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

PROXENSE, LLC'S PRELIMINARY RESPONSE TO PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 8,352,730

TABLE OF CONTENTS

I. INTRODUCTION 1
II. CLAIM CONSTRUCTION 1
A. 37 C.F.R. § 42.100(B) STATEMENT 1
B. PREVIOUSLY CONSTRUED TERMS 2
1. Access Message 2
III. THIRD-PARTY TRUSTED AUTHORITY 7
IV. RESPONSE TO GROUNDS FOR INVALIDITY RAISED 8
A. [GROUND 1] – CLAIMS 1, 2, 4-9. 11, 12, AND 14-17 ARE NOT RENDERED OBVIOUS BY BURGER 8
B. [GROUND 2] – CLAIMS 3, 10, AND 13 ARE NOT RENDERED OBVIOUS BY BURGER AND ROBINSON 26
V. CONCLUSION 26

EXHIBIT LIST

No.	Exhibit Description
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
2005	Opening Claim Construction Brief in *Proxense v. Microsoft Corporation,* No. 6:23-cv-00319-ADA
2006	Claim Construction Order in *Proxense v., Microsoft Corp.,,* No. 6:23-cv-00320-ADA
2007	Miriam Webster Definition of Access availiable at https://www.merriam-webster.com/dictionary/access
2008	Chase Article on Credit Card Processing availiable at https://www.chase.com/personal/credit-cards/education/basics/credit-card-processing

I. INTRODUCTION

Pursuant to 35 U.S.C. § 313 and 37 C.F.R. § 42.107, Patent Owner Proxense LLC ("Proxense") submits the following Preliminary 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 patent at issue is currently being asserted against Petitioner in *Proxense v. Microsoft Corporation,* No. 6:23-cv-00319-ADA (W.D. Tex. May 2, 2023) ("*Proxense v. Microsoft*"). Petitioner and Patent Owner have exchanged Markman briefs, and the Court has issued a Claim Construction Order (Exhibit 2006). Pursuant to Rule 42.100(b), Patent Owner requests the Board consider and adopt the District Court's construction. The same District Court and PTAB has construed the challenged claims contrary to the specific grounds asserted in the Petition. Accordingly, it is unlikely that Petitioner could credibly pursue the specific grounds asserted in the Petition. *Inter partes* review, consequently, should not be instituted.

II. CLAIM CONSTRUCTION

A. 37 C.F.R. § 42.100(b) Statement

Terms appearing within the claims of the 042 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*, 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 2006, respectively.

B. Previously Construed Terms

Pursuant to Rule 42.100(b), Patent Owner requests the Board to consider and adopt the relevant constructions previously given for 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).

1. Access Message

The Board declined to adopt the District Court's construction of "access message" in favor of the plain and ordinary meaning. *See Google, LLC v. Proxense, LLC*, IPR2023-00232, Paper 10 at 12 (PTAB Jul. 24, 2024);. However , the plain and ordinary meaning of "access message" improperly excludes an embodiment disclosed in the specification. "We normally do not interpret claim terms in a way that excludes embodiments disclosed in the specification." *Oatey Co. v. IPS CORP.*, 514 F. 3d 1271, 1276 (Fed.Cir. 2008). Accordingly, Patent Owner respectfully requests the Board reconsider its construction in *Google, LLC v. Proxense, LLC*, IPR2023-00232, Paper 10 (PTAB Jul. 24, 2024)

The plain and ordinary meaning of "access message" is a message enabling entry to, communication with, or use of an object. When used as a noun, "access" means:

"**a:** permission, liberty, or ability to enter, approach, or pass to and from ***a place*** or to approach or ***communicate with a person or thing***

Investigators wanted to get *access* to his home.

consultants who have easy *access* to the president

b: freedom or ability to ***obtain or make use of something***

paying for *access* to the Internet

c: a way or means of entering or approaching

A canal provides *access* to ***the river***.

a building that provides wheelchair *access* [=a way for people in wheelchairs to enter]

d: the act or an instance of ***accessing something***".

Exhibit 2007.

When used as verb, per the definition (d) above, "access" means:

"to get at **:** to gain access to: such as

a: to be able to ***use, enter***, or get near (***something***)

accessed the computer by phone

a system that makes it easier to *access* the money in your bank account

b: to open or load (***a computer file, an Internet site, etc***.)

a file that can be *accessed* by many users at the same time"

Id. (emphasis added).

Common to all the above definitions is that something is made available. Per definitions (a) and (c) (as a noun), the something made available is a place, e.g., a building, so that entry is permitted. Additionally, per definitions (a), (b), and (d), a thing is made available to use, enter, or communicate with. Also, per definition (a), a person is made is made available to communicate with. People, places, and things are objects. Accordingly, the plain and ordinary meaning of "access" is to enable entry to, communication with, or use of an object. Therefore, the plain and ordinary meaning of "access message" is a message enabling entry to, communication with, or use of an object.

Petitioner has acknowledged the relevant object to which access is granted is an application. Consistent with the definitions (a), (b), and (d) above, Petitioner asserted before the District Court that an "access message" means "a message enabling access", where the object was an application. In support of their arguments before the District Court, Petitioner noted, "Moreover, although not in the context of 'access message' specifically, the specification describes sending a 'message to the ***application 330***, or otherwise allowing access to the ***application***' that is 'responsive to a successful authentication by trusted key authority 320." Exhibit 2005 at 5 (citing 730 Patent at 5:23–26; 954 Patent at 6:15–17; 905 Patent at 6:17–19). Additionally, Petitioner offered FIG. 7 (reproduced below as annotated by Petitioner) of the 730 Patent as evidence of "the only depiction of 'access message' in the figures". Exhibit 2005 at 5. As can be seen, Petitioner specifically highlighted and drew attention to box 740 "Send Access Message To The Application." By calling out Box 740 of FIG. 7 as the "the only depiction of 'access message' in the figures" and noting that specification specifically describes sending the message to the application, Petitioner clearly acknowledge and argued that the object to which entry to, communication with, or use of was made available is an ***application***.

