IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICROSOFT CORPORATION,
Petitioner,

v.

PROXENSE, LLC
Patent Owner

U.S. Patent No. 8,352,730
IPR Case No.: IPR2024-00775

PATENT OWNER RESPONSE TO PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

I. INTRODUCTION 1

II. CLAIM CONSTRUCTION 1

A. 37 C.F.R. § 42.100(B) STATEMENT 1

B. THIRD-PARTY TRUSTED AUTHORITY 2

III. RESPONSE TO GROUNDS FOR INVALIDITY RAISED 7

A. [GROUND 1] – CLAIMS 1, 2, 4-9. 11, 12, AND 14-17 ARE NOT RENDERED OBVIOUS BY BURGER 7

1. Petitioner's First Example is Inoperable 7

2. Petitioner's Second Example Contradicts the Express Language of the Claims 15

3. Petitioner's Third Example Contradicts the Language of the Claims 20

B. [GROUND 2] – CLAIMS 3, 10, AND 13 ARE NOT RENDERED OBVIOUS BY BURGER AND ROBINSON 22

IV. CONCLUSION 22

EXHIBIT LIST

No.	
2001	Claim Construction Order in *Proxense v. Samsung Electronics, Co., Ltd. et al.*, No. 6.21-CV-00210-ADA
2002	Memo In Support of Claim Construction Order in *Proxense v. Samsung Electronics, Co., Ltd. et al.*
2003	Markman Transcript from *Proxense v. Samsung Electronics, Co., Ltd. et al.*
2004	Claim Construction Order in *Proxense v., Google LLC*, No. 6:23-cv-00320-ADA
2006	Claim Construction Order in *Proxense v., Microsoft Corp.*, No. 6:23-cv-00320-ADA
2007	Merriam-Webster Definition of Access available at https://www.merriamwebster.com/dictionary/access
2008	Chase Article on Credit Card Processing availiable at https://www.chase.com/personal/credit-cards/education/basics/credit-cardprocessing
2009	Stripe Statistics (2024): Revenue, Market Share & Growth Rate, https://capitaloneshopping.com/research/stripe-statistics/
2010	How Online Payment Processing Works | PayPal US, https://www.paypal.com/us/brc/article/how-online-payments processing-works
2011	How credit card processing works | Stripe, https://stripe.com/en-de/resources/more/how-credit-card-transaction-processing works-a-quick-guide
2012	How PayPal helps sellers process and accept credit card payments | PayPal US, https://www.paypal.com/us/brc/article/how-paypal-works-for-sellers.
2013	Card authorization explained: How does it work? | Stripe, https://stripe.com/resources/more/card-authorization-explained#what-is-card authorization.
2014	Definition of transaction | PCMag, https://www.pcmag.com/encyclopedia/term/transaction
2015	Transaction Definition & Meaning - Merriam-Webster, https://www.merriam-webster.com/dictionary/transaction

I. INTRODUCTION

Pursuant to 35 U.S.C. § 316(a)(8) and 37 C.F.R. § 42.120, Patent Owner Proxense LLC ("Proxense" or "Patent Owner") submits the following Patent Owner Response to the Petition for *inter partes* review of claims 1-17 of U.S. Patent No. 8,352,730 ("the 730 Patent") filed by Petitioner, Microsoft Corporation ("Petitioner" or "Microsoft").

The Petition asserts grounds of invalidity that are incompatible with the plain meaning of the claims and go well beyond the broadest reasonable interpretation. The explicit language of the claims recites "third-party trusted authority" that is a third party to a transaction in which the principal parties are a user allowed access and an application being accessed. Yet, the Petition asserts grounds of invalidity based upon transactions wherein the "third-party trusted authority" is a third-party with respect to as user and a bank, an advertiser, or a hotel. The Petition attempts to make up for these shortcomings with conclusionary statements of its expert that are devoid of any articulated reasoning and rational underpinning. Additionally, the proposed modification would render the prior art inoperable. Consequently, the Petition fails to establish the unpatentability of claims 1-17 of the 730 Patent.

II. CLAIM CONSTRUCTION

A. 37 C.F.R. § 42.100(b) Statement

Terms appearing within the claims of the 730 Patent have been construed four 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"), P*roxense, LLC v. Google LLC*, No. 6:23-cv-00320 (W.D. Tex. May 2, 2023) ("Proxense v. Google"), *Proxense, LLC v., Microsoft Corporation*, No. 6:23-cv-00319-ADA (W.D. Tex. May 2, 2023) ("Proxense v. Microsoft"), and *Proxense, LLC v. Apple*, Inc, No. 6:24-cv-00143 (W.D. Tex. March 18, 2024). The Claim Construction Orders issued in the foregoing are provided as Exhibits 2001, 2004, and 2006, respectively. Pursuant to Rule

42.100(b), Patent Owner requests the Board consider and adopt the claim constructions previously given in the foregoing cases. 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).

B. Third-Party Trusted Authority

The Board has maintained its construction of "third-party trusted authority" as "a trusted authority that is an entity separate from the parties to a transaction." Paper 9, at 11. Patent Owner does not dispute this construction, nor has Patent Owner disputed this construction. However, the Patent Owner has consistently disputed the implicit construction of the ***transaction*** and the ***principal parties*** thereto.

