

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,

Petitioner,

v.

PROXENSE, LLC

Patent Owner

U.S. Patent No. 8,352,730 B2
IPR Case No. 2024-00232

PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I.	Introduction	1
II.	Related Matters.....	2
III.	The ‘730 Patent.....	3
IV.	Claim Construcion.....	4
A.	Applicable Law.....	4
B.	Claim Construction issued by W.D. Texas.....	4
1.	37 C.F.R. § 42.100(b) Statement.....	4
2.	Previously Construed Terms	6
C.	Third Party Trusted Authority	6
D.	Receiving an Access Message Allowing Access to an Application.....	7
E.	Grounds 1 and 2: Obviousness over Ludtke and Obviousness over Ludtke and Kon	8
1.	Third Party Trusted Authority	10
2.	Receiving an Access Message Allowing Access to an Application.....	17
V.	Conclusion	25

TABLE OF AUTHORITIES

	Page(s)
 Cases	
<i>GPNE Corp. v. Apple Inc.</i> , 830 F.3d 1365 (Fed.Cir. 2007)	12, 19
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005) (en banc)	2, 4, 8, 18
<i>Proxense v. Samsung Electronics, Co., Ltd. et al.</i> , No. 6:21-CV-00210 (W.D. Tex. March 5, 2021)	1
<i>Regents of the Univ. of Minnesota v. AGA Medical Corp.</i> , 717 F.3d 929 (Fed.Cir. 2013)	12
<i>SafeTCare Mfg., Inc. v. Tele-Made, Inc.</i> , 497 F.3d 1262	8
<i>SkinMedica, Inc. v. Histogen Inc.</i> , 727 F.3d 1187 (Fed.Cir 2013)	8, 18
<i>Sony Corp. v. Iancu</i> , 924 F.3d 1235 (Fed.Cir. 2019)	12
<i>Thorner v. Sony Computer Ent. Am. LLC</i> , 669 F.3d 1362 (Fed. Cir 2012)	3, 4, 8
<i>Verizon Services Corp. v. Vonage Holdings Corp.</i> , 503 F. 3d 1295	8
<i>Watts v. XL Systems, Inc.</i> , 232 F.3d 877 (Fed.Cir. 2000)	12, 18
 Rules and Statutes	
35 U.S.C. § 316	1
37 C.F.R.§ 42.120.....	1

EXHIBIT LIST

No.	Exhibit Description
2001	Claim Construction Order in <i>Proxense v. Samsung Electronics, Co., Ltd. et al.</i> , No. 6:21-CV-00210-ADA
2002	Memorandum In Support of Claim Construction Order in <i>Proxense v. Samsung Electronics, Co., Ltd. et al.</i>
2003	<i>Intentionally Left Blank.</i>
2004	Claim Construction Order in <i>Proxense v., Google LLC</i> , No. 6:23-cv-00320-ADA
2005	Opening Claim Construction Brief in <i>Proxense v. Microsoft Corporation</i> , No. 6:23-cv-00319-ADA
2006	Responsive Claim Construction Brief in <i>Proxense v. Microsoft Corporation</i>
2007	Reply Claim Construction Brief in <i>Proxense v. Microsoft Corporation</i>
2008	Sur-reply Claim Construction Brief in <i>Proxense v. Microsoft Corporation</i>
2009	Case Schedule in <i>Proxense v., Google LLC</i>
2010	Order Denying Motion to Transfer in <i>Proxense v., Google LLC</i>
2011	Order from the Federal Circuit Regarding Mandamus Petition
2012	Order Denying Motion to Transfer in <i>Proxense v. Microsoft Corporation</i>
2013	Google's Invalidity Contentions Cover Pleading
2014	Email from William Atnipp, dated May 3, 2024
2015	Microsoft's Amended Preliminary Invalidity Contentions
2016	Claim Construction Order in <i>Proxense v., Microsoft Corp.</i> , No. 6:23-cv-00319-ADA
2017	Opening Claim Construction Brief in <i>Proxense v. Google, LLC</i> , No. 6:23-cv-00320-ADA
2018	Declaration of Troy Carrothers

I. INTRODUCTION

Pursuant to 35 U.S.C. § 316 and C.F.R. § 42.120, the Patent Owner, Proxense LLC (“Proxense,” or “Patent Owner”) submits this Patent Owner Response in response to the Petition for *Inter Partes* Review of claims 1-6 and 8-17 of U.S. Patent No. 8,352,730 B2 (Ex. 1001, the ‘730 Patent, the “Patent at Issue”).

Proxense respectfully submits claims 1-6 and 8-17 (the “claims at issue”) are patentable over instituted grounds, as each of the grounds relies on references and combinations of references failing to show all elements of the claimed invention. Specifically, the asserted references, either alone or in combination, fail to show two claim elements: (1) sending codes for authentication by a “third party trusted authority”; as well as (2) receiving an “access message” from a third party trusted authority enabling or announcing access to an application. More specifically, the following claim elements are missing from and are not rendered obvious by the prior art of the instituted grounds with respect to all claims at issue:

sending one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority (**claim 1**);

sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority (**claim 8**);

requesting authentication of the one or more codes and the other data values by the agent (**claim 12**);

send the plurality of codes and the other data values to agent for authentication to determine whether the one or more codes and the other data values are legitimate, wherein the agent is a third-party trusted authority (**claim 15**);

receiving an access message from the agent allowing the user access to an application (**claims 1, 15**);

receives an access message from the agent allowing the user access to an application (**claim 8**);
receiving an access message from the agent, and in response to a positive access message, allowing the biometrically verified user access to an application (**claim 12**).

Because claims 1, 8, 12, and 15 are the independent claims from which all of the other claims at issue depend, all of the remaining claims at issue are patentable over the instituted grounds.

II. RELATED MATTERS

The Patent at Issue is currently being asserted against Petitioner in *Proxense v. Google LLC*, No. 6:23-CV-00320 (W.D. Tex. May 2, 2023). The Patent at Issue is also currently being asserted in *Proxense v. Microsoft Corporation*, No. 6:23-cv-00319-ADA (W.D. Tex. May 2, 2023). The Patent at Issue is also currently being asserted in *Proxense, LLC, v. Apple, Inc.*, No. 6:24-cv-00143 (W.D. Tex. March 18, 2024).

