

Microsoft Corp. (Petitioner)
v.
Proxense, LLC. (Patent Owner)

Petitioner's Demonstratives

Case No. IPR2024-00846
U.S. Patent No. 8,886,954
Before Hon. David C. McKone, Thu A. Dang, and Kevin F. Turner
Administrative Patent Judges



DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Table of Contents

• Related Proceedings	3
• The '954 Patent	6
• Construction of Third-party trusted authority (TPTA)	10
• Overview of Burger	23
• Issue 1 – Burger Discloses a TPTA	34
• Example Use Cases of Burger's TPTA Disclosure	39
• Issue 2 – Burger Renders Obvious an Access Message	56

Related Proceedings

Related 954 Proceedings

954 Proceeding	Petitioner	Outcome / Current Status
IPR2024-00233	Google	Director Review Pending; FWD found all challenged claims unpatentable (claims 1-7, 10-12, and 22-27)
IPR2024-00846	Microsoft	This Proceeding
IPR2024-01327	Microsoft	Institution Denied (Joinder)
IPR2024-01334	Apple	Joining Google IPR
IPR2024-01485	Apple	Institution Denied (Joinder)

Related 730 Proceedings

730 Proceeding	Petitioner	Outcome / Current Status
IPR2021-01444	Samsung	Institution Denied
IPR2024-00232	Google	Terminated – Adverse Judgment
IPR2024-00775	Microsoft	Terminated – Adverse Judgment
IPR2024-01326	Microsoft	Institution Denied (Joinder)
IPR2024-01333	Apple	Terminated – Adverse Judgment
IPR2024-01486	Apple	Institution Denied (Joinder)

Re-Examination Control Number 90/015,052 (pending; Non-Final Office Action issued)

Asserted Grounds

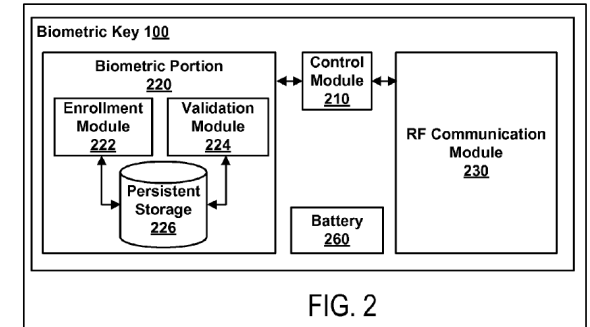
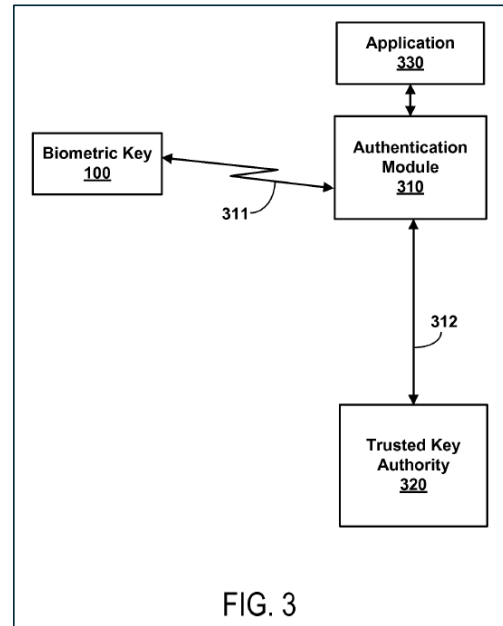
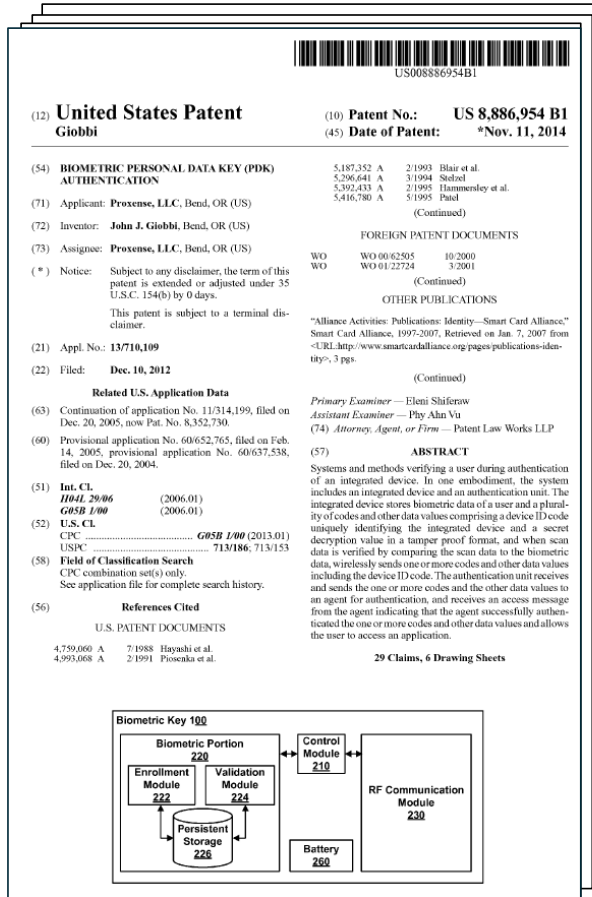
Ground	Claim(s)	35 U.S.C. § 103
1	1, 2, 4, 5, 7-13, 15, 16, 18-24, 26-29	Burger
2	3, 14, 17	Burger and Robinson
3	6, 25	Burger and Orsini