The claims of the 730 Patent explicitly recite a transaction of allowing a user to access an application. *See* 730 Patent, claim 1 ("allowing the user access to an application"); claim 8 ("allowing the user access to an application"); claim 12 ("allowing the biometrically verified user access to an application"); and claim 15 ("allowing the user to access an application"). The principal parties to the transaction are the user allowed access and the application being accessed. Accordingly, Patent Owner is not now disputing, nor has in any of the numerous post-grant proceedings before the Office disputed, the construction of "third-party trusted authority." Rather, Patent Owner is merely attempting to construe the ***transaction*** and the ***principal parties*** thereto, which limit the scope of "third-party trusted authority."

Before determining whether an entity is a "third-party trusted authority" or a principal party, it is necessary to construe the transaction specified in the claims and the principal parties thereto. That is, before determining whether an active participant is a "third-party trusted authority," it is necessary to evaluate the transaction specified in the claims and the relationship of

each party specified in the claims thereto. The Board stated this issue more concisely: "we evaluate a party's relationship to the transaction to determine whether it is a principal party to the transaction or a third-party." Paper 9, at 11.

Before a party's relationship to the transaction can be evaluated, the transaction must first be identified. A transaction is an activity or a request involving two parties. *See* Ex. 2014 (Defining a transaction as "***[a]n activity or request***. Orders, purchases, payments as well as changes, additions and deletions are typical transactions… Ad hoc queries are a type of transaction as well; however, they are usually just acted upon, and the query transaction is not saved." (emphasis added)); *See also* Ex. 2015 (Defining a transaction as "***a communicative action or activity involving two parties*** or things that reciprocally affect or influence each other" (emphasis added)). The express language of the claims recites the action / activity of "allowing the user access to an application" or "allowing the biometrically verified user access to an application." Accordingly, the claims recite the transaction is allowing a user access to an application, identifying the principal parties as the user allowed access and the application being accessed. A person or organization cannot be a principal party to the transaction unless they are directly affected or influenced. Here the user is directly affected by being allowed access and the application is directly affected by being accessed. The claims, therefore, require a ***transaction*** of allowing a user access to an application, in which the ***principal parties*** are the user allowed access and the application being accessed. The "third-party trusted authority," therefore, is a third-party with respect to the user being allowed access and the application being accessed.

Furthermore, as the Board noted in other proceedings, the specification discloses an embodiment in which the "third-party trusted authority" is a third-party with respect to a

transaction having as principal parties a user being allowed access and an application being accessed.

> "[T]he trusted key authority of the preferred embodiments of the '730 patent, which actively participates in a transaction, for example by receiving a request for authentication with a code, determining whether the code is valid, authenticating the code, and transmitting an access code to the requester, which ***allows a user access to an application***. Ex. 1001, 7:10–22, Fig. 7. Although the trusted key authority in this example is not ***a principal party to the transaction (here, those parties are the user and the application)***, it is an active participant in facilitating the transaction." *Google LLC v. Proxense, LLC,* IPR2024-00232, Paper 10, at 11.

"Although reluctant to exclude an embodiment, this [Board] must not allow the disclosed embodiment to 'outweigh the language of the claim." *Rolls-Royce, PLC v. United Technologies Corp.*, 603 F. 3d 1325, 1334 (Fed. Cir. 2010). *See also TIP SYSTEMS, LLC v. Phillips & Brooks/Gladwin,* 529 F. 3d 1364, 1373 (Fed. Cir. 2008) ("However, to construe the claim term to encompass the alternative embodiment in this case would contradict the language of the claims… Our precedent is replete with examples of subject matter that is included in the specification, but is not claimed."); and *Schoenhaus v. Genesco, Inc.*, 440 F. 3d 1354, 1359 (Fed. Cir. 2006) ("[W]here a patent specification includes a description lacking a feature, but the claim recites that feature, the language of the claim controls."). As such, when the claim language is limited to certain embodiments of "third-party trusted authority," the language of the claims controls, not the embodiments disclosed in the specification.

As characterized by the Board, one possible embodiment of a "third-party trusted authority" is a third-party with respect to a user being allowed access and an application being accessed. Independent claims 1, 8, 12, and 15 of the 730 Patent each explicitly recites a user and an application, and no other party aside from a "third-party trusted authority." Furthermore, each

of the independent claims explicitly recites the underlying action of allowing the user access to the application. Accordingly, all of the independent claims of the 730 Patent explicitly recite the elements of the embodiment in which the "third-party trusted authority" is a third-party with respect to a user being allowed access and an application being accessed. Thus, to construe "third-party trusted authority" to include anything but a third-party to a transaction in which the principal parties are a user being allowed access and an application being accessed (i.e., where the underlying transaction is the user being allowed access to the application), would be to allow potentially disclosed alternative embodiments to "outweigh the language of the claim[s]" as to "contradict the language of the claim[s]." "Third-party trusted authority," therefore, cannot be construed to encompass third parties to transactions other than those in which the principal parties are a user being allowed access and an application being accessed, and the underlying transaction is allowing a user access to an application.

Petitioner's grounds for invalidity, however, advances unreasonably broad constructions contradicting the express language of the claims. Included within the Petitioner's asserted grounds for invalidity are instances in which the "third-party trusted authority" is a third-party with respect to an advertiser and a user and a hotel and a user, merely because at some point during the transaction the user access an application. The scope of "third-party trusted authority" cannot be expanded to include instances of a third-party with respect to other transactions that occur after the user has already been allowed access to an application.

The expansion of claim scope proposed by petitioner, as outlined above, was rejected in *In re Suitco Surface, Inc.,* 603 F.3d 1255 (Fed. Cir. 2010). There, the patent at issue included claims defining an element ("material") by the action it performed ("finishing the top surface of the floor"). *Id,* at 1260. That court rejected a construction of "material" that did not require the material

to perform the action of "finishing." *Id, at* 1260 ("A material cannot be finishing any surface unless it is the final layer on that surface. Otherwise, the material would not be "finishing" the surface in any meaningful sense of the word.").