The District Court issued a Claim Construction Order on January 23, 2024, a copy of which is attached as Exhibit 2004. The same Court also issued a claim construction order in another matter involving the 730 patent involving the same claim terms at issue here attached here as exhibit 2001. *Proxense v. Samsung Electronics Co. Ltd.*, No. 6:21-CV-00210, Dkt 043 (W.D. Tex. Jan. 18, 2022); The Court's claim construction order from *Proxense v Microsoft* is attached as exhibit 2016. *Proxense v. Microsoft Corporation*, No. 6:23-cv-00319, Dkt 042.

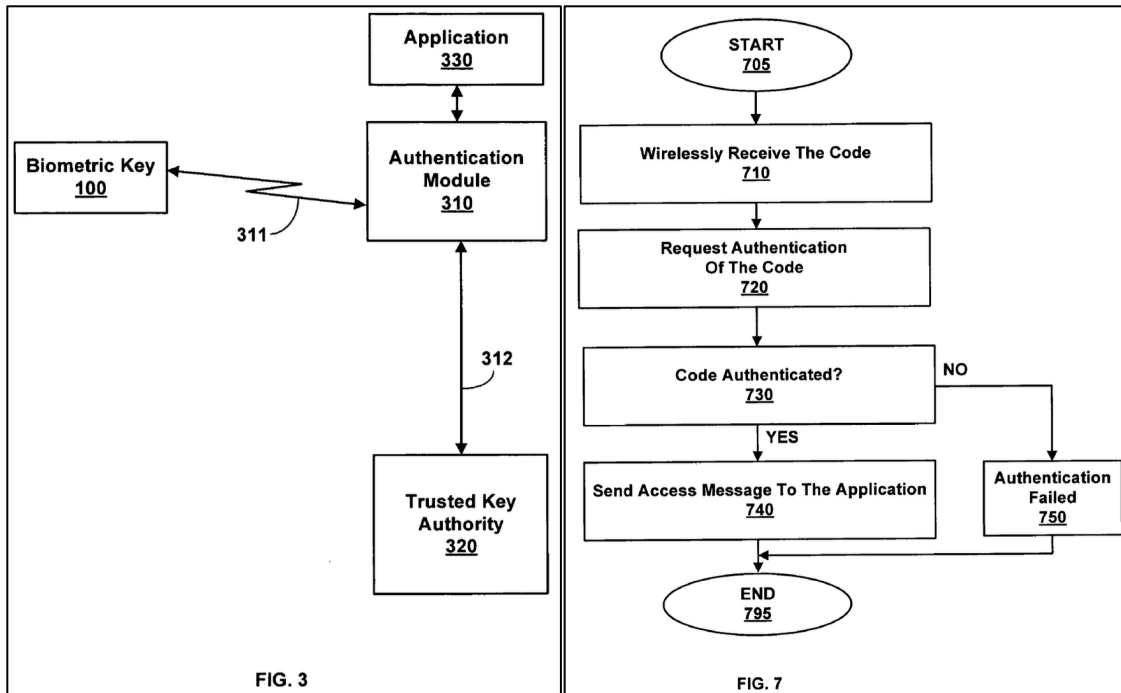
Final Invalidity Contentions were served by Petitioner on March 18, 2024, a copy of which is attached as Exhibit 2013.

For the major elements that are missing in all of Petitioner's prior art references, Patent Owner presents below a summary of the constructions currently requested by each party in District Court.

The validity of the Patent at Issue has also been challenged in the following proceedings before the Office. IPR2024-01333, IPR2024-01326, IPR2024-00775.

III. THE ‘730 PATENT

The ‘730 patent relates to a personal digital key that authenticates a user by sending a device ID code to a third party trusted authority for authentication and wherein an access message is received from the trusted third party enabling or announcing access to an application. With reference to Figure 2, an enrollment module 222 registers a user with biometric key 100 by persistently storing biometric data associated with the user (e.g., a digital image of the retina, fingerprint, or voice sample) in persistent storage 226. 730 Pat. at 4:1–2, 4:24–28; 4:43–55. With reference to Figure 3(reproduced below), authentication module 310 requires the device ID code (indicating successful biometric verification) from the personal digital key and provides that ID code to the third party trusted authority. 730 Pat. at 6:18-47. Authentication module 310 then sends a message to application 330 to allow the user access to the application responsive to a successful authentication by trusted key authority 320. 730 Pat. at 5:16-18; 5:34–36, 6:28-30, Fig. 7 (reproduced below).



IV. CLAIM CONSTRUCTION

A. Applicable Law

In *inter partes* review, claims are construed under *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). 83 Fed. Reg. 51,340 (Oct. 11, 2018). Under *Phillips*, claim terms are generally given in their ordinary and customary meaning as understood by a person of ordinary skill in the art when read in the context of the specification and prosecution history. *Phillips* 415 F.3d at 1313. “There are only two exceptions to this general rule: 1) when a patentee sets out a definition and acts as his own lexicographer, or 2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution.” *Thorner v. Sony Computer Ent. Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir 2012).

B. Claim Construction issued by W.D. Texas

1. 37 C.F.R. § 42.100(b) Statement

Terms appearing within the claims of the 730 Patent have been construed three times by a district court in *Proxense, LLC v. Samsung Electronics, Co., Ltd. et al.*, No. 6:21-CV-00210 (W.D.

Tex. March 5, 2021) (“*Proxense v. Samsung*”), *Proxense, LLC v., Google LLC*, No. 6:23-cv-00320-ADA (W.D. Tex. May 2, 2023) (“*Proxense v. Google*”), and *Proxense v. Microsoft*. The Claim Construction Order and Memorandum in Support of Claim Construction Order issued in *Proxense v. Samsung*, along with a Transcript of the Markman hearing, are provided herewith as Exhibits 2001, 2002, and 2003, respectively. Likewise, the Claim Construction Orders issued in *Proxense v. Google* and *Proxense v. Microsoft* are provided herewith as Exhibits 2004 and 2016, respectively.

In the above identified related matter before the Western District Texas, the Hon. Alan Albright provided the following constructions:

Term	Court’s Construction
“integrated device”	No Construction necessary. Plain and Ordinary meaning.
“persistently storing biometric data of [a/the] user and a plurality of codes and other data values comprising a device ID code uniquely identifying [an/the] integrated device and a secret decryption value”	Plain and ordinary meaning wherein the meaning is: “ persistently storing biometric data of [a/the] user and a plurality of codes and other data values are stored; within this storage is also (1) a device ID code uniquely identifying an integrated device and (2) a secret decryption value.”
“an access message ... [allowing / allows] The user [access to an application / to access an application]”	No Construction necessary. Plain and ordinary meaning.
“The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the use”	No construction necessary. Plain and ordinary meaning.