Pet., 1; MSC-1003, ¶20.

Proxense did not advance any arguments against the secondary references or combinations.

The '954 Patent

The '954 Patent



MSC 1001 (954 Pat.), FIGS. 2, 3; Pet., 3-4.

'954 Claim 1

1. A method comprising:
persistently storing biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is not capable of being subsequently altered;
responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;
comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;
responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes and other values from the plurality of codes and other data values for authentication to a third party that operates a trusted authority, wherein the one or more codes and other data values includes the device ID code; and
receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values sent to the third party and allowing the user access to the application.

MSC-1001 (954 Pat.), 10:5-28.

9

Construction of “third-party trusted authority” (TPTA)

The '954 patent recites a “third party that operates a trusted authority,” not a “third-party trusted authority,” which is recited in related US Patent No. 8,352,730. Because Patent Owner uses these terms interchangeably, to avoid confusion, Petitioner refers to the “third party that operates a trusted authority” as the “third-party trusted authority.” Pet., Rep., 1.

The Board's Construction of TPTA

Institution Dec.

To be clear, below, we evaluate Petitioner's showing as to obviousness over Burger based on the ordinary meaning of third party that operates a trusted authority, namely, "a trusted authority that is an entity separate from the parties to a transaction."

Paper 8, 11.

Patent Owner has Modified Its Understanding of TPTA

Proxense FIRST advanced a construction in the Samsung -01444 IPR, which the Board adopted.

We agree with Patent Owner. The plain meaning of “third-party trusted authority” suggests an entity or party separate from the principal parties to a transaction. See, e.g., THE AMERICAN HERITAGE COLLEGE DICTIONARY 1433 (4th ed. 2004) (“third party n. . . . 2. One other than the principals involved in a transaction.”) (Ex. 3002).

Pet., 3 (citing MSC-1007 (ID in IPR2021-01444), 14).

Proxense THEN advanced further narrowing constructions through “implicit” constructions.

Patent Owner has consistently disputed the implicit construction of the *transaction* and the *principal parties* thereto.

Rather, Patent Owner is merely attempting to construe the *transaction* and the *principal parties* thereto, which limit the scope of “third-party trusted authority.”

POR, 2.

Patent Owner has attempted to incorporate several different limitations into the construction of TPTA

POR

be identified. A transaction is an activity or a request involving two parties. *See* Ex. 2014 (Defining

...

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 being 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 being 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.

Patent Owner Adopts An Incorrect TPTA Construction

Let's Recap the Evolution of PO's Understanding

Samsung -01444 IPR	Current IPR
TPTA is an entity or party separate from the principal parties in a transaction. TPTA is separate from the system being accessed.	TPTA is a third party with respect to the user being allowed access and the application being accessed.

Patent Owner Mischaracterizes the Claims

POR

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 being allowed access and an application being accessed. Yet, the Petition asserts grounds of invalidity based upon transactions wherein the “third-party trusted

POR, 1.

Patent Owner’s entire case rests on a factually incorrect assertion and misunderstanding of the claim. (Pet. Rep., 2)



Claim 1

responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes and other values from the plurality of codes and other data values for authentication to a third party that operates a trusted authority, wherein the one or more codes and other data values includes the device ID code; and receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values sent to the third party and allowing the user access to the application.