Petitioner's actions here demand the same result. The present claims are limited by the recital of a "third-party trusted authority" that is a third-party with respect to a transaction defined by the actions performed by the principal parties ("allowing the user access to an application" / "allowing the biometrically verified user access to an application"). Petitioner is thereby violating the principle set forth in *In re Suitco* by asserting an overly broad construction of "third-party trusted authority" such that it is a third-party with respect to ***any*** transaction in which a user at some point accesses an application. In so doing, Petitioner asks the Board to construe "third-party trusted authority" so broadly as to include instances in which it is a third-party with respect to any transactions, including those where the principal parties do not engage in the activity of allowing the user access to an application, which is a claim requirement. Such a construction is impermissible ***even*** under a broadest-reasonable standard. "The broadest-construction rubric coupled with the term 'comprising' does not give the PTO an unfettered license to interpret claims to embrace anything remotely related to the claimed invention." *In re Suitco,* at 1260.

Here, as in *In re Suitco,* the claims require a specific action to be performed (i.e., "allowing the user access to an application" / "allowing the biometrically verified user access to an application"). The "third-party trusted authority," therefore, is limited to instances in which it is a third-party with respect to principal parties engaged in the activity of allowing the user access to the application – just as how the "material" at issue in *In re Suitco* was limited to those performing the action of "*finishing* the *top* surface of the floor." Thus, just because a user may complete a transaction with a hotel or advertiser after accessing an application does not make any other party

a "third-party trusted authority" per the claims. Rather, the "third-party trusted authority" is limited to being a third-party with respect to the parties directly engaged in the transaction specified in the claims – that is the user allowed access to the application and the application being accessed. Even under the broadest reasonable interpretation standard, therefore, the "third-party trusted authority" is limited to a third-party with respect to a user allowed access to an application and the application being accessed.

III. RESPONSE TO GROUNDS FOR INVALIDITY RAISED

A. [GROUND 1] – Claims 1, 2, 4-9. 11, 12, and 14-17 Are Not Rendered Obvious by Burger

The Petition asserts three examples of how Burger (U.S. Publication No. 2005/0050367) supposedly renders obvious claims 1, 2, 4-9, 11, 12, and 14-17 of the 730 Patent. The first relies on conclusory statements, devoid of any articulated reasoning and rational underpinning, which propose an inoperable modification. The second goes well beyond any reasonable interpretation by conflating separately recited elements of the claims. The third also exceeds any reasonable interpretation of the claims by rendering claim limitations meaningless.

1. Petitioner's First Example is Inoperable

The first example asserted in the Petition relies on conclusory statements devoid of any articulated reasoning and rational underpinning. Additionally, the proposed modification would render the prior art inoperable. Consequently, the first example fails to establish the unpatentability of claims 1, 2, 4-9. 11, 12, and 14-17 of the 730 Patent.

Independent claims 1, 8, 12, and 15, from which claims 2, 4-7, 9, 11, 12, and 14-17 depend, each require receiving an access message allowing the user access to an application responsive to authentication of one or more codes by a third-party trusted authority. Petitioner does not assert that Burger teaches this sequence of steps. Rather, Petitioner asserts it would have been obvious

to receive an access message so that the Pocket Vault grants access to a user and displays sensitive information (e.g., credit or debit card info) for conducting a transaction. Paper 2, 50–55 (citing Ex. 1005 ¶¶ 103, 155 158, 182–186, 320, 517–527, Figs. 7B, 10A, 19, 24, 25; Ex. 1003 ¶¶ 109 110, 112). Neither the Petition nor Dr. Traynor offer anything more than a conclusory statement devoid of any articulated reasoning and rational underpinning. But "rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006). Such, however, cannot be provided because the proposed modification would break the prior art system and render the it inoperable.

In making the above conclusory assertion, Petitioner acknowledges the teachings of Burger are related to processing debit and credit card transactions, such that the sensitive information is a credit or debit card used to complete the transaction. The Petition further equates the claimed "access message" with an "approval message" discussed in Burger.

> "As noted above, the controller 402 of the network server 114 also transmits an encrypted approval message in operation 2408 after the Pocket Vault 102 is authorized by confirming that the Pocket Vault ID is valid (step 2006 in FIG. 24 (reproduced below); step 2506 in FIG. 25 (reproduced below))… Because this encrypted approval message ('***access message***') is received by the Pocket Vault 102 in response to the Pocket Vault ID being successfully authenticated by the network server 114, Burger also discloses '***responsive to authentication of the one or more codes and the other data values by the agent, receiving an access message from the agent allowing the user access to an application***' in this additional way." Paper 2, at 52 (emphasis in original).

Burger is unquestionably using the term "approval" with respect to the processing of credit and debit card transactions. For instance, Burger states:

> "Generally, a retailer does not need to see ***a credit or debit account number***, while the ***approving entity contacted on the dialup modem does***. Today, credit and debit cards have this information embossed on the card and recorded in the magnetic Stripe on the back of the card. If the magnetically encoded information is unreadable due to mechanical wear of the magnetic stripe or for other reasons, the embossed image can always be read by the clerk and manually keyed in." Burger, ¶ [0320] (emphasis added).

In the above passage, Burger is clearly stating that an approving entity is receiving credit card or debit card information, and the receipt of such information is necessary for the approval. Accordingly, if the information cannot be read from the card it must be keyed in by the clerk. These are readily recognized as the common steps of using a credit card or a debit card to make a purchase.