In addition, Patent Owner and Petitioner agreed to the following constructions:

Term	Court’s Construction
“device ID code”	“a unique code identifying a device”
“access message”	“a signal or notification enabling or announcing access”

“persistently storing . . . a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered”	No Construction necessary.
--	----------------------------

Exhibit 2017

2. Previously Construed Terms

Pursuant to Rule 42.100(b), Patent Owner requests the Board to consider and adopt the relevant constructions previously given to the following terms in *Proxense v. Samsung*, *Proxense v. Google*, and *Proxense v. Microsoft*. See *Loper Bright Enterprises v. Raimondo*, 144 S. Ct. 2244, 2273 (2024). This Board must “presume, unless otherwise compelled, that the same claim term in the same patent or related patents carries the same construed meaning.” *Omega Engineering, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1334 (Fed. Cir. 2003).

C. Third Party Trusted Authority

The term “third-party trusted authority” was previously construed consistent with its plain and ordinary meaning to mean “a trusted authority that is an entity separate from the parties to a transaction.” Ex. 1007 at 15. This Board has adopted that construction as well. DI at 4, 12, 30. Patent Owner agrees with this construction but challenges its application in the Petition, in particular the finding that the “parties to a transaction” of the Patent (relative to the claimed third party trusted authority) can be a user and a vendor or merchant. Petitioner incorrectly implies that Patent Owner has agreed to such a construction in which the parties to a transaction could be a user and a vendor. Pet. at 30.

This is consistent with Patent Owner’s previous “agree[ment] that at a ‘third- party trusted authority’ is *an institution or entity that is outside of the multi-party system (user and application or vendor)* that is being authenticated” and the Board’s construction that third-party trusted authority is a trusted authority that is an entity separate from the parties to the transaction,” and one that is “separate from

the principal parties to a transaction.” Ex. 1007, 13-15 (emphases added).”

However, the proper reading of Patent Owner statement, as quoted from Patent Owner’s Preliminary Response from IPR2021-01444, is that the parties could be either a user and an application (where a user is utilizing the claimed device or method) or, in another embodiment, a vendor and an application (where a vendor is utilizing the claimed device or method as a type of user). The Patent at Issue provides no intrinsic support for Petitioner’s construction. This is the case because, as demonstrated in Section G.1 below, the specification and claim language at issue requires that at least one of the parties to the claimed transaction must be the application being accessed. As such, the Petition does not accurately reflect the construction that Patent Owner has agreed to and, for the reasons detailed in Section G.1 below, the Board should reject Petitioner’s proposed construction.

D. Receiving an Access Message Allowing Access to an Application

The Petitioner and Patent owner agree on the construction of the term “access message” to mean “a signal or notification enabling or announcing access.” However, Petitioner is taking a contrary position here by claiming that a “transaction confirmation” can be an access message Pet. at 32 (“[a]fter validating that the transaction device is in good standing and that the selected account has sufficient funds for the transaction, the TPOCH *issues a transaction confirmation*’ (access message) ‘*back to the personal POS terminal*’”), 41, 50, 56.

Petitioner’s new construction fails to account for the claim term “access to an application” when referencing the prior art Ludtke. By removing entirely that claim limitation “access to an application” and truncating the term to “access message” as though that was all that the claims require, petitioner fails to show that this limitation is disclosed. As explained in detail below, a “transaction confirmation” alone is neither a message enabling nor a message

announcing access to an application; it is a message announcing that a transaction has been completed.

The plain and ordinary meaning of “access message” is a message enabling entry to, communication with, or use of an object wherein the object is the claimed application. *See* Access Definition & Meaning - Merriam-Webster, <https://www.merriam-webster.com/dictionary/access> (emphasis added). Common to all of the definitions in this reference is that something is made available. Additionally, per definitions (a), (b), and (d) of this reference, a thing is made available to use, enter, or communicate with. Specifically, the “things” referred to in the definition are objects (people, places, and things). Accordingly, the plain and ordinary meaning of “access” is to enable entry to, communication with, or use of an object.

The relevant “object” for which access is enabled or announced in the claims of the Patent at Issue, in every independent claim, is an **application**. The claims explicitly recite this requirement. “The construction that stays true to the claim language and most naturally aligns with the patent's description of the invention will be, in the end, the correct construction.” *Renishaw PLC v. Marposs Societa'per Azioni*, 158 F. 3d 1243, 1250 (Fed. Cir. 1998). It would be improper to construe “access message” as something other than a signal or notification enabling or announcing a user’s access to (ability to enter, communicate with, or make use of) an application.

E. Grounds 1 and 2: Obviousness over Ludtke and Obviousness over Ludtke and Kon

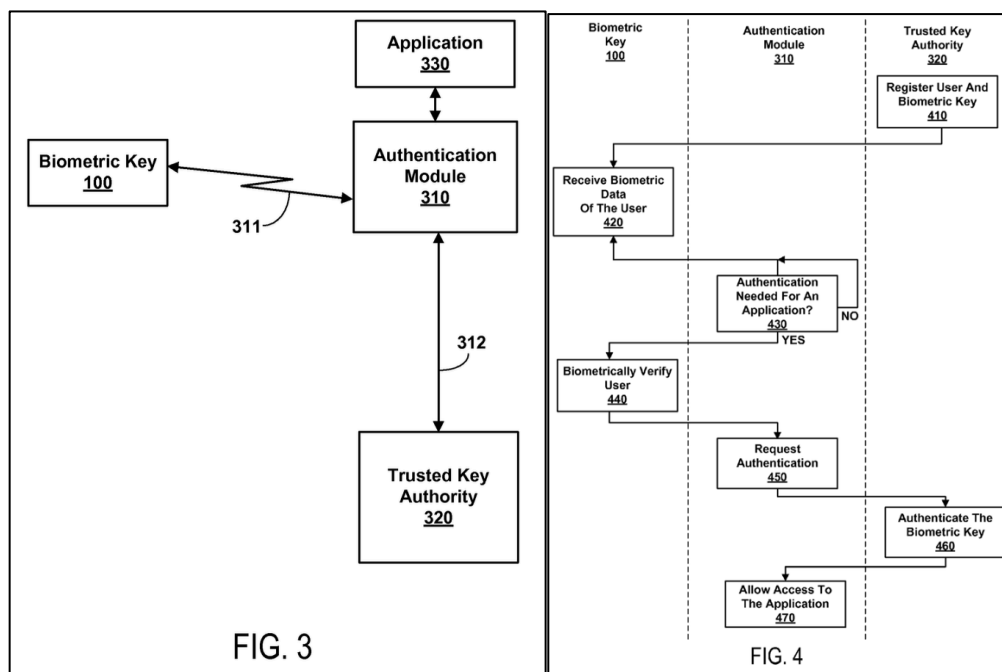
The Petition fails to demonstrate that Ludtke et al. (Ex. 1005, U.S. Patent No. 7,188,110 to (“Ludtke”)), either alone or in combination with Kon et al. (U.S. Patent Application Publication No. 2002/0046336) (“Kon”)) renders obvious (1) a third party trusted authority; nor