MSC-1001, claim 1.

15

Patent Owner's Construction Has Several Flaws

Petitioner Reply (Paper 14)

The plain reading of the independent claims makes clear that Proxense's implied construction has no support in the claim language. MSC-1033, ¶[13]. For instance, the claims do not recite the word "transaction," nor do they claim that a transaction includes the "allowing" operation such that one would understand the transaction in the Board's construction of a "third-party trusted authority" to be limited to the "allowing" operation. MSC-1033, ¶[13].

Paper 14, 4.

Claim 1

responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes and other values from the plurality of codes and other data values for authentication to a third party that operates a trusted authority, wherein the one or more codes and other data values includes the device ID code; and receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values sent to the third party and allowing the user access to the application.

MSC-1001, claim 1.

16

Patent Owner's Construction Has Several Flaws

Petitioner Reply (Paper 14)

the transaction. MSC-1033, ¶[14]. Claim 16, for instance, recites that the “allowing” is performed in response to receiving the access message. It is the “receiving” feature that includes the “third-party trusted authority,” which invokes a transaction by virtue of the Board’s construction, not the “allowing” feature that is performed in response to the “receiving” feature. MSC-1033, ¶[14]. Proxense’s incorrect implied constructions creates a link between the “receiving” and “allowing” steps that does not exist. The issue here is not whether the claim language controls over embodiments in the specification (as Proxense would have it). See POR, 6, 7. Instead, it is that Proxense is creating a link between claim features that does not exist and interpreting the claims in a manner that is not supported by the specification. Indeed, there is no basis for the transaction to be limited to “allowing a user access to an application.” MSC-1033, ¶[15].

Paper 14, 5.

Claim 16

requesting authentication of the integrated device using the one or more codes and other data values by the trusted authority;
receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party; and
in response to receiving the access message, allowing the biometrically verified user access to the application.

MSC-1001, claim 16.

The '954 Patent Description of a Party

Institution Dec.

transaction.” *Id.* at 23. Instead, we evaluate a party’s relationship to the transaction to determine whether it is a principal party to the transaction or a third-party. *Id.* at 11 (“The ‘witness’ role mentioned in the Specification (Ex. 1001, 7:30–33) refers to an agent’s relationship to the principal parties to the transaction, not to the level of activity the agent engages in.”), 22 (“We agree with Petitioner that, in this example, the TPCP is separate from, and thus a third party to, the principal parties to the transaction (the user and the vendor/retailer/service provider) and also a third party to the financial institution that pays the vendor.”).

Paper 8, 11.

'954 Patent

one embodiment of the present invention. An agent checks 510 an identification of the user and establishes a profile. The agent can be, for example, a government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness. The agent can follow standardized procedures such as requiring identification based on a state issued driver license, or a federally issued passport in order to establish a true identity of the user.

MSC-1001, 7:27-36.

The '954 Patent Description of a Transaction

Petitioner Reply (Paper 14)

Second, there is no intrinsic support for Proxense's implied construction. MSC-1033, ¶[16]. The '954 patent mentions the word "transaction" once in the context of a "bank transaction[]," which is similar to the prior art mapping presented in the Petition. MSC-1001, 1:31; Pet., 35 ("Obtaining payment information or authorization for charging a credit card or bank account"). The plain and ordinary meaning of "transaction" is also relatively broad. For instance, the Merriam-Websters Dictionary describes a "transaction" as "a communicative action or activity involving two parties or things that reciprocally affect or influence each other" or "an act, process, or instance of transacting." MSC-1008, 1252; Pet., 41, MSC-1003, ¶[113]. Proxense fails to properly explain why a

Paper 14, 6.

'954 Patent

tials, such as a password, before allowing access. Similarly, a PIN number can be required by an ATM machine before allowing a person to perform automated bank transactions. A

MSC-1001, 1:29-31.

The '954 Patent Description of an Application

'954 Patent

Application 330 is a resource that can be accessed by a verified and authenticated user. Application 330 can be, for example, a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file, a financial account (e.g. a savings account, checking account, brokerage account, credit card account, credit line, etc.) and the like. In one embodiment, a file

MSC-1001, 6:18-24; Pet., 51.