Additionally, Burger makes clear that the token may be processed through conventional commercial card readers. The token, therefore, is nothing more than a credit card or debit card account identifier.

> "[T]he routine 1900 proceeds to a step 1920, wherein it is determined whether any requests have been made to ***authorize transactions***. Such a request may be made, for example, by ***a merchant*** operating a commercial interface station 104c. In this regard, it should be appreciated that, when a token 102a is employed to engage in a transaction with a commercial card reader 106 or a commercial bar code reader 107, a request for ***transaction approval*** may not be made to the network server 114. Instead, such a ***transaction approval*** request may be made through conventional, existing communication and approval channels for such devices." Burger, ¶ [0473] (emphasis added).

However, being a replacement for conventional credit and debit cards, the token is utilized to "authorize" a transaction with a merchant by submitting a request for an "approval." This is apparent when one considers the entirety of the flow detailed by Burger. Petitioner cites a portion

of the flow "an encrypted approval message in operation 2408" as alleged evidence of the disclosure of an "access message." Paper 2, at 52. Operation 2408 is part of a routine implemented after step 1920, of the above passage.

> "When, ***at the step 1920***, it is determined that a request to authorize a transaction has been made, routine 1900 ***proceeds to a step 1922***, wherein the request to authorize the transaction is processed. An example of a routine that may be employed to implement ***the step 1922 is discussed in more detail below in connection with FIG. 24***." Burger, ¶ [0474] (emphasis added).

> "***FIG. 24*** is a flow diagram illustrating an example of a routine that may be employed ***to implement the step 1922*** of the primary routine 1900 (FIG. 19)." Burger, ¶ [0511] (emphasis added).

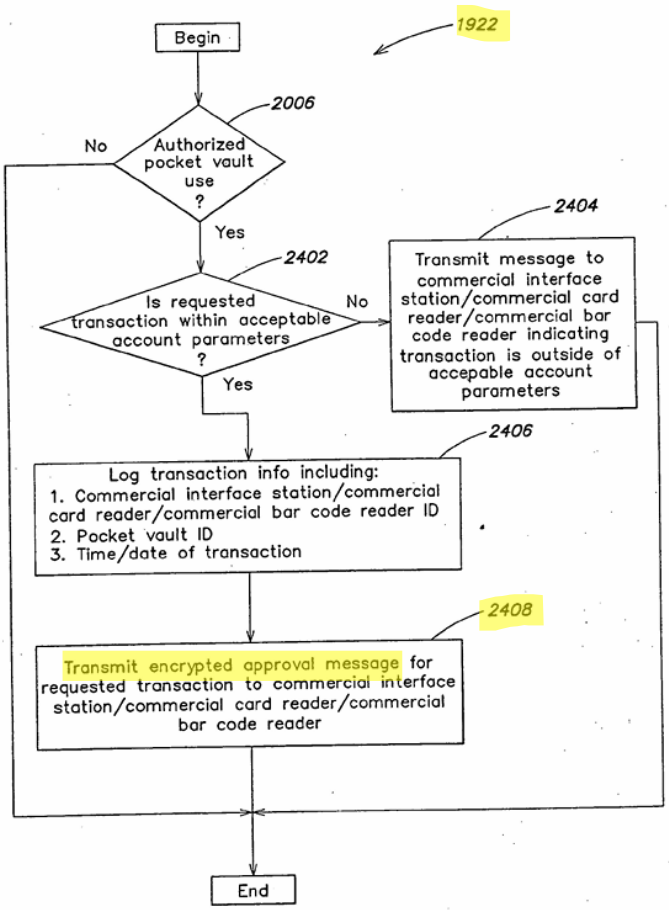

FIG. 24

Accordingly, what the Petitioner identifies as the "access message" is actually merely an ***approval*** obtained during ***authorization*** of a credit or debit card transaction.

The terms "approval" and "authorization" have an accepted meaning with respect to credit / debit card transactions. "Authorization" is one of two stages in payment processing. "Approvals" are the result of the "authorization" process and indicate that funds have been secured to pay the vendor for a specific transaction from a designated account. If the approval was received prior to the release of the credit card or debit card information, as Petitioner suggests, funds would be secured without any knowledge of the account from which they are to be drawn or even the ability of the account to provide sufficient funds.

With respect to processing online payments, Stripe and PayPal are two of the biggest players.