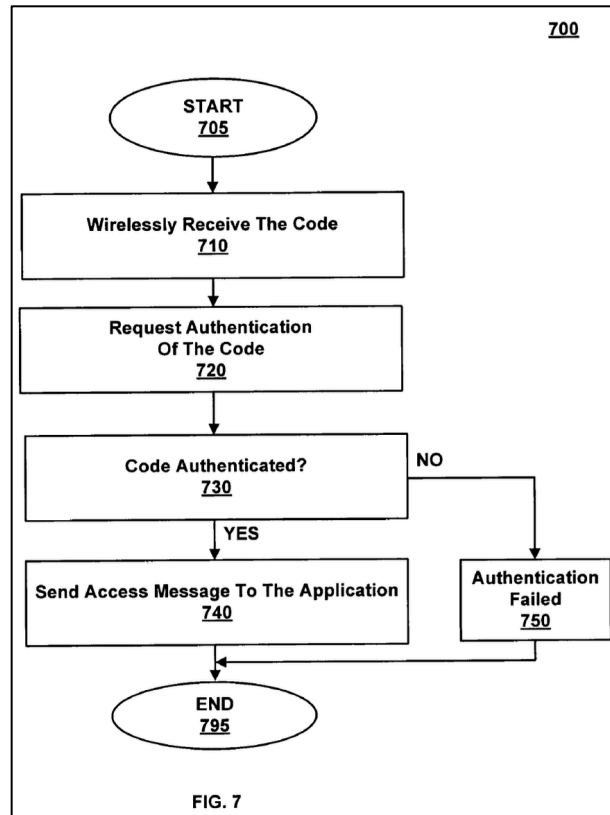
(2) receiving an access message allowing access to an application. These references thus cannot render any of the challenged claims invalid and unpatentable.

As demonstrated fully below, the transaction processing clearing house of Ludtke (TPCH) is fundamentally different from the third party trusted authority (TPTA) of the Patent at Issue in the following two ways. **First**, the TPCH is the application being accessed. In every single example in Ludtke, the TPCH that authenticates the user also has the user's account information, makes the final transaction authorization, completes the transaction, and sends a confirmation that promises payment to the merchant. This includes the example where the TPCH causes a third party financial institution to settle the transaction after it is completed because, by the express language of Ludtke, the TPCH confirms the transaction and causes the settlement in that example too. By contrast, the TPTA of the present Patent can only authorize the user and send an access message regarding that authorization to the application. The TPTA never authorizes the transaction because it cannot make a promise on behalf of the application being accessed; this is a key aspect of the present invention. **Second**, the TPCH does not send an access message to an application — instead it sends a confirmation to the merchant. The TPCH's confirmation is not regarding access to an application, it is a promise to pay. Ludtke's TPCH is therefore set up to provide access to the private data that it holds (transaction privacy information, which is the application the user is trying to access) at the time that the TPCH authenticates the transaction device. By contrast, the claims of the 730 Patent require an additional step: for the application to receive an access message from the TPTA. By definition, the application must be separate from the TPTA because there would be no need to receive an access message allowing access to that application if the TPTA and the application being accessed were the same entity as is the case with Ludtke's TPCH.

1. Third Party Trusted Authority

The 730 Patent only discloses embodiments where the parties to the transaction are a user and an application being accessed by that user. *See* 730 Pat. Abstract; 2:1–5; 5:15–39 (“System 300 comprises an authentication module 310 in communication with biometric key 100, a trusted key authority 320, and an application 330 . . . Application 330 is a resource that can be accessed by a verified and authenticated user.”); 6:2–4 (“In one embodiment, authentication can be required prior to allowing access to an application (e.g., application 330).”); 7:18–23 (If authentication is successful, the trusted key authority sends an access message to the application to allow user access and/or provide additional information from the profile 740 (such as the user's age).”; Figs. 3, 4, 7 (reproduced below). No other embodiment is provided in the specification that would permit the parties to be anything other than a user and an application that the user is trying to access.





Nor does the grocery store example (DI at 11) expand the scope of the 730 patent claims such that a grocery merchant can be the claimed “application.” The grocery store example of the Patent at Issue refers to the **location** of the application being accessed, it does not discuss a transaction between a merchant and a user:

In one embodiment, the functionality of trusted key authority 320 is provided by a server or other computerized device.

In an open system, where unknown users can attempt authentication (e.g., in a public grocery store), trusted key authority 320 provides verification that a key presenting a certain code is legitimate. By contrast, in a closed system, only known users are legitimate (e.g., owners of a home), the trusted key authority 320 can be maintained locally and serves to verify that the key belongs to one of the limited number of users that can use the system.

730 Pat. 5:50-60. The focus of the grocery store example is to show that the claimed system might be found in a public place where the potential users are unknown. “[P]ublic grocery

store” and “owners of a home” are examples of possible locations for the system, not an example of parties to the transaction. The grocery store example pertains to an application that can be accessed by a system located in a public place. For the same reason, the second example in that paragraph does **not** disclose an embodiment where the user and the owners of a home are the parties to a transaction. The mere fact that the location is a public grocery store does not alter the parties to the transaction as those parties are disclosed throughout the entire specification and claims to be a user and an application. Notably, the words vendor and merchant do not appear in the Patent at Issue at all. Even if the grocery store example could be read as disclosing an embodiment where the parties are a user and the grocery store (a reading for which there is no support in the specification) the claims of the Patent do not include such an embodiment. The claims of this Patent only refer to a transaction where the parties are a user and an application being accessed.