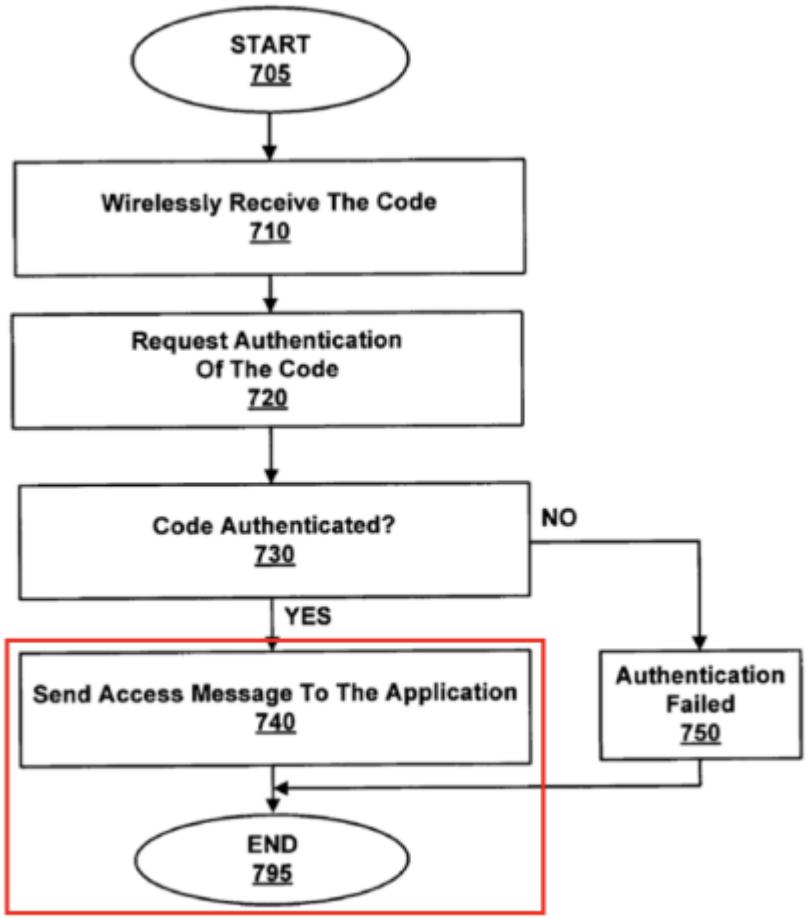


FIG. 7

Petitioner's argument before the District Court acknowledged that the object accessed is an application. As noted above, the plain and ordinary meaning of "access message" is a message enabling entry to, communication with, or use of an object. The claims explicitly recite the object accessed is an application. 730 Patent, Claim 1 ("receiving an access message from the agent allowing the user ***access to an application***"); Claim 8 ("receives an access message from the agent allowing the user ***access to an application***"); Claim 12 ("in response to a positive access message, allowing the biometrically verified user ***access to an application***"); and Claim 15 ("receiving an access message from the agent allowing the user to ***access an application***") (emphasis added). "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). As the claims explicitly recite the access message allows access to an application, it would be improper to construe "access message" as other than enabling the user to enter, communicate with, or make use of an application.

Though claims explicitly require "allowing the user to access an application" responsive to the receipt of an access message, the claims do not specify how. That, rather, is detailed in the Specification, which presents two embodiments for how the user is allowed "to complete a financial transaction." "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)." 730 Patent; 7:18-21(emphasis added). In the first embodiment, the access message allows the user access to an application itself, such that nothing further is required for the user to access the application. The second is by the user providing additional information to the application upon receipt of the access message. Providing additional information to the application necessary requires the user obtaining access to the application enabling the user to communicate with the application and provide the additional information. In the second embodiment, therefore, access to the application requires that the application receives both the access message permitting access to communicate and the additional information provided by the user to the application. To know when to provide the information, the user would have to receive some sort of signal or notification. Accordingly, with regards to accessing slot machine, the specification details:

> "For example, a user can be standing proximate to a slot machine in a casino which requires that a user be over the age of 21. The slot machine can detect the biometric key in the user's pocket, and, in response, ***spawn a conspicuous pop-up window on the slot machine requesting age verification***. Alternatively, the biometric key can

blink an LED. In other embodiments, biometric verification is not necessary and ***only the key itself is authenticated***."

730 Patent; 6:4-11 (emphasis added). The above excerpt explicitly discloses embodiments of receiving a signal or notification, such as a conspicuous pop-up window or blinking LED, alerting access to an application – i.e., casino machine. Generally, the claims should not be interpreted to exclude embodiments in the specification. *See Oatey Co. v. IPS CORP.*, 514 F. 3d 1271, 1276 (Fed.Cir. 2008). Accordingly, it is wrong to limit the construction of "access message" to its plain and ordinary meaning.

The construction of access message, therefore, needs to capture all the disclosed embodiments. The District Court did so by construing "access message" to mean "a signal or notification enabling or announcing access." The District Court's construction, which captures all disclosed embodiments while being consistent with the plain and ordinary meaning of access message, should be adopted by the Board, with the understanding that access – as argued by the Petitioner before the District Court and described in the specification – means the ability to enter, communicate with, or make use of an application.