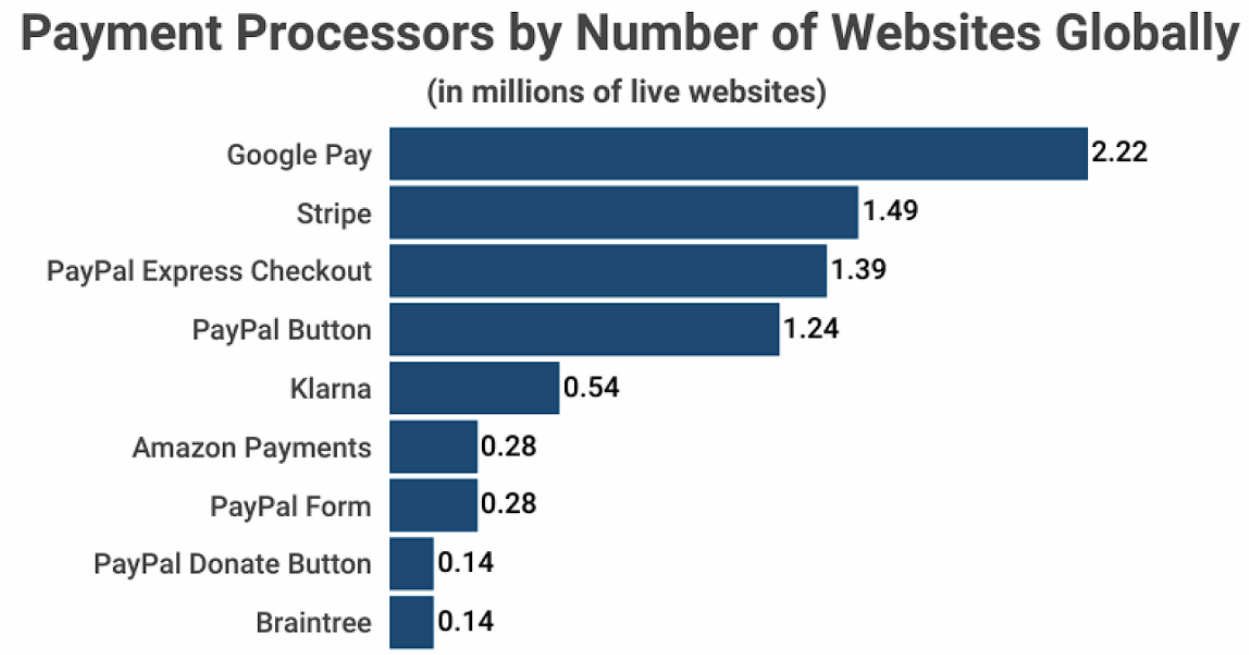

Exhibit 2009.

According to PayPal, "[t]here are two stages to online payment processing: ***authorization*** (***approving the sale***) and settlement (getting the money in your account)." Ex. 2010 (emphasis

added). Similarly, Stripe states that "[c]redit card processing occurs when electronic transactions involving credit cards are ***authorised***, authenticated and settled between the cardholder, the business and their respective financial institutions." Ex. 2011. The agreement between PayPal and Stripe indicates that "approval" and "authorization" are terms of art used to reference various phases of processing credit and debit card transactions.

There is also agreement as to the meaning of the terms "authorization" and "approval," thereby demonstrating the terms have an accepted meaning within the relevant art. PayPal simply defines "authorization" as "approving the sale." Ex. 2010. PayPal explains that during "card ***authorization***" a "payment processor sends a request to the customer's issuing bank to check to see if they have enough credit to pay for the item," and the "issuer responds with a yes (an ***approval***) or a no (a denial)." Ex. 2010 (emphasis added). Accordingly, "authorization" is the process of obtaining an "approval," which is a message issued by a bank indicating an account has sufficient funds to pay for a transaction. But, without knowledge of the account, the bank could not issue such a message. Consequently, the system would be rendered inoperable if the "approval" was received prior to the release of the account information, as Petitioner proposes. PayPal further details how a vendor should respond to an authorization: "Once the payment is authorized, the customer receives confirmation that the purchase is complete. You'll also get a notification so you can start processing the order." Ex. 2012. Thus, an "approval" is treated as payment from an account. If the "approval" were received, as Petitioner suggests, before the credit / debit card information were released, there would be no account from which to draw the payment at that time.

PayPal defines "settlement" as the "second piece of the online payment system process (where you get paid)." Ex. 2010. During the settlement process, "[t]he card issuer sends the funds

to your merchant bank, which deposits the money into your account." Ex. 2010. The settlement process is not instantaneous and often occurs days after the receipt of the approval. "Although the settlement process can sometimes take a few days, certain banks might allow you to access your funds even before they are officially transferred." Ex. 2010. Regardless of its duration, "settlement" is defined by PayPal to be a transfer of funds following issuance of an "approval." But, if the "approval" were received, as Petitioner suggests, before the credit / debit card information were released, there would be no account from which to transfer the funds into the merchant's account. Consequently, the merchant would not get paid and the whole system would break.

Stripe defines "authorization," "approval," and "settlement" consistent with PayPal. Stripe defines "***authorization***" as "***approval*** from a credit or debit card issuer (usually a bank or credit union) that states the cardholder has sufficient funds or the available credit needed to cover the cost of a transaction they're using a card to complete." Ex. 2013 (emphasis added). As with PayPal, Stripe states the authorization should be accepted as payment completing a purchase. "If the transaction is ***approved***, the business can complete the sale and provide the goods or services to the customer." Ex. 2011 (emphasis added). Accordingly, as with PayPal, Stripe recognizes that an authorization completes a purchase and a vendor should respond by providing the goods or services, and is thus a payment accepted by the vendor, though settlement has not yet occurred. Petitioner's proposed modification of receiving the approval prior to release of the account information, however, would be asking a bank to guarantee an account has sufficient funds without knowledge of the account – which is impossible.

Stripe defines "settlement" as "when the funds actually move from the issuing account to the business account." Ex.2013. During the funds transfer, "card networks coordinate with the

issuing banks to transfer the funds for each transaction to the acquiring bank, which receives the funds in the merchant account." Ex. 2011. As with PayPal, Stripe acknowledges settlement can take some time to complete, stating that the "entire process usually takes one to three working days." Ex. 2011. Regardless of its duration, "settlement" is defined by both Stripe and PayPal to be a transfer of funds following issuance of an "approval." Again, if the "approval" were received, as Petitioner suggests, before the credit / debit card information were released, there would be no account from which to transfer the funds into the merchant's account.