The claims of the Patent at Issue require that the application to be an entity separate from the TPTA. **Claims 1 and 15** each recite “receiving an access message from the agent allowing the user access to an application.” Similarly, **claim 8** recites “receives an access message from the agent allowing the user access to an application.” Likewise, **claim 12** recites “receiving an access message from the agent; and in response to a positive access message, allowing the biometrically verified user access to an application.” The independent claims of the 730 Patent each recite three participants: the user; the third-party trusted authority; and the application the user is allowed to access. Thus, for all independent claims, the claims explicitly require the parties to the transaction be the user and the application, and that the transaction is the user gaining access to the application. The access message allowing access to an application must be *received* from the agent and thus **the claimed agent cannot be the same entity as the**

application under the wording of these claims. See *SIMO Holdings Inc. v. Hong Kong uCloudlink Network Tech. Ltd.*, 983 F.3d 1367, 1378 (Fed. Cir. 2021) (“we should not infer that any particular embodiment is included in a claim when there is probative evidence that sufficiently indicates the contrary disclosed embodiments may be within the scope of other allowed but unasserted claims.”). The “third-party trusted authority,” therefore, is required by the express language of the claims to be a third-party with respect to the user and the application being accessed.

Here, the Board had made the following consistent observation: “[a]lthough the trusted key authority in this example is not a principal party to the transaction (*here, the parties are the user and the application*), it is an active participant in facilitating the transaction.” DI at 11 (emphasis added).

The TPCCH of Ludtke is the application being accessed. The TPCCH of Ludtke authenticates the transaction device, and confirms the transaction and authorizes it, it does not split these steps up like the claims of the Patent at Issue require. Ludtke follows what would have been, at the time, a standard credit card transaction and does not teach, like the Patent at Issue does, a change to this ordering of steps. Carrothers Decl.¹ ¶¶ 20-22. The following are all of the embodiments for how TPCCH of Ludtke confirms a transaction:

“The *TPCH, at step 1520, confirms the transaction and provides the confirmation to the vendor* and the user. At step 1525 *the vendor completes the transaction* without knowledge of the identity of the user.” Ludtke, 27:13-16 (emphasis added).

“Assuming that the transaction is successful, *the TPCCH returns a confirmation message to the retail POS terminal*, step 1616, which in turn may display an appropriate message to the clerk, step 1617. The clerk may then return the

¹ The Declaration of Troy Carrothers is attached hereto as Exhibit 2018.

transaction device and perhaps *a paper receipt of the transaction to the user*, step 1618.” Ludtke, 27:60-65 (emphasis added).

“After validating that the transaction device is in good standing and that the selected account has sufficient funds for the transaction, *the TPOCH issues a transaction confirmation back to the personal POS terminal*. The personal POS terminal reflects the transaction confirmation back to the web browser and the transaction device. The transaction device may display a transaction confirmation to the user and may additionally record the transaction in its local storage. The personal POS terminal may also record the transaction in its local storage. In addition, in alternate embodiments, *the personal POS terminal may enter the transaction directly into the user's personal finance program* (e.g., Quicken) which may be executing on the user's PC or on the personal POS terminal.” Ludtke, 29:15-28 (emphasis added).

“Secure distribution of physical (or electronic) content to the user is performed once the transaction is authorized. Subsequently, the *TPCH receives confirmation that the content was successfully shipped* to the user and the user has acknowledged receipt of the content. Once the confirmation is received, *the TPOCH processes the settlement of funds.*” Ludtke, 29:29-34 (emphasis added); see also Carrothers Decl. ¶¶ 20-22.

In all of the foregoing embodiments, TPOCH both authenticates the device and confirms the transaction and the merchant accepts the confirmation as payment. Carrothers Decl. ¶¶ 20, 21. Accordingly, the TPOCH is being accessed to provide a payment to the merchant via a confirmation message (i.e., authorization), which completes the transaction. Carrothers Decl. ¶¶ 20, 21. (“the transaction between the cardholder and the merchant is completed when the merchant accepts an authorization as payment.”) The TPOCH of Ludtke is thus the application that the user is trying to access -- the ability to pay the vendor with the user’s account (the private information) is the application. Ludtke thus fails to separate the application being accessed from the TPOCH. Carrothers Decl. ¶¶ 20, 30-31.

In an attempt to establish an “application” that is separate from the TPCCH and the user, the Petition points to the disclosures of Ludtke that deal with settlement (the actual transfer of funds at some point after the transaction has been completed) rather than either authorization or transaction confirmation. Carrothers Decl. ¶¶ 20-28. Ludtke itself teaches that “[t]he settlement of funds involves the transfer of the appropriate financial credit into the vendor’s account.” Ludtke, 29:35-36; Carrothers Decl. ¶ 21. Ludtke discloses four such settlement paradigms: (1) “the account is managed completely by the TPCCH, and thus the funds transfer is handled completely inside of the TPCCH.” Ludtke, 29:37-39; (2) , “the TPCCH 110 interfaces to at least one financial processing system 140 to perform associated financial transactions, such as confirming sufficient funds to perform the transaction, and *transfers to the vendor 125 the fees required to complete the transaction.*” Ludtke, 6:51-55 (emphasis added); (3) “the TPCCH may issue a funds settlement request to a third-party financial institution on behalf of the user, **causing the necessary funds to be transferred** to the vendor from the user’s account.” Ludtke, 29:43-46; and (4) “[T]he FP140 is contacted by the TPCCH requesting a generic credit approval of a particular account... The TPCCH 110 can request the credit using a dummy charge ID that can be listed in the monthly credit statement sent to the user, so that the user can reconcile his credit statement.” Ludtke, 7:12-20. All four of these settlement methods taught by Ludtke occur after the merchant has accepted the transaction confirmation (transaction authorization) issued by the TPCCH as payment and has tendered the goods or services. Carrothers Decl. ¶¶ 28-30. Moreover, all four settlement methods involve accessing the TPCCH as the application because the TPCCH controls the account. See Carrothers Decl. ¶¶ 28-30. Whether the TPCCH has the account on file or has control of the account at a financial institution, the result is the same: The TPCCH is performing the established function of a clearing house to settle the transaction by causing the

appropriate amount of money to be transferred from the user's account registered with the TPCB to the vendor's account. Carrothers Decl. ¶¶ 28-30. Each of the above four settlement methods is discussed in more detail below. See also Carrothers Decl. ¶¶ 28-30.