III. THIRD-PARTY TRUSTED AUTHORITY

The PTAB has construed the term "third-party trusted authority" on six separate occasions. *See Samsung Electronics America, Inc. v. Proxense, LLC*, IPR2021-01444, Paper 11 at 11-15 (PTAB Feb. 28, 2022); *Samsung Electronics America, Inc. v. Proxense, LLC*, IPR2021-01447, Paper 12 at 10-14 (PTAB Feb. 28, 2022); *Samsung Electronics America, Inc. v. Proxense, LLC*, IPR2021-01448, Paper 12 at 8-11 (PTAB Feb. 28, 2022); *Google, LLC v. Proxense, LLC,* IPR2023-00232, Paper 10 (PTAB Jul. 24, 2024); *Google, LLC v. Proxense, LLC,* IPR2023-00233, Paper 10 (PTAB Jul. 24, 2024);. and *Google, LLC v. Proxense, LLC,* IPR2023-00234, Paper 10 (PTAB Jul. 24, 2024). In each instance, the term was construed consistent with its plain and

ordinary meaning to mean "a trusted authority that is an entity separate from the parties to a transaction." IPR2021-01444, Paper 11 at 15; IPR2021-01447, Paper 12 at 14; IPR2021-01448, Paper 12 at 11; IPR2024-00232, Paper 10 at 12; IPR2024-00233, Paper 10 at 12; and IPR-2024-00234, Paper 10 at 11. In three of the six previous IPRs, the PTAB determined the parties to the transaction include the application being accessed, such that the third-party trusted authority is not the application being accessed. *See* IPR2021-01444, Paper 11 at 26-27; *accord* IPR2021-01447, Paper 12 at 23-24; and *accord* IPR2021-01448, Paper 12 at 25-26. But in the other three IPRs, the PTAB took the position that the third-party trusted authority *is* an active participant in facilitating the transaction—because it is authenticating devices vis a vis ID codes . *See* IPR2024-00232, Paper 10 at 11; IPR2024-00233, Paper 10 at 11; and IPR2024-00234, Paper 10 at 10-11. Patent Owner disagrees that such authentication renders the third-party trusted authority as an active participant.

The claims of the 730 Patent recite three participants: the user; the third-party trusted authority; and the application the user is allowed to access. As noted *supra*, the PTAB has already construed a third-party trusted authority to be "a trusted authority that is an entity separate from the parties to a transaction." The third-party trusted authority, therefore, is not a party to the transaction. This only leaves the user and the application the user is allowed to access. Thus, the claims explicitly require the parties to the transaction be the user and the application. As the third-party trusted authority is not a party to the transaction, it cannot be the application being accessed.

IV. 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

As detailed *supra*, when correctly construed, claims 1, 2, 4-9. 11, 12, and 14-17 require; 1) that the third-party trusted authority is not the application being accessed; and 2) the access

message enables access to an application. Burger (U.S. Publication No. 2005/0050367) fails to either element. Failing to disclose all the elements of the claims, Burger cannot render the challenged claims invalid and unpatentable.

Previously, "third-party trusted authority" was construed consistent with its plain and ordinary meaning to mean "a trusted authority that is an entity separate from the parties to a transaction." IPR2021-01444, Paper 11 at 15; IPR2021-01447, Paper 12 at 14; IPR2021-01448, Paper 12 at 11; ; IPR2024-00232, Paper 10 at 12; IPR2024-00233, Paper 10 at 12; and IPR-2024-00234, Paper 10 at 11. An important aspect of the PTAB's construction, as shown by the application of its construction to the asserted art, is that the "third-party trusted authority" is **separate from the system being accessed**. *See* IPR201-01444, IPR2021-01444, Paper 11 at 25-26 ("Host processing unit 32, because it is not an entity separate from host facility 4, is not a third-party trusted authority.") and ("Here, the DPC is the resource to be accessed, but it is a party to the transaction, rather than a third party.")). Accordingly, consistent with Fig. 3 (reproduced below), the "third-party trusted authority" is separate from the biometric key and application. IPR2021-01444, Pater 11 at 14 ("This is consistent with the description in the Specification. For example, Figure 3, reproduced above, depicts trusted key authority 320 as an entity separate from biometric key 100, authentication module 310, and application 330. As the Specification states, "[t]rusted key authority 320 is a third-party authority that is present in some embodiments in order to provide enhanced security." Ex. 1001, col. 5, ll. 40–42.").

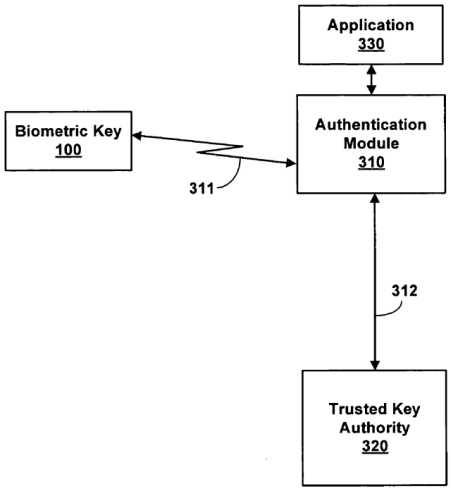


FIG. 3

The "third-party trusted authority" is thus a distinct entity whose role is to authenticate and provide an "access message" allowing the user to enter, communicate with, or make use of an application. *See* IPR2024-00234, Paper 10 at 10 ("In another preferred embodiment of the '905 Patent, trusted key authority 320 plays an active role in transactions, e.g., verifying to a grocery store that a biometric key presented by a customer is legitimate, thereby allowing the transaction to proceed."); and 730 Patent, Claim 1 ("***receiving an access message from the agent*** allowing the user ***access to an application***"); Claim 8 ("***receives an access message from the agent*** allowing the user ***access to an application***"); Claim 12 ("***in response to a positive access message***, allowing the biometrically verified user ***access to an application***"); and Claim 15 ("***receiving an access message from the agent*** allowing the user to ***access an application***") (emphasis added). Accordingly, the third-party trusted authority (shown in FIG. 3 below as "trusted key authority 320") is not what is being accessed to provide credit, access funds, download data, or otherwise perform a transaction (shown in FIG. 3 below as "application 330"). It is a distinct entity whose role is to authenticate. Server 114 of Burger, which the Petition cites as third-party trusted

authority, is a single entity combining the application to be accessed to perform a transaction with the trusted authority providing the authentication.

The Pocket Vault System described by Burger contains a **single** network server 114 hosting both the application to be accessed and the trusted authority. The combination of the application to be accessed and the trusted authority into a single entity is shown in FIGS. 1, 4 and 27, along with their accompanying descriptions. FIG.1 of Burger (reproduced below) shows a Pocket Vault network system in which network server 114 forms the hub of the system and serves as the entity storing information, acting as a service provider, and controlling access. Burger, ¶ [0051] ("FIG. 1 is a block diagram illustrating an example of a network system in which a portable electronic authorization device (also referred to herein as a "Pocket Vault") may be employed according to one embodiment of the invention"); and ¶ [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.").