Consistent with the accepted meaning of "authorization" as the process in which a request is sent to an issuing "bank to check to see if they have enough credit to pay for the item" (Ex. 2010) such that the resulting "approval" indicates "the cardholder has sufficient funds or the available credit needed to cover the cost of a transaction" (Ex. 2013), Burger teaches that ***prior to*** transmission of the "encrypted approval message" at step 2408, it is first determined if the transaction is within acceptable parameters set by the issuing bank.

> "[T]he ***routine 1922*** proceeds to a step 2402, wherein it is determined whether the requested transaction is within ***acceptable account parameters (e.g., as set by the media issuer).***" Burger, ¶ [0514] (emphasis added).
>
> "When, at the step 2402, it is determined that the requested transaction is within acceptable account parameters, information regarding the transaction is logged into the database 406 of the network server 114 (FIG. 4)." Burger, ¶ [0517].
>
> "After the step 2406, ***the routine 1922 proceeds to a step 2408***, wherein an ***encrypted approval message is transmitted*** to the entity with which the transaction is being attempted (e.g., a commercial interface Station 104C, a card reader 106, or a barcode reader 107)." ¶ [0518] (emphasis added).

However, if the "approval message" was issued prior to the release of the financial media (i.e., token or credit / debit card number) it would be impossible to determine if the transaction is

within "acceptable account parameters" because the applicable account parameters could not be identified absent knowledge of the account. Burger, itself, even acknowledges the necessity of providing the debit / credit card information to obtain an approval when it states that "[g]enerally, a retailer does not need to see ***a credit or debit account number***, while the ***approving entity contacted on the dialup modem does***." Burger, ¶ [0320] (emphasis added). Consequently, as explicitly acknowledged by Burger, the whole system would break if the approval were obtained prior to the release of the credit or debit card information as Petitioner suggests. It is axiomatic that obviousness cannot be based on a proposed modification that would render the prior art inoperable. *In re Gordon,* 733 F.2d 900 (Fed. Cir. 1984). Accordingly, Petitioner's first example fails to demonstrate the unpatentability of claims 1, 2, 4-9. 11, 12, and 14-17.

2. Petitioner's Second Example Contradicts the Express Language of the Claims

Attempting to escape the broken system of its first example, the Petitioner asserts an example in which an advertiser is a purported principal party to the transaction. Paper 2, at 43–44, 46–49 (citing Ex. 1005 ¶¶ 38, 110, 117, 147, 236–238, 541, Figs. 1, 10; Ex. 1003 ¶¶ 106 108). This example is contradictory to the language of the claims.

As an initial matter, each of the independent claims recites a specific transaction (allowing the user access to an application) in which the principal parties are the user being allowed access and the application being accessed. As the Board acknowledges, "we evaluate a party's relationship to the transaction to determine whether it is a principal party to the transaction or a third-party." Paper 9, at 11. Accordingly, a "third-party trusted authority" is a third party with respect to the user being allowed access and the application being accessed. Petitioner, however, disregards the specific transaction recited in the claims as to make the

"third-party trusted authority" a third party with respect to any user accessing an application and any other party with whom the user is transacting.

Petitioner asserts an advertiser is a principal party to the transaction of a user "obtaining advertisement content or related information" from "a party/company operating the network server 114." Paper 2, at 43-44. Thus, Petitioner's second example is based upon "a transaction between a Pocket Vault holder/user and an entity such as the advertiser 108." Paper 2, at 46. But this is not the transaction recited in the claims.

Claims 1, 8, 12, and 15 define the transaction, consistent with an embodiment disclosed in the specification, as either "allowing the user access to an application" or "allowing the biometrically verified user access to an application." To construe the claims, as Petitioner contends, such that the "third-party trusted authority" is a third party with respect to an advertiser would read out from the claims the recited transaction of allowing the user access to the application. Such a construction would be contrary to the well-established "principle that claim language should not be treated as meaningless." *HZNP Medicines LLC v. Actavis Laboratories UT*, 940 F. 3d 680, 692 (Fed. Cir. 2019). Furthermore, Petitioner's characterization of the transaction exceeds even the broadest reasonable interpretation by extending the claims to embrace any transaction that occurs before or after a user happens to access an application. *In re Suitco,* at 1260 ("The broadest-construction rubric coupled with the term 'comprising' does not give the PTO an unfettered license to interpret claims to embrace anything remotely related to the claimed invention."). Consequently, Petitioner's second example fails to demonstrate the unpatentability of claims 1, 2, 4-9. 11, 12, and 14-17.

Even if claims 1, 8, 12, and 15 could be construed such that the "third-party trusted authority" is a third party with respect to a transaction between a user and an advertiser (which

Patent Owner does not concede), Petitioner's second example would still be unreasonably broad by equating two separately identified elements (i.e., the third-party trusted authority and the application). *Microsoft Corp. v. Proxyconn, Inc.*, 789 F.3d 1292, 1299 (Fed. Cir. 2015) ("The Board's construction, which expands the 'two other computers 42 and 46' to include the separately identified caching computer, is unreasonably broad in light of the language of the claims and specification.").

Each of independent claims 1, 8, 12, and 15 recite a third-party trusted authority and an application as distinct and separate elements. Furthermore, claims 1, 8, 12, and 15 each define the application via a Markush group "consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file."

The second example proposed by Petitioner would render meaningless the separate recitation of the application and third-party trusted authority by equating the two. As the Board correctly recognized, in the second example of Burger, "network server 114 may serve as a conduit for advertisers to target particular classes of Pocket Vault holders, and channel information to them." Paper 9, at 25. This is clearly shown in Figure 1 of Burger (reproduced below) and its description of the network server 114.