First, where the account is fully managed by the TPCB and the funds transferred inside the TPCB, the TPCB is the application being accessed by the user to make payment. The TPCB directs the transfer of funds from an account held by the TPCB to the vendor's account. Carrothers Decl. ¶ 24. Even if the settlement process was the proper scope for Ludtke's confirmation message, the TPCB would still be the application being access in this structure.

Second, where the TPCB interfaces with a financial processing system, the TPCB still fully in control of the funds; the TPCB here "transfers to the vendor 125 the fees..." In this method, the TPCB issues the user credit based on the availability of funds from the user's account at the financial institution. Carrothers Decl. ¶ 25. The TPCB again is in control of the funds and the transaction and, as such, is the application being accessed. At some point in the future, after the transaction has been completed, a settlement occurs as between the user and the TPCB. Carrothers Decl. ¶ 25. Even if the settlement process was the proper scope for Ludtke's confirmation message, the TPCB would still be the application being access in this structure.

Third, where the TPCB issues a settlement request to a third party financial institution, by the clear teachings of Ludtke, the TPCB is "causing the necessary funds to be transferred." Again, because the TPCB can exercise control over the user's account, the TPCB is the application being accessed. Carrothers Decl. ¶ 26. The difference is that here, unlike in the second example above, the TPCB directs the financial institution to settle with the vendor on the user's behalf. Carrothers Decl. ¶ 26. Nevertheless, the settlement request being discussed here, again, occurs after the TPCB has confirmed the transaction. Carrothers Decl. ¶ 26. This process

is much like an “account on file” transaction. Carrothers Decl. ¶ 26. But the authorization of the transaction, the confirmation that leads to the transaction being completed and still comes from the TPOCH. Carrothers Decl. ¶ 26. Even if the settlement process was the proper scope for Ludtke’s confirmation message, the TPOCH would still be the application being access in this structure.

Fourth, where the TPOCH directly gets credit approval with a dummy charge, the TPOCH, with access to the user’s account, is still the application that provides the approval. Carrothers Decl. ¶ 27. Here, the TPOCH provides access to a registered account to issue the “dummy charge,” collects funds from the user’s account and completes the transaction. Carrothers Decl. ¶ 27. The only difference in this method is that the goods and source is being hidden for privacy reasons and the transaction device and decipher the dummy charge and replace it with the private information for the user at a later time. Carrothers Decl. ¶ 27. This embodiment also does not change the fact that the TPOCH is the application being accessed by the user to make the payment.

Because Ludtke fails to disclose authentication by a third party trusted authority which is separate from the entity that is the application being accessed, Petitioner has not demonstrated that any of the claims of the Patent at Issue are unpatentable as obvious over Ludtke, alone or in combination with Kon.

2. Receiving an Access Message Allowing Access to an Application

Petitioner ignores, and therefore fails to establish obviousness for the explicit claim limitation that requires receiving an access message “allowing access to an application.” Every single asserted claim requires that the access message allow access to or announce access to an application. Petitioner clearly ignores the “application” requirement by citing to Ludtke’s recital of a message that confirms the transaction. Pet. at 32 (“[a]fter validating that the transaction

device is in good standing and that the selected account has sufficient funds for the transaction, the TPCCH *issues a transaction confirmation*’ (access message) ‘*back to the personal POS terminal*’”), 41, 50, 56. Petitioner fails to account for this claim term.

Ludtke discloses a transaction device that receives a transaction confirmation, not an authentication device that receives an access message. As a results, Petitioner fails to demonstrate that Ludtke discloses receiving an access message enabling or announcing access to an application because Ludtke only discloses confirming a transaction. Petitioner can only demonstrate that “Ludtke’s transaction devices receives an indication of ‘approval of the transaction to be performed.” Pet. 32-35, 41-44. In other words, Ludtke only provides a conformation once the transaction has been fully completed. As Petitioner points out,

After validating that the transaction device is in good standing and that the selected account has sufficient funds for the transaction, the TPCCH issues a transaction confirmation back to the personal POS terminal. The personal POS terminal reflects the transaction confirmation back to the web browser and the transaction device.

Pet. 32-33; (citing Ludtke, 29:10-23; Decl., 112).

This disclosure, and all related Ludtke disclosures that are cited in the Petition, show a transaction confirmation, not access to an application.

First, the transaction confirmation of Ludtke does not allow access to the POS terminal; the user already has access to the POS terminal and all of its software when they are triggering the transaction in the first place. The same is true for Ludtke’s disclosures related to a vendor’s website or URL: the user gains access to these resources at the beginning of the transaction. The authentication of the transaction device does not provide the user with any access to the “[host application software” or the “user application” software on the POS terminal that the user did not have before authenticating. Ludtke, 25:34-58. As described in Ludtke,

the POS terminal may collect the necessary information from the transaction device, e.g., digital wallet, combine it with the purchase data, and send it to the TPCCH. The TPCCH may then authorize the transaction, store data relevant to the transaction in its records and trigger a financial transfer to the vendor's account.

Ludtke, 23:50-55; see also 21:51-57 (“In one embodiment, a POS terminal is the link between the digital wallet or privacy card and the transaction privacy clearinghouse (TPCH) of the eCommerce system. The main purpose of the POS terminal is to establish a secure transaction connection between the transaction device and the TPCCH and to transfer transaction data to the TPCCH for completion of the transaction.”). A similar process for web transactions is shown in Figure 17 of Ludtke. Instead of receiving data from the digital wallet via a magnetic stripe on a privacy card, the POS

communicates with the transaction device, asking the transaction device to validate the user, confirm the user wants to make this transaction, and get the appropriate information for which account the user to use for payment.

Ludtke, 28:58-62. This is also shown by step 6 in Figure 17:

When information on the user's side of the transaction has been set up to perform a transaction, the personal POS terminal opens a secure communication session to the TPCCH, requesting a transaction. The personal POS terminal provides the transaction record that it received from the web browser and the unique ID of the transaction device. The TPCCH uses the unique ID of the transaction device to process the transaction.

Ludtke, 29:6-14. Accordingly, for both web and retail transactions, the primary purpose of Ludtke's POS terminal is to establish a secure connection with the TPCCH and to transfer transaction data to the TPCCH. Consequently, the user must have been allowed access to the merchant's store and POS prior to the receipt of the transaction confirmation from the TPCCH.