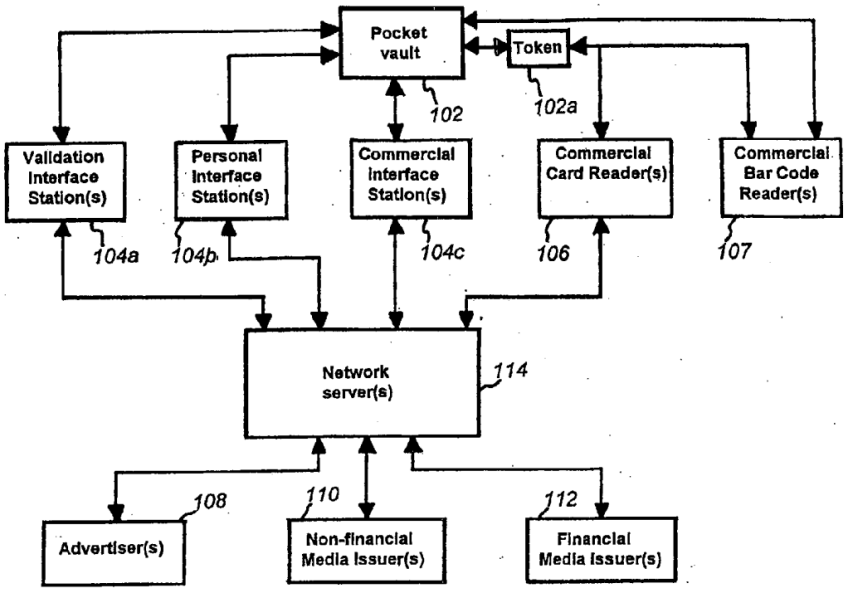


Fig. 1

After initially presenting network server 114 as a **single** entity acting both as a key authority and application, Burger reiterates that network server 114 is a key authority and application when detailing FIG. 4.

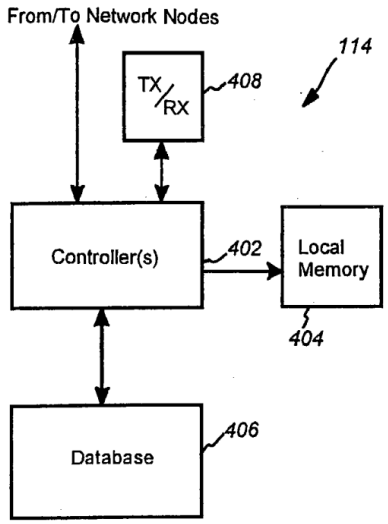


Fig. 4

"FIG. 4 shows an example embodiment of the network server 114 shown in FIG.1. As shown, the network server 114 may comprise one or more controllers 402, as

well as a local memory 404, a database 406, and a transceiver 408 coupled thereto. The illustrated components of the network server 114 are well known, and therefore will not be described in detail. The transceiver 408 may, for example, be used to communicate with other devices in the network system 100 (FIG. 1) using a wireless network Such as Bluetooth. The controller 404 may also communicate with other network devices via the Internet or a direct connection Such as the type established using a dial up modem.

The local memory 404 may have instructions stored therein which, when executed by the controller 402, cause the controller 402 to implement the routines described below in connection with FIGS. 19-25 and/or FIGS. 30-39. In some embodiments, the local memory 404 and/or data base 406 act as a website and execute software which may be accessed by a browser or similar software module operating on a computer....

The database 406 may, for example, comprise a relational database, and may be used to store the majority, if not all, of the data maintained by the network server 114. The database 406 may, for example, keep a real-time record of critical reference data along with transaction histories, back-up files, and security audit trail information for key events. Examples of specific items that may be stored in the database 406 include: a list of current Pocket Vault holders and appropriate contact information for each; records regarding the versions of software loaded onto each Pocket Vault 102, each pocket vault interface unit 302, and each interface station computer 304; a list of currently authorized or registered Pocket Vaults 102, identified by chip ID and linked to the holder list; a list of currently authorized or registered tokens 102a, identified by chip ID and linked to the holder list; a list of currently authorized locations for interface Stations 104 and telephone or other access lines therefor, including business information for each Such location and an indication as to the type of interface station 104 it is (e.g., a validation interface Station, a personal interface Station, or a commercial interface Station); a list of currently authorized or registered interface Station operators and the interface stations 104 with which they are associated; a list of currently authorized or registered interface Stations 104, identified by chip ID and linked to the list of

> authorized operators therefor, as well as encrypted cookie ID information (if any) for the respective interface stations 104; authorized media data received from media issuers that has not yet been downloaded to individual Pocket Vaults 102; backup data sets for individual Pocket Vault holders; detailed trans action histories for Pocket Vault registrations indicating where each Pocket Vault 102 was shipped from and to, where each Pocket Vault 102 was registered, which authorized interface Station operator conducted the registration process, when that authorized operator was added to the list of authorized operators at a particular location, who Sub mitted the key information to add the operator, which corporate representative associated with the network Server 114 met with which representative associated with the interface Station in establishing each new location for a validation interface station 104a, to whom and when each Pocket Vault 102 was issued; and communication encryption protocols. Each Pocket Vault account defined on the network server 114 may be defined to support multiple Pocket Vaults 102, as well as to identify other family members who may share certain contents of the Pocket Vaults 102 (e.g., family membership in a local museum).

Burger, FIG 4 and ¶¶ [0144]-[0146].