Patent Owner's Construction Violates the *Thorner* Factors

Petitioner Reply (Paper 14)

Third, Proxense fails to satisfy the guidelines set forth by the Federal Circuit for adopting narrow constructions. The Federal Circuit explained that a narrow construction of a claim term may be adopted “1) when a patentee sets out a definition and acts as his own lexicographer,” and “2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution.”

Thorner v. Sony Comput. Entm't Am. LLC, 669 F.3d 1362, 1365 (Fed. Cir. 2012).

Paper 14, 8.

Patent Owner's Reliance on *In re Suitco Surface* is Misplaced

Petitioner Reply (Paper 14)

Fifth, Proxense's reliance on *In re Suitco Surface, Inc.* is misplaced. According to Proxense, in *In re Suitco Surface, Inc.*, the claim language recited an element that performed an action, and the Petitioner in that case was incorrectly mapping to an element that did not have to perform this action. POR, 5, 6. But here, Petitioner's prior art mapping satisfies all the claimed features and all the performed actions, such as the receiving and allowing operations. Unlike *In re Suitco Surface, Inc.*, the issue here is not of mapping to an element that fails to perform an action. Rather, it is that Proxense advances an unsupported narrow construction to further limit a term already construed by the Board multiple times in an attempt to overcome Petitioner's prior art invalidity challenge. Proxense

Paper 14, 9.

Overview of Burger

Burger

MSC-1005

(19) **United States**
 (12) **Patent Application Publication** (10) Pub. No.: US 2005/0050367 A1
 Burger et al. (43) Pub. Date: Mar. 3, 2005

(54) **PORTABLE ELECTRONIC AUTHORIZATION SYSTEM AND METHOD**
 (75) Inventors: Todd O. Burger, Lexington, MA (US);
 Karlin B. Jensen, Reading, MA (US)

Correspondence Address:
 Robert M. Abrahamson
 Wolf, Greenfield & Sack, P.C.
 600 Atlantic Avenue
 Boston, MA 02110-2206 (US)

(73) Assignee: Chameleon Network, Inc., Concord, MA

(21) Appl. No.: 10/954,810

(22) Filed: Sep. 30, 2004

Related U.S. Application Data

(60) Division of application No. 10/302,319, filed on Mar. 19, 2003, and which is a continuation-in-part of application No. 09/968,628, filed on Oct. 1, 2001, which is a continuation-in-part of application No. 09/675,438, filed on Sep. 28, 2000.
 (60) Provisional application No. 60/366,098, filed on Mar. 19, 2002. Provisional application No. 60/379,964, filed on May 13, 2002. Provisional application No. 60/156,356, filed on Sep. 28, 1999. Provisional application No. 60/167,006, filed on Nov. 23, 1999. Provisional application No. 60/184,425, filed on Feb. 23, 2000. Provisional application No. 60/217,542, filed on Jul. 12, 2000.

Publication Classification
 (51) Int. Cl.⁷ H04L 9/32
 (52) U.S. Cl. 713/262

ABSTRACT

In one embodiment, an apparatus comprises a user authenticator and a transponder. The transponder is permitted to emit a wireless signal representing information stored in the apparatus in response to a wireless interrogation signal after the user authenticator has authenticated the identity of the user. In another embodiment, an apparatus comprises, a memory, a user input, and a transponder. The memory stores at least first and second distinct codes. The user input permits a user to select any one of the at least first and second codes for transmission in response to a wireless interrogation signal. The transponder emits a wireless signal representing the selected one of the at least first and second codes in response to an interrogation signal. In yet another embodiment, a token that may be used to engage in a transaction at a point of sale comprises a substrate, a rewritable memory, and a reconfigurable display. The rewritable memory is supported by the substrate and can be selectively configured to store information on the token that identifies an account that is to be used to engage in the transaction at the point of sale. The substrate and memory are configured and arranged such that the substrate can be selectively interfaced with an apparatus at the point of sale to permit the apparatus to read the contents of the memory. The reconfigurable display is also supported by the substrate and displays at least some of the information that is stored in the rewritable memory.

