value of a parameter and responsive to determining that the value of the parameter sensed satisfies a criterion, selectively establishing a master-slave relationship and selectively requesting an authorization to establish said capability.” Ex. 2006, ¶103.

Additionally, *Murakami* (in place of *Jazayeri*) does not overcome the deficiencies of the *Carlson-Jazayeri* combination. Petitioner relies on *Murakami*’s sensor “used to measure a heartbeat waveform, a dynamic variable determined by measuring a user’s heartbeat.” Pet., 73 (citing *Murakami*, 32:30-33:6). Specifically, the Petition relies on an embodiment wherein a waveform is monitored, and “25 features are extracted out of a waveform to create a list of 25 parameters, each parameter requesting a different unique feature for a particular person’s heartbeat waveform.” *Murakami*, 32:20-22. *Murakami* teaches “tak[ing] more than one reading of the biometric for purposes of individualization.” *Murakami*, 32:31-33:1. “In one preferred embodiment 30 heartbeats were taken and monitored to do the individualization for each person being identified. In another preferred embodiment, a hundred heartbeats were used. In capturing a good sample, it is preferred to take as many samples as is possible.” *Murakami*, 33:1-4. *Murakami* even acknowledges that “taking a large number of sample waveforms takes time and using an extended period of time to individualize the waveform may be impractical.” *Murakami*, 33:4-6. As a result, a POSITA would have understood that *Murakami*’s biometric sensor

provides updated security but at the expense of a significant amount of the user's time. Ex. 2006, ¶104. A POSITA would not have been motivated to implement *Murakami*'s biometric sensor for everyday use or for functionalities that require little or no delay. Ex. 2006, ¶104.

As discussed above in Section VI.B.1, the PPAI request in *Carlson* is supposed to be “transparent” to the user. *Carlson*, 15:67-16:3. Therefore, a POSITA would have understood that *Carlson* teaches away from using *Murakami*'s biometric sensor for its PPAI request because the *Murakami* sensor would be inconvenient and cause unwanted delay. Ex. 2006, ¶105. A POSITA would have understood that the added security from the heartbeat sensor of *Murakami* would not be beneficial in *Carlson*'s system because *Carlson* emphasizes that the user should not “experience any delay in conducting [a] purchase.” *Carlson*, 15:63-67. Therefore, a POSITA would not have been motivated to implement *Murakami*'s biometric sensor in *Carlson*'s device because of the delay introduced. Ex. 2006, ¶105.

For at least these reasons, *Carlson* alone or in combination with *Murakami* does not disclose or render obvious this limitation. Ex. 2006, ¶106. Grounds 5-8 fail. Ex. 2006, ¶106

C. *Carlson’s PPAI Would Not Have Rendered Obvious “receiving the authorization to establish the capability responsive to said selectively requesting an authorization and establishing the capability at the smartphone responsive to said receiving the authorization.” (Grounds 1-8)*

Claim limitation 1[b] states “*receiving the authorization to establish the capability* responsive to said selectively requesting an authorization, and establishing the capability at the smartphone responsive to said receiving the authorization.” (emphasis added). “[T]he capability” refers to “a capability at a smartphone to conduct a financial transaction” of claim limitation 1[pre]. Claim limitation 8[a] similarly states “*receiving the authorization to establish the capability*, responsive to said selectively requesting an authorization, and establishing the capability at the smartphone responsive to said receiving the authorization.” (emphasis added). Again, “the capability” refers to “a capability to conduct a financial transaction” of claim limitation 1[pre]. All dependent claims depend from one of the two independent claims that include these limitations. Petitioner alleges that “*Carlson-Jazayeri* teaches Claim 1(b).” Pet., 29; *see also id.*, 36 (addressing claim limitation 8[b] and stating “[s]ee *supra* Claim 1(b)”).

The Petition alleges that *Carlson* teaches limitation 1[b], stating that “[o]nce the portable *wireless device has received the [PPAI]*, the transaction may continue.” Pet., 29 (quoting *Carlson*, 13:10-11) (emphasis in original); *see also id.*, 36. But as explained above, *Carlson’s* PPAI is not an authorization and does not establish the

capability to conduct a financial transaction. *See supra* Section VI.A; Ex. 2006, ¶¶108-109.

The PPAI of *Carlson* does not disclose and would not have rendered obvious “the authorization to establish the capability.” Therefore, for Grounds 1-4 the proposed combinations fail to disclose or render obvious “receiving the authorization to establish the capability” of independent claims 1[b] and 8[b], and thus all dependent claims as well. Ex. 2006, ¶109. Grounds 1-4 fail.

Regarding Grounds 5-8, the Petition states that “Grounds 5-8 differ from Grounds 1-4 only in the proposed modifications to *Carlson* pertaining to the biometric sensor and authentication process.” Pet., 73. Accordingly, Grounds 5-8 also do not disclose and would not have rendered obvious “receiving the authorization to establish the capability” via *Carlson*’s PPAI. Ex. 2006, ¶110. Grounds 5-8 therefore fail to disclose or render obvious “the authorization to establish the capability” of independent claims 1[b] and 8[b], and thus all dependent claims as well. Ex. 2006, ¶110. Grounds 5-8 fail.

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 6,989 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