The above specifically details that the network server 114 depicted in FIG. 4 has both a database 406 and local memory 404. Burger, ¶ [0144] ("FIG. 4 shows an example embodiment of the network server 114 shown in FIG.1. As shown, the network server 114 may comprise one or more controllers 402, as well as a local memory 404, a database 406, and a transceiver 408 coupled thereto."). As Burger notes, local memory 404 contains instructions for the various routines accessed by the user and implemented by controller 402 of network server 114. Burger, ¶ [0145] ("The local memory 404 may have instructions stored therein which, when executed by the controller 402, cause the controller 402 to implement the routines described below in connection with FIGS. 19-25 and/or FIGS. 30-39."). In other instances, local memory 404 and/or database 406 act as the websites and execute software accessed by the user. Burger, ¶ [0145] ("In some

embodiments, the local memory 404 and/or data base 406 act as a website and execute software which may be accessed by a browser or similar software module operating on a computer."). Whether stored on local memory 404 or database 406, network server 114 is the entity having the application to be accessed by the user. Burger additionally describes database 406 as all the data maintained by network server 114, including a listing of currently authorized or registered Pocket Vaults. Burger, ¶ [0146]. Maintaining a listing of registered and authorized Pocket Vaults, network server 114 is the entity acting as the key authority. Thus, server 114 is a single entity performing authentication as a key authority and running the application to be accessed.

The dual nature of network server 114 is repeated by Burger a third time when describing FIG. 27 (reproduced below), which illustrates the Pocket Vault network system. Burger, ¶ [0530] ("FIG. 27 illustrates a network system similar to that described hereinabove.").

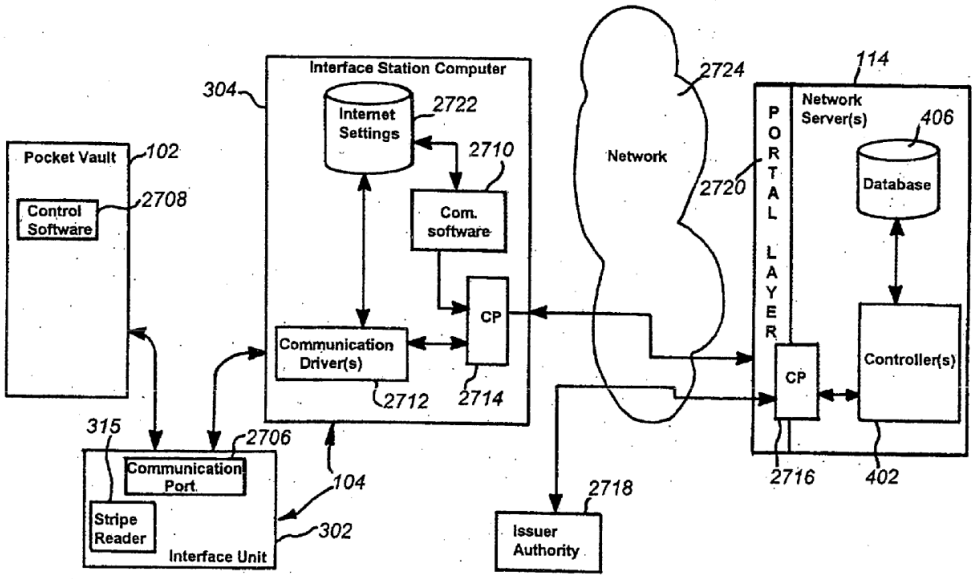
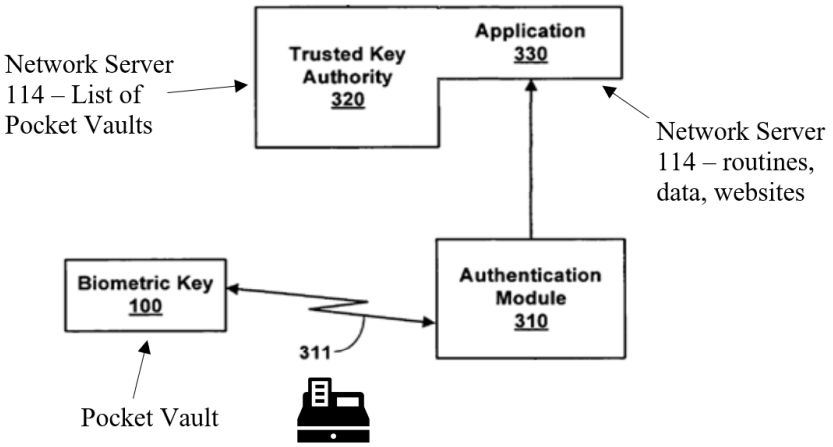


Fig. 27

Again, Burger details that network server 114 stores data, applications, and websites accessible by the user. Burger, ¶ [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 such, with FIG. 27, Burger reiterates that network server 114 is the application to be accessed. Burger also repeats that network server 114 is the key authority performing authentication. Burger, ¶ [0541] (“Overall, the networking arrangement illustrated in FIG. 27 allows the Pocket Vault 102 to access the network server 114. It also allows the interface station computer 304 to access restricted portions of the network server 114, such as, for example, user data stored in the database 406, when access is authenticated through communication from the Pocket Vault 102 to the network server 114.”); and ¶ [0558] (“If the website determines that the Pocket Vault 102 has been validated and authenticated, then the network server 114 may enable the authenticated holder to access or perform functions relating to some or all of the restricted area of the database 406 containing that holder's information.”). With FIG. 27, consequently, Burger is repeating that dual nature of network server 114 as both key authority and application.

As previously noted, in construing “third-party trusted authority,” the PTAB noted the separation between the key authority 320 and application 330, as depicted in FIG. 3 of the patent at issue. Burger, however, repeats again and again that within the Pocket Vault system network, server 114 functions both as the application accessed and the key authority controlling access. As such, recreating FIG. 3 to match the teachings of Burger produces the following figure lacking the separation noted by the PTAB.



PRIOR ART FIG. 3

(Burger's Pocket Vault System)

As the figure shows, the Pocket Vault system as described by Burger lacks a third-party trusted authority.