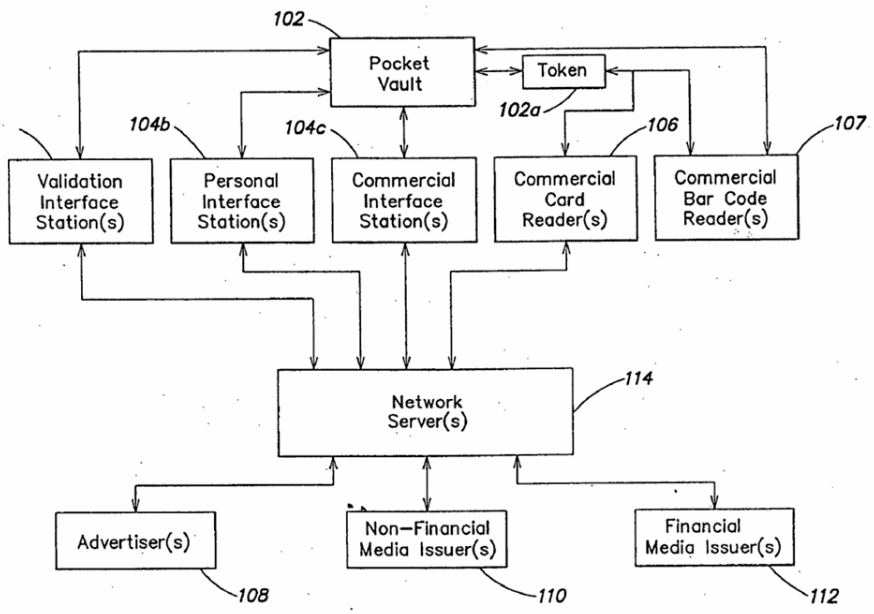

FIG. 1

"As shown in FIG. 1, ***the network server 114 may form the hub of the network system 100***" and "may therefore serve as: (1) ***a repository of information for the network***, (2) the entity that controls access to the stored information by the other network devices, and (3) ***a service provider for*** financial and non-financial media issuers, ***advertisers***, as well as Pocket Vault holders." Burger, ¶ [0098].

"The respective media stored on the Pocket Vault 102 may be issued by different and unrelated media issuers." Burger, ¶ [0104].

[T]he computers 108, 110, and 112, together with the ***network server 114***, may represent a secure infrastructure of ***server databases capable of storing information for purposes of delivering personalized services to holders of Pocket Vaults 102***." Burger, ¶ [0111] (emphasis added).

The information stored within the database of the network server 114 may include advertisements.

"[T]he network server 114 may also serve as ***a repository for information regarding*** media issuers or ***advertisers***." Burger, ¶ [0117] (emphasis added).

> "Additionally, the network server 114 may serve as a conduit for advertisers to target particular classes of Pocket Vault holders, and ***channel information to them***." Burger, ¶ [0117].

Network server 114, therefore, acts as a conduit for advertisers by storing ads and delivering them to Pocket Vaults, such that advertisements would be received by the Pocket Vault from the network server 114. The conduit activity of the network server, accordingly, is accomplished by the network server 114 operating as a shared ***hard drive*** or some form of file sharing ***software*** upon which advertisements can be placed by advertisers and retrieved later by Pocket Vaults.

Moreover, advertisers contract with the operator of network server 114 to have their ads delivered. "The advertiser 108 (FIG. 1) may, for example, have ***made arrangements*** with the company operating the ***network server 114*** to have certain advertising ***information uploaded to Pocket Vaults 102*** when particular Pocket Vault holders interface their Pocket Vaults 102 with their personal interface stations 104b." Burger, ¶ [0237] (emphasis added). Making arrangements with the company operating the network server 114 would require the advertiser uploading the advertisement to the network server 114 consistent with its role of a data store. Burger, ¶ [0098] ("As shown in FIG. 1, the network server 114 may form the hub of the network system 100… As discussed in more detail below, the network server 114 may therefore serve as: (1) a repository of information for the network, (2) the entity that controls access to the stored information by the other network devices, and (3) a service provider for financial and non-financial media issuers, advertisers, as well as Pocket Vault holders."); and ¶ [0538] ("In one embodiment, the network server 114 stores both data and applications that are accessible to users. The network server 114 may, for example, store and serve a website, i.e., a collection of web pages and data that are available to users via a browser."). As the advertiser places information within the network server

114 that is later accessed by the user, the network server 114 must be providing file sharing ***software*** or acting as a shared ***hard drive*** that user accesses to receive the advertisement. Both software and a hard drive are applications per the Markush groups of claims 1, 8, 12, and 15. Consequently, the network server 114 is the application being accessed per the express language of claims 1, 8, 12, and 15 in Petitioner's second example.

Claims 1, 8, 12, and 15, however, recite the application and third-party trusted authority as distinct elements. Consequently, permitting network server 114 to be both the application and the third-party trusted authority, as Petitioner proposes, would render meaningless the recitation of the third-party trusted authority and the application being accessed as distinct elements, and thus would be contrary to the well-established "principle that claim language should not be treated as meaningless." *HZNP Medicines LLC v. Actavis Laboratories UT*, 940 F. 3d 680, 692 (Fed. Cir. 2019). Furthermore, it would result in an unreasonably broad interpretation by equating two separately identified elements (i.e., the third-party trusted authority and the application). *Microsoft Corp. v. Proxyconn, Inc.*, 789 F.3d 1292, 1299 (Fed. Cir. 2015) ("The Board's construction, which expands the 'two other computers 42 and 46' to include the separately identified caching computer, is unreasonably broad in light of the language of the claims and specification."). Consequently, this provides a second independent reason why Petitioner's second example fails to demonstrate the unpatentability of claims 1, 2, 4-9. 11, 12, and 14-17.