Second, likewise, the transaction confirmation received from the TPCB of Ludtke does not allow access to a website; the user already has access to the website at the beginning of a transaction. When making a web transaction, “[t]he user triggers the purchase, usually by clicking on a ‘Buy’ or similar button in the web browser.” Ludtke, 28:34-35. “Once a transaction has been triggered, the browser communicates with the personal POS terminal, requesting it to initiate a transaction.” Ludtke, 28:50-52. Then, as detailed above, the POS establishes a secure connection with the TPCB and transfers transaction data to the TPCB. Accordingly, to initiate a transaction, the user must have been allowed access to the website prior to the receipt of the confirmation from the TPCB.

Third, the transaction confirmation of Ludtke does not allow access to the functions of the transaction device/digital wallet; the user already has access to all of those functions. While the transaction device may receive receipts after each transaction, access to the files storing the receipts is constant, it is not somehow “allowed” by the receipt of any transaction confirmation. Rather, “[t]he user then has the data readily available for use on demand, whether it is for a business expense report or for personal record keeping.” Ludtke, 10:37–39. Accordingly, the user always has access to files storing electronic receipts.

Failing to find a direct disclosure of an access message that enables or announces access to an application, the Petition claims that a person of ordinary skill in the art would have intuited such an access message for other (undisclosed) wallet services. Pet. 32-33. The petition points to two disjointed, unrelated discussions in Ludtke: (1) a discussion of Ludtke’s transaction device such that “[o]nce the device has been initialized for secure transactions, additional services could be downloaded to the device.” Pet. 33 (citing Ludtke 19:45-50); and (2) a discussion of the “Art Background” generically stating that passwords or pins can be used for accessing “voice mail,

bank balances, dialing cards, credit reports, paying for purchases, depositing money, accessing stored messages, logging onto computers, etc.” Pet. 33 (citing Ludtke, 1:22-31). These two disclosures are completely unmoored from one another.² There is no disclosure within Ludtke of what the “additional services” could be, let alone any connection whatsoever between the theoretical “additional services” and the list of things that can be accessed with pins or passwords in the prior art. Ludtke thus makes no disclosure, nor says anything that renders obvious, that its transaction device can be configured to require authentication to access stored messages or log into a computer.

Nor is an ATM disclosed by Ludtke. Petition also claims that, from the Art Background’s mention of “depositing money” a person of ordinary skill would have intuited an ATM from Ludtke’s disclosures as an application of the authentication device. Pet. 34-46; Gray Decl. ¶115. Again, Ludtke makes no such disclosures. A clearing house can receive a deposit but Petitioner provides no citation nor extrinsic evidence as to how one of ordinary skill might make a clearing house that is configured to complete transactions give access to an ATM. Ludtke only discloses that a payment method as between a user and a merchant could be a debit card or directly from a bank account. Ludtke 18:52-55. But paying with a debit card is not a disclosure of an ATM. *See also*, Ludtke, 5:49-52 (“The transaction device may represent a single account such as a particular credit card, or it might represent multiple accounts such as a credit card, telephone card and debit card.”); 8:33-36 (“The user 240 uses the privacy card 205 to interface to the POS terminal in a manner similar to how credit cards and debit cards interface with POS terminals.”).

² The Gray Declaration claims that Ludtke defines the “additional services” in the “Art Background” section but the disclosure discussed therein provides no basis for this claim. Gray Decl. ¶114.

Thus, what is disclosed in Ludtke is specifically a “transaction device” not an access device.

Ludtke thus makes no disclosure, nor renders obvious, that its transaction device can be configured to access an ATM.

Nor does Ludtke’s discussion of digital content disclose an access message enabling or announcing access to an application. Petitioner states that Ludtke teaches access to an application because it discloses that “[s]ecure distribution of physical (or electronic) content...is performed once the transaction is authorized”—that is, once the access message is sent “back to the *web browser*” webpage. Pet. at 33. Petitioner references several disclosures within Ludtke where physical or digital content is distributed by the vendor after the vendor is paid by the TPC. Pet. at 26, 33 (citing Ludtke, 28:15-18, 28:26-40, 29:10-23, 29:29-30). However, even if the vendor of digital content could properly be considered the application being accessed (it cannot, as demonstrated above, the application the user seeks to access is their account for payment), Ludtke does not disclose a signal or notification enabling or announcing access to the digital content; Ludtke only discloses the delivery of that digital content to the user following the completion of a transaction. Thus, even if a vendor could be considered the application being accessed, the only thing disclosed in Ludtke is that a vendor can determine whether to deliver physical or digital goods to a user based on whether or not the vendor gets payment or a promise to pay **not** a signal enabling or announcing access. Such a signal is not disclosed nor is there any evidence that it would have been obvious.

Ludtke’s disclosures with respect to a web transaction for digital content are made with reference to Figure 17 (reproduced below). Ludtke 28:13-18 (“An example of a web-based transaction performed in accordance with the teachings of the present invention is discussed with reference to FIG. 17.”).

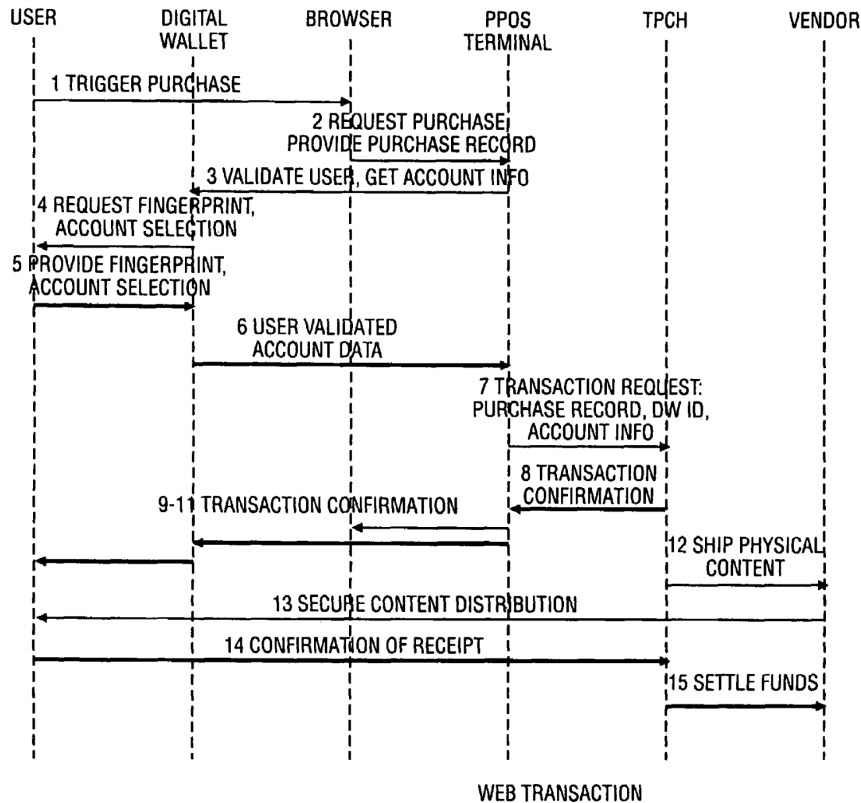


FIG. 17

As seen in figure 17 above, and in the teaching of Ludtke, the only reference to a “signal” that Petitioner points to is the access message is **the signal whereby the user initially requests the content**, not the delivery of the content.