Despite the above architecture of the Pocket Vault System, the Petition asserts that network server 114 is a third-party trusted authority when accessed by the Pocket Vault user to authorize a transaction. Here the transaction is between the user and the Pocket Vault System. Specifically, the user is requesting from the Pocket Vault System the issuance of credit. In essence, the user is going to Pocket Vault to get money – as if it were an ATM. Instead of cash, the user receives the equivalent of a promissory note from the Pocket Vault System to tender payment to the merchant. The Pocket Vault user may then present that promissory note to the merchant as a guarantee of payment. The transaction, accordingly, is between only the user and the Pocket Vault System. The process of this transaction is detailed by Burger in FIGS. 19, 24, and 25, each of which depict routines performed by Server 114, including routine 2006 – determining whether the attempted use of the Pocket Vault is authorized. Accordingly, server 114 is the very system authenticating the Pocket Vault and performing the remainder of routine 1922 to processes the request to authorize

a transaction. As such, server 114 is not separate from the system being accessed to process the transaction and thus is not a third-party trusted authority.

When processing a transaction, server 114 determines whether to issue credit to the Pocket Vault user. As such, the Pocket Vault user is accessing server 114 to request credit. If the Pocket Vault user's request for credit is granted by server 114, the request is authorized by that server. Accordingly, at step 1922 server 114 is responding to a request for credit made by the Pocket Vault user. To do so, server 114 utilizes the routine depicted in FIG. 24 (reproduced below). Burger, ¶ [0473] ("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.").

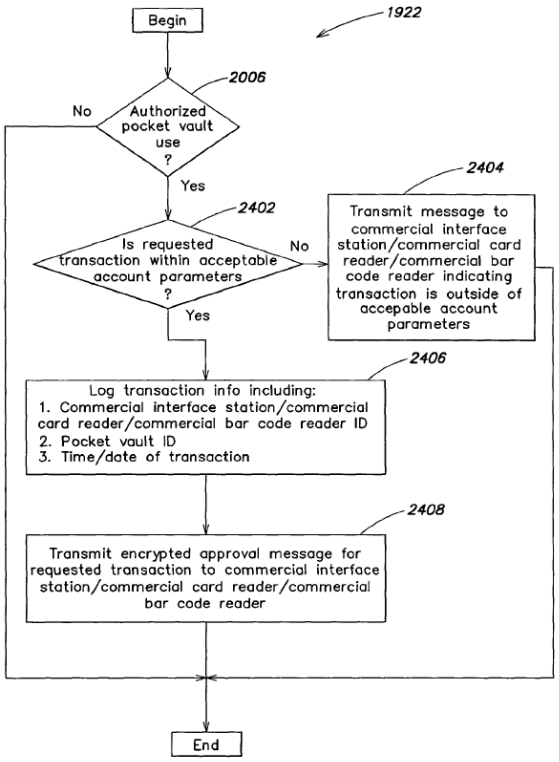


FIG. 24

The first element server's 114 FIG. 24 routine is a determination by server 114 whether the attempted use of the Pocket Vault is authorized at step 2006. Burger, ¶ [0511] ("As shown, the routine 1922 begins at the step 2006 (discussed below in connection with FIG. 25), wherein it is determined whether the attempted use of the Pocket Vault 102 is authorized.").

The routine performed by the server 114 to determine authorized use of the Pocket Vault is shown in FIG. 25 (reproduced below). Burger, ¶ [0519] ("FIG. 25 is a flow diagram illustrating an example of a routine that may employed to implement the step 2006 of the routines 1904 (FIG. 20), 1914 (FIG. 22), and 1922 (FIG. 24).").

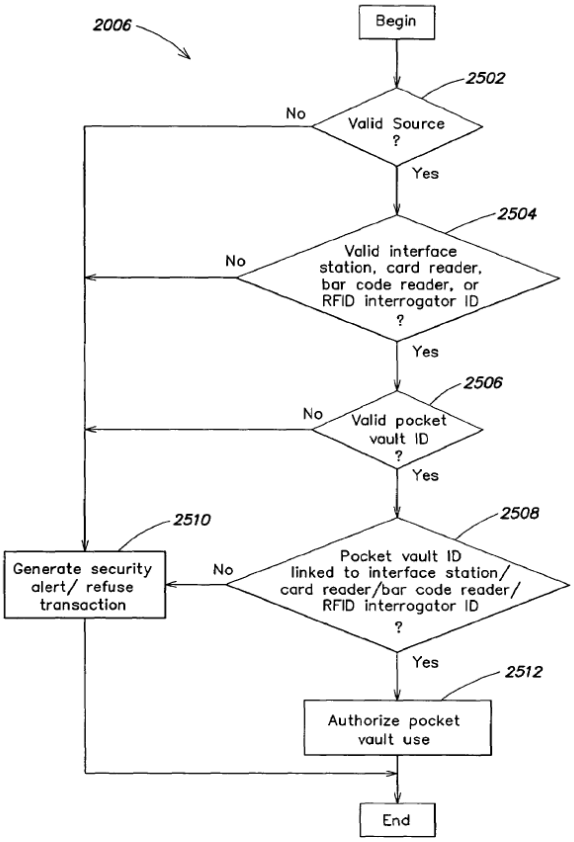


FIG. 25

As shown, at step 2506, server 114 determines if the Pocket Vault ID is valid. Thus, server 114 is authenticating the Pocket Vault as an initial step in processing the Pocket Vault user's request

for credit. After server 114 authenticates the Pocket Vault, server 114 continues the routine of transaction authorization by moving onto step 2402 in FIG. 24. At this point server 114 determines if the requested transaction is within acceptable account parameters. Accordingly, server 114 is making the determination to approve the request for credit. If server 114 determines the transaction is acceptable, server 114 continues process 1922 by logging the transaction at step 2406 and transmitting an approval message at step 2408. Burger, ¶ [0513] ("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).") As demonstrated by FIG. 24, therefore, server 114 **is the system being accessed to authorize the transaction** by issuing credit to the Pocket Vault user, making it a party to the transaction. Being both a party to the transaction, and the system responsible for authenticating the Pocket Vault, server 114 cannot a third-party trusted authority.