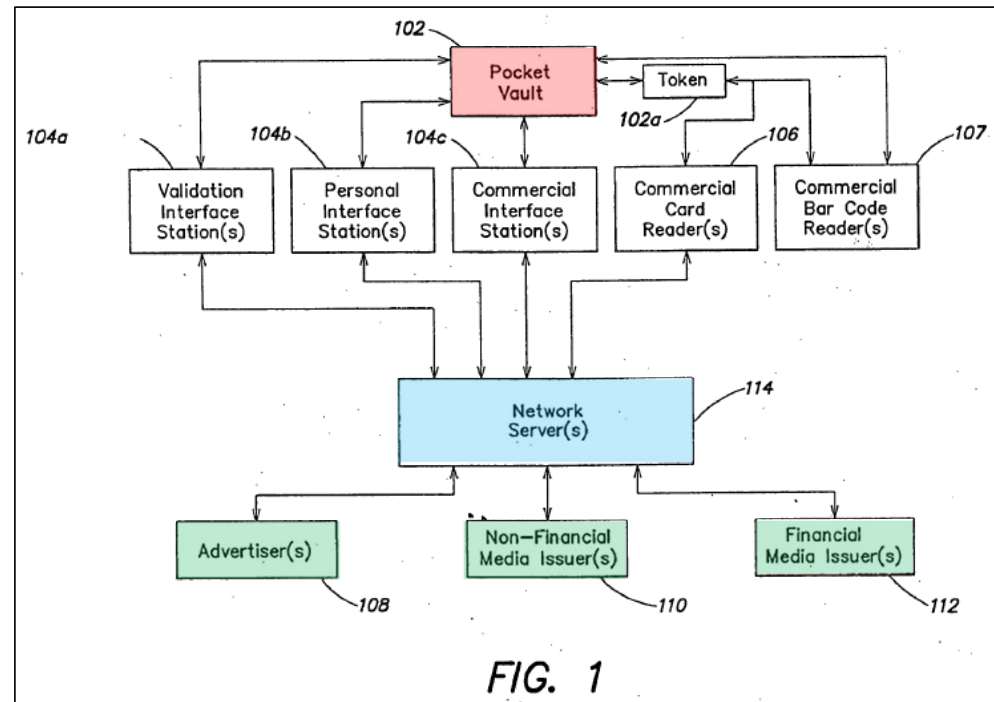
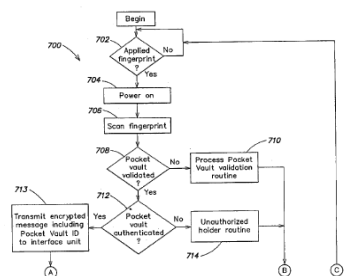


FIG. 1

Pet., 5; MSC-1005, FIG. 1.

Burger

MSC-1005.

Burger's Pocket Vault is a "Point of Transaction" Device

Burger

[0094] Because the device may incorporate many different media that are commonly stored in a person's wallet or elsewhere, possibly including both financial and non-financial media, it is much more than a simple point-of-sale (POS) device. Therefore, the device may be more appropriately referred to as a multi-purpose, "point-of-transaction" device. In any situation of presentment, whether for purposes such as building security, demonstrating membership or using credit or debit capacity, the system is designed to perform tasks more safely, securely and with greater ease than is possible with prior art systems. Further, while certain computer technologies are involved, the preferred embodiment is such that some people may barely recognize it as a computer, seeing instead a more comfortable to carry, easier-to-use, safer and more securely packaged means of transporting typical wallet contents and other items.

MSC-1005, ¶[94]; Pet., 23; MSC-1003, ¶[90].

Burger's Pocket Vault Provides Security

Burger

[0116] Because of the creation of the above-described trust relationships, each Pocket Vault 102 and each interface station 104 may communicate securely with the network server 114, as well as with any other networked devices or sites that require a high level of trust. Also, the existence of these trust relationships enable individual Pocket Vaults 102 to accept other services provided by the network servers 114,

...

any of the interface stations 104a-c. Therefore, if a Pocket Vault 102 is lost or stolen, the Pocket Vault holder need only obtain a new Pocket Vault 102, and the entire contents of the lost Pocket Vault 102 can be uploaded thereto, in a single communication, in a matter of seconds. In addition, in the event that a validated Pocket Vault 102 is lost or stolen, the network server 114 may void the chip ID of that Pocket Vault 102, so that the Pocket Vault 102 cannot be used by a third party, even if the holder validation security (e.g., the bio-metric scanning or PIN entry requirement) is somehow breached. Voiding the chip ID of the Pocket Vault 102 may, for example, prevent the Pocket Vault 102 from assigning any media information to the associated Chameleon Card.