The user has selected items to be purchased and is ready to trigger a purchase. The user may either navigate to a web page by using the facilities of the web browser, or by triggering a shopping activity using the transaction device. For example, if the transaction device is used to trigger shopping activity, the user may tap on an on-screen icon being displayed by the transaction device, e.g., digital wallet; and the digital wallet transmits a signal to the PC or DTV, via the personal POS terminal, which then transmits the signal to the web browser.

This disclosure refers to step 1 of figure 17, wherein the signal relates only to the user **triggering the purchase**. Petitioner thus incorrectly claims that the disclosed “signal” occurs after the transaction confirmation. Pet. at 26. Figure 7 above and Ludtke’s teachings make clear

that the transaction confirmation to the transaction device is an independent step from the delivery of goods (whether physical or digital) to the user. No access message enabling or announcing access to an application (even if the digital content can be said to be an application) is thus disclosed.

Because the invention of Ludtke is a transaction device, Ludtke focuses its disclosure on a vendor that completes a transaction. Ludtke Figs. 15-19. Ludtke's disclosures also include a discussion of sending a transaction confirmation to the user and vendor, of issuing a receipt to the user, and of vendor then completing the transaction. For instance, Ludtke discusses the shipping, return, and warranty system being managed by the TPC. Ludtke 32:5-33:29.

In light of those disclosures in Ludtke, the Gray declaration does not provide adequate extrinsic evidence that receiving an access message allowing access to an application would have been obvious. First, from a generic statement in the Art Background, Gray attempts to establish that a person of ordinary skill would have applied the transaction device to all of the possible things that passwords and pins can be used for mentioned in the background of the invention. Gray Decl. ¶¶ 114-117. As explained above, the Gray declaration does not establish that any of those was actually disclosed in Ludtke as something that could possibly be used with the disclosed "transaction device." Nor does he establish that it would have been obvious at the time, relying only on hindsight. Gray Decl. ¶¶ 116-117. Notably, and despite Petitioner's claims, none of the cites provided by petitioner have anything to do with pairing the transaction device to a computer or an ATM. Gray Decl. ¶¶ 116-117; Pet. at 35 (citing Ludtke, 1:22-31, 1:38-39, 5:49-52, 8:32-35, 18:52-55, 19:45-50).

Having failed to establish any actual "additional services" being disclosed in Ludtke, Gray also fails to establish that a person of ordinary skill would find it obvious, for a third party

to provide an access message enabling to announcing access to such services (even if they were disclosed). Gray Decl. §117. (“Accordingly, to the extent not expressly disclosed or suggested, a POSITA would have been motivated to configure Ludtke’s transaction device to access applications including an ATM, software, hardware, and a file, and had a reasonable expectation of success in doing so.”) Gray provides no valid reasoning, only hindsight again. Thus, even if the transaction device of Ludtke was disclosed with any of these “additional services,” the claim element of receiving an access message from the agent is not provided by this extrinsic evidence.

By failing to identify an access message relative to an application, Petitioner is ignoring a key aspect of the present invention of the Patent. Namely, the separation of tasks as between a third party that authenticates and an application that is being accessed (e.g. an application that can complete a transaction for the user). Petitioner does so because Ludtke skips a step that is required by the claims- authorization (TPTA) and transaction completion (access to the application) are all done in a single step within Ludtke and a transaction confirmation results. That is fundamentally different from the access message of the 730 Patent claims, which comes from the TPTA after authorization. As such, Ludtke is missing this claim element which is required by all independent claims at issue.

Because Ludtke fails to disclose receiving an access message from the third party trusted authority enabling or announcing access to *an application*, Petitioner has not demonstrated that any of the claims of the Patent at Issue are unpatentable as obvious over Ludtke, alone or in combination with Kon.

V. CONCLUSION

The Petition fails to demonstrate that Ludtke alone or in combination with Kon discloses (a) “third party trusted authority,” or (b) “receiving an access message allowing access to an

application” as properly construed. The Petition thus fails to demonstrate the challenged claims invalid and unpatentable.

Dated: October 15, 2024

Respectfully submitted by,

By: /David L. Hecht/
David L Hecht Reg. No 61,618
Hecht Partners LLP
125 Park Avenue, 25th Floor
New York, NY 10017
Tel: 212-851-6821
E: dhecht@hechtpartners.com

Counsel for Patent Owner

CERTIFICATE OF SERVICE (37 C.F.R. § 42.6(e))

Pursuant to 37 C.F.R. § 42.6(e), the undersigned hereby certifies that Patent Owner's Response was served on October 15, 2024 by e-mailing copies to the e-mail addresses as provided in Petitioner's Petition.

Dated: October 15, 2024

Respectfully submitted,

By: /David L. Hecht/
David L Hecht Reg. No 61,618
Hecht Partners LLP
125 Park Avenue, 25th Floor
New York, NY 10017
Tel: 212-851-6821
E: dhecht@hechtpartners.com

Counsel for Patent Owner

CERTIFICATE OF WORD COUNT

Under the provisions of 37 C.F.R. § 42.24, the undersigned hereby certifies that word count for the foregoing Patent Owner Response (excluding the table of contents, certificate of service, word count, or listing of exhibits) total 7,267 words, which is less than the number of words allowed under 37 C.F.R. § 42.24(b)(1).

Dated: October 15, 2024

Respectfully submitted,

By: /David L. Hecht/
David L Hecht Reg. No 61,618
Hecht Partners LLP
125 Park Avenue, 25th Floor
New York, NY 10017
Tel: 212-851-6821
E: dhecht@hechtpartners.com

Counsel for Patent Owner