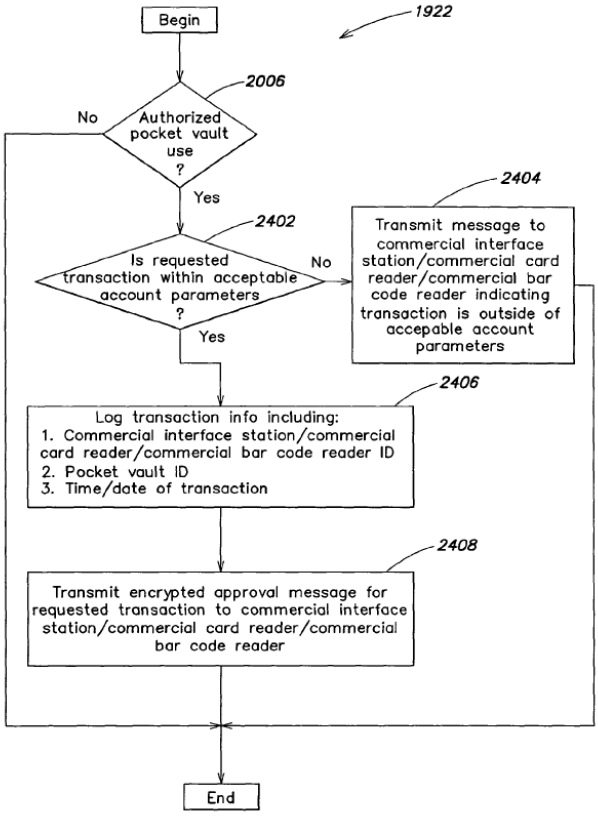


FIG. 24

In addition to the process of authorizing a transaction initiated in FIG. 19, Burger discloses authorization routine 1414 shown in FIGS. 17A and 17B (reproduced below) and initiated in primary routine 1400 running on an interface station as depicted in FIG. 14.

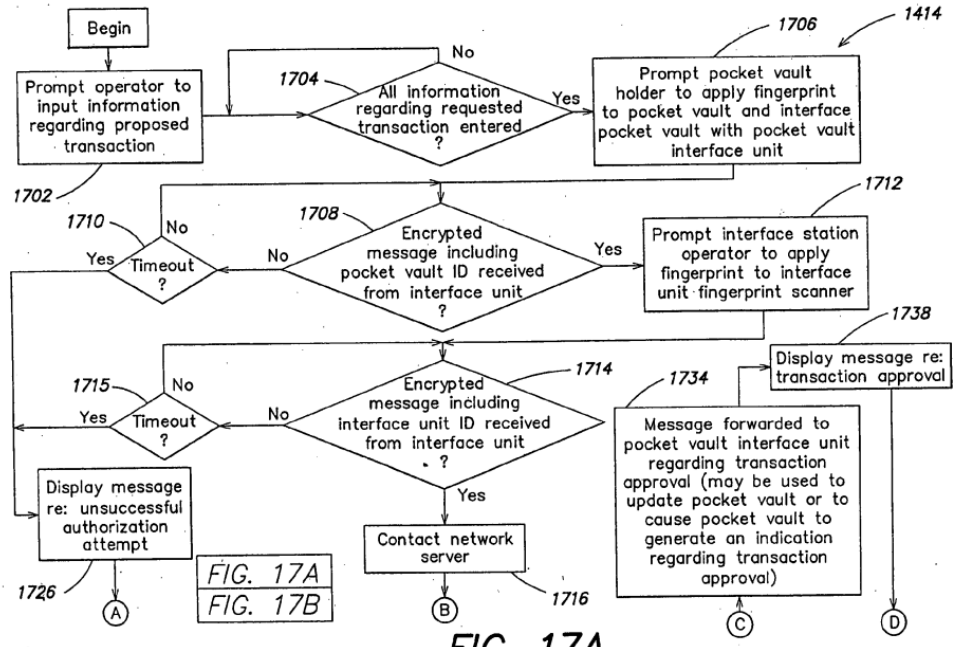


FIG. 17A

FIG. 17A
FIG. 17B

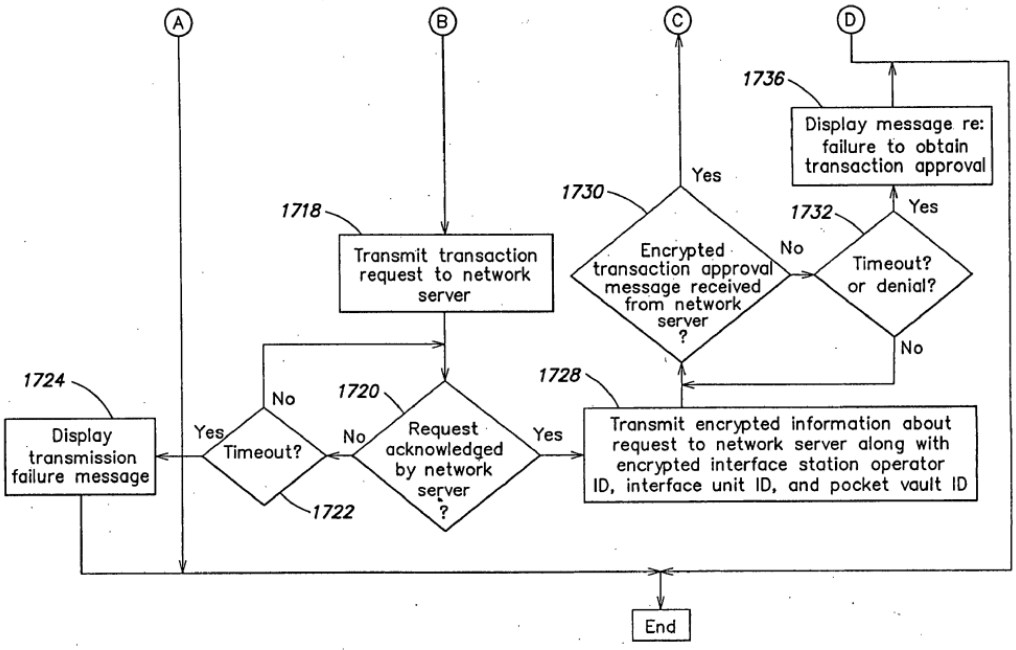


FIG. 17B

In routine 1414, the authorization request is transmitted to the Pocket Vault network server 114, which responds with an approval message. Burger, ¶ [0436] ("When, at the steps 1722 and 1724, it is determined that the request has been acknowledged in a timely manner, the routine 1414