[0158] When used by a consumer, retailers may verify authenticity by matching the information displayed on the token 102a with that revealed in the swipe or other token reading process. Without a match, the token 102a may be rejected.

MSC-1005, ¶[158]; Pet. 7, 17, 36, 38, 42.

[0320] 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. There is no way for this embossing to disappear when it is not needed and appear at just the right time, either with a standard card or a Smartcard. As a result, such numbers are generally in view and this visibility may lead to fraud. In one embodiment, the Pocket Vault 102 may

MSC-1005, ¶[320]; Pet. 17, 38, 42, 53.

MSC-1005, ¶[116]; MSC-1003, ¶[109]; Pet. 37-38.

Burger

MSC-1005.

Burger's Pocket Vault Use Method Encompasses the '954 Patent's Method

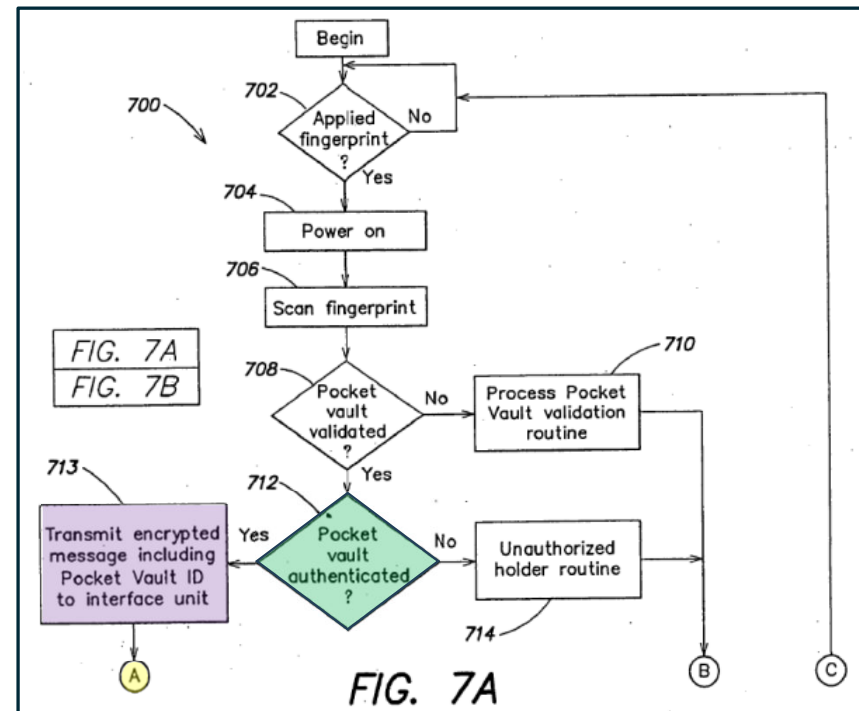
Burger

[0184] When, at the step 708, it is determined that the Pocket Vault 102 has already been validated, the routine 700 proceeds to a step 712, wherein it is determined whether Pocket Vault 102 has been authenticated, e.g., whether the fingerprint scanned at the step 706 matches one of the fingerprints stored in the fingerprint memory 212.

[0186] When, at the step 712, it is determined that the Pocket Vault 102 has been properly authenticated, the routine 700 proceeds to a step 713, wherein an encrypted message including the unique Pocket Vault chip ID is transmitted to the pocket vault interface unit 302, in the event that the Pocket Vault 102 is interfaced or in communication with such a device.

MSC-1005, ¶¶[184], [186]; Pet., 10-12.

Burger



MSC-1005, FIG. 7A; Pet., 11.