3. Petitioner's Third Example Contradicts the Language of the Claims

Petitioner's third example similarly ignores limitations expressly stated and elements separately identified in the claims.

Petitioner's third example is a user downloading a hotel room key to their pocket vault 102 and using their pocket vault 102 to unlock a hotel room, such that the application being accessed is the keyless lock of the hotel room. Paper 2, at 59 (citing Ex. 1005 ¶¶ 94, 102, 128–129, 679–

680). The Board has observed that within this example, the user downloads the key card onto their pocket vault 102 from the hotel's website. Paper 9, at 27.

But this renders Petitioner's third example inconsistent with the express language of claims 1, 8, 12, and 15. If the application that is being accessed is the keyless lock, then the hotel room key would be the access message. Independent claims 1, 8, 12, and 15 recite that the access message is received from the third-party trusted authority. 730 Patent, claim 1 ("receiving an access message ***from the agent***"); claim 8 ("receives an access message ***from the agent***"); claim 12 ("receiving an access message ***from the agent***"); and claim 15 ("receiving an access message ***from the agent***") (emphasis added). In Petitioner's third example of a hotel room key, however, the hotel room key is supposedly received (i.e. downloaded) from the hotel's website and activated by the network server 114. As the hotel key is not received from network server 114 acting as a third-party trusted authority, it cannot be equated to an access message without rendering the claim language requiring receipt of the access message ***from the third-party trusted authority*** meaningless. Accordingly equating a hotel room key downloaded from a hotel's website to an access message is contrary to the well-established "principle that claim language should not be treated as meaningless." *HZNP Medicines LLC v. Actavis Laboratories UT*, 940 F. 3d 680, 692 (Fed. Cir. 2019). Consequently, Petitioner's third example fails to demonstrate the unpatentability of claims 1, 2, 4-9. 11, 12, and 14-17.

Claims 1, 8, 12, and 15 define the transaction, consistent with an embodiment disclosed in the specification, as either "allowing the user access to an application" or "allowing the biometrically verified user access to an application." To construe the claims, as Petitioner contends, such that a hotel is a principal party would read out from the claims the recited transaction, which allows the user access to the application, and thus would be contrary to the well-established

"principle that claim language should not be treated as meaningless." *HZNP Medicines LLC v. Actavis Laboratories UT*, 940 F.3d 680, 692 (Fed. Cir. 2019). Furthermore, Petitioner's characterization of the transaction exceeds even the broadest reasonable interpretation by extending the claims to embrace any transaction before or after which a user may also access an application. *In re Suitco,* at 1260 ("The broadest-construction rubric coupled with the term 'comprising' does not give the PTO an unfettered license to interpret claims to embrace anything remotely related to the claimed invention."). Consequently, Petitioner's third example fails to demonstrate the unpatentability of claims 1, 2, 4-9. 11, 12, and 14-17.

B. [GROUND 2] – Claims 3, 10, and 13 Are not Rendered Obvious by Burger and Robinson

The Petition does not assert Robinson (U.S. Publication No. 2003/0177102) discloses the "third-party trusted authority" that is a third-party with respect to a user allowed access to an application and the application being accessed. Nor does Petitioner assert Robinson discloses an "access message." As noted supra, Burger fails to disclose these elements. Thus, the Petition fails to establish that Burger in combination with Robinson discloses all the elements of claims 1, 8, and 12 upon which claims 3, 10, and 13, respectively, depend. Accordingly, because all the elements of the independent claims are not met, the Petition fails to establish that Burger in COMBINATION WITH ROBINSON INVALIDATES DEPENDENT CLAIMS 3, 10 AND 13.

IV. CONCLUSION

The Petition fails to demonstrate Burger alone or in combination with Robinson renders claims 1-17 of the 730 Patent obvious. The Petition thus fails to demonstrate the challenged claims invalid and unpatentable.

Dated: February 10, 2025

Respectfully submitted by,

/s/David L. Hecht
David L. Hecht (Lead Counsel)
(Reg. No. 61,618)
dhecht@hechtpartners.com
HECHT PARTNERS LLP
125 Park Avenue, 25th Floor
New York, NY 10017
P: (212) 851-6821

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 Proxense, LLC's Patent Owner Response was served on Petitioner by e-mailing copies to the following e-mail addresses as provided in Petitioner's Petition:

W. Karl Renner
Roberto Devoto
Usman Khan
FISH & RICHARDSON P.C.
axf-ptab@fr.com
devoto@fr.com
khan@fr.com

Dated: February 10, 2025

Respectfully submitted by,

/s/David L. Hecht
David L. Hecht (Lead Counsel)
(Reg. No. 61,618)
dhecht@hechtpartners.com
HECHT PARTNERS LLP
125 Park Avenue, 25th Floor
New York, NY 10017
P: (212) 851-6821

CERTIFICATE OF WORD COUNT (37 C.F.R. § 42.24(d))

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, certificate of word count, or listing of exhibits) total 6,493 words, which is less than the 14,000 words allowed under 37 C.F.R. § 42.24(b)(2).

Dated: February 10, 2025

Respectfully submitted by,

/s/David L. Hecht
David L. Hecht (Lead Counsel)
(Reg. No. 61,618)
dhecht@hechtpartners.com
HECHT PARTNERS LLP
125 Park Avenue, 25th Floor
New York, NY 10017
P: (212) 851-6821