proceeds to a step 1728, wherein encrypted information about the requested transaction is transmitted to the network server 114, along with the interface station operator ID, the interface unit ID, and the Pocket Vault ID."); and ¶ [0437] ("After the step 1728, the routine 1414 proceeds to steps 1730 and 1732, wherein it is determined whether an encrypted transaction approval message has been received from the network server 114 prior to the expiration of a timeout period measured by the step 1732."). Accordingly, as with the process initiated in FIG. 19, the Pocket Vault network server 114 is being accessed to authorize a transaction, and as such is the application being accessed.

Examining how credit card transactions work presents a clear picture of Pocket Vault's further participation in the transactions as the resource being accessed to tender payment. Routines 1400 and 1900 result in the transmission of an approval message from the server 114 to the merchant. Burger, ¶ [0513] ("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)."); and ¶ [0437] ("After the step 1728, the routine 1414 proceeds to steps 1730 and 1732, wherein it is determined whether an encrypted transaction approval message has been received from the network server 114 prior to the expiration of a timeout period measured by the step 1732."). The acquisition of an approval message is an element of the authorization element of a credit card transaction process terminating in the issuing bank sending an authorization response to the merchant. *See* Exhibit 2008 (Defining the "authorization" of a credit card transaction as including: "send[ing] an authorization request to the issuing bank, which approves or declines the request" and the "issuing bank send[ing] its decision back to the card association, where it then goes down the line, finally reaching the merchant."). As server 114 of the Pocket Vault system issues the encrypted

transaction approval to the merchant in Steps 2408 and 1730, Server 114 of Pocket is acting as the issuing bank. The transaction process next continues to settlement, during which the merchant redeems the batch approved authorizations for a transfer of funds into the merchant's account.

> "In the settlement stage, the merchant will finally receive funds from the transactions.
>
> 1. The merchant sends their batched approved authorizations to the payment processor.
> 2. The payment processor sends the authorizations to the card association.
> 3. The card association forwards them to the issuing bank.
> 4. The issuing bank transfers the funds to the merchant bank and charges an 'interchange fee". This typically happens within 24 to 48 hours of the transaction.
> 5. The merchant bank delivers funds to the merchant account."

Exhibit 2008.

Per the settlement process, the encrypted transaction approval sent to the merchant in Steps 2408 and 1730 issued by server 114 is payment provided by Pocket Vault that completes the transaction between the user and the merchant. Per settlement, the merchant would send the Pocket Vault transaction approval to payment processor to be presented to Pocket Vault acting as the issuing bank. Pocket Vault would then transfer the funds to the merchant account for deposit into the merchant's account. Accordingly, by sending the encrypted transaction approval to the merchant, Pocket Vault is providing a promissory note that the user may use as payment in the transaction – making the encrypted transaction approvals issued by Pocket Vault's payments completing the transaction. A payment completing a transaction between the merchant and the user is not an access message allowing the user access to an application, as required by claims 1, 2, 4-9. 11, 12, and 14-17. Additionally, by being accessed to provide payment to the merchant, server 114 of the pocket vault system is the application being accessed and thus not a third-party trusted authority.

In addition to use of the Pocket Vault system to providing payment in the form of transactions approvals, the Petition references downloading of hotel keys to a Pocket Vault as evidence of network server 114 being a third-party However, Burger clearly details that the key is **downloaded from the Pocket Vault network server 114,** making the network server 114 the application being accessed. Burger, ¶ [0676] ("Next, the prospective hotel guest may link to the network server 114 (while staying within the hotel's website), and follow on-screen instructions for downloading the key card for his/her room onto the Pocket Vault 102 (e.g., to ensure that the Pocket Vault 102 is interfaced with the pocket vault interface unit 302, and to ensure that the Pocket Vault holder has activated the Pocket Vault 102 by the appropriate Security mechanism such as a thumbprint for bio-metric ID verification).")

Finally, the Petition presents other advertisements, files, websites and computer software as other examples of applications. Yet each of these applications is provided by server 114 thereby making network server the application being access and not a third-party trusted authority. 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."); ¶ [0145] ("In some embodiments, the local memory 404 and/or data base 406 act as a website and execute software which may be accessed by a browser or similar software module operating on a computer."); 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 detailed *supra*, when correctly construed, the challenged claims require: 1) that the third-party trusted authority is not the application being accessed; and 2) the access message enables access to an application. Burger fails to either element. Failing to disclose all the elements of the claims, Burger cannot render the challenged claims invalid and unpatentable. Consequently, the Petition fails to establish Burger invalidates 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" nor "access message" elements. As noted supra, Burger fails to disclose these, and 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 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.

V. CONCLUSION

The Petition fails to demonstrate a reasonable likelihood that the Petitioner will prevail as to any of the challenged claims. *Inter partes* review of the 730 Patent should therefore be denied.

Dated August 21, 2024

Respectfully submitted by,

By: /David L. Hecht/
David L. Hecht (Reg. No. 61,618) (lead counsel)
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 Preliminary Response was served on August 24, 2024 by e-mailing copies to the following e-mail addresses as provided in Petitioner's Petition:

IPR42342-0136IP1@fr.com; PTABInbound@fr.com; axfptab@fr.com, devoto@fr.com and khan@fr.com

Dated: August 21, 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 SERVICE (37 C.F.R. § 42.6(e))

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 6,107 words, which is less than the 14,000 words allowed under 37 C.F.R. § 42.24(b)(1).

Dated: August 21, 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