27

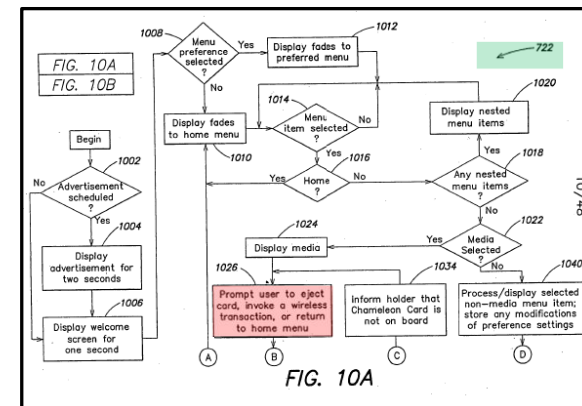
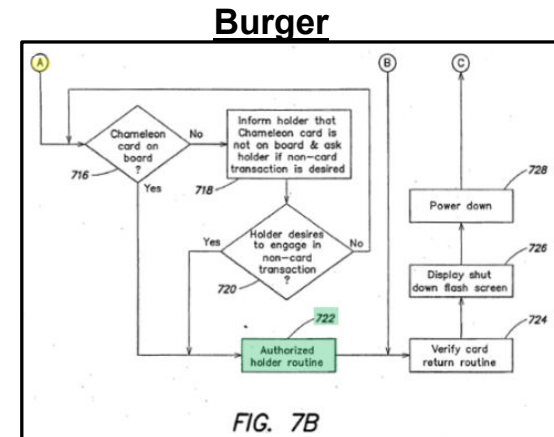
MSC-1005.

Burger's Pocket Vault Use Method Encompasses the '954 Patent's Method

Petition

In some embodiments, after the unique Pocket Vault chip ID is transmitted and a Chameleon Card (token) is determined to be on-board the Pocket Vault, an “AUTHORIZED HOLDER” routine (step 722) is performed, as shown in FIGS. 7B, 10A, (reproduced below) and 11. MSC-1005, ¶¶[189]-[195]. In the “AUTHORIZED HOLDER” routine, advertisements sent from an advertiser 108 to the network server 104 are provided to the Pocket Vault for display. MSC-1005, ¶¶[236]-[238], FIG. 10A. In addition, a user can make selections to enter a wireless transaction. MSC-1005, ¶¶[257]-[262], FIGS. 10A, 11; MSC-1003, ¶[64].

Pet., 12.



MSC-1005, FIGS. 7B, 10A; Pet., 12, 50.

28

Burger

MSC-1005.

Burger's Pocket Vault Use Method Encompasses the '954 Patent's Method

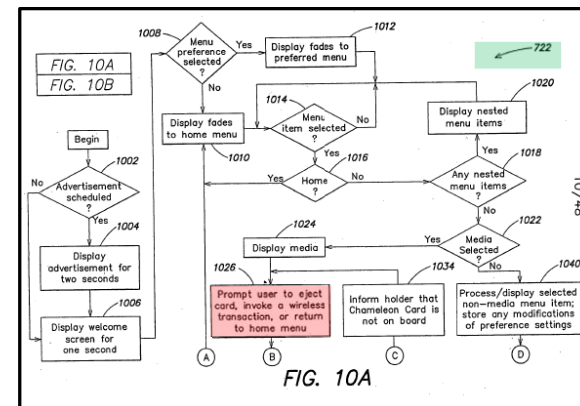
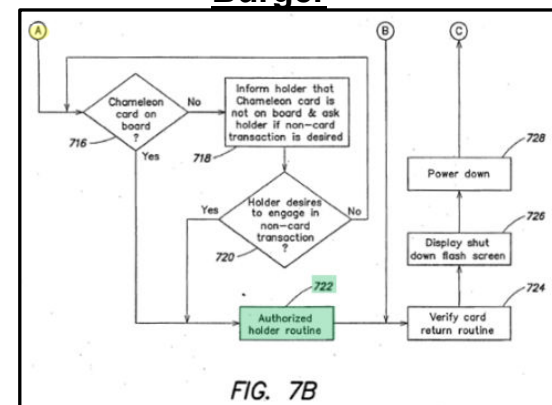
Burger

[0194] When, at the step 716, it is determined that the Chameleon Card is on-board the Pocket Vault 102, the routine 700 also proceeds to the step 722, wherein the **AUTHORIZED HOLDER routine** (discussed below in connection with FIGS. 10 and 11) is executed. FIGS. 26G-N

[0256] After the step 1024, the routine 722 proceeds to a step 1026, wherein the holder is prompted to choose to: (1) EJECT the card, (2) to invoke a **WIRELESS transaction**, or (3) to return to the HOME menu.

MSC-1005, ¶¶[194], [256]; Pet., 12.

Burger



MSC-1005, FIGS. 7B, 10A; Pet., 12, 50.

29

Burger

MSC-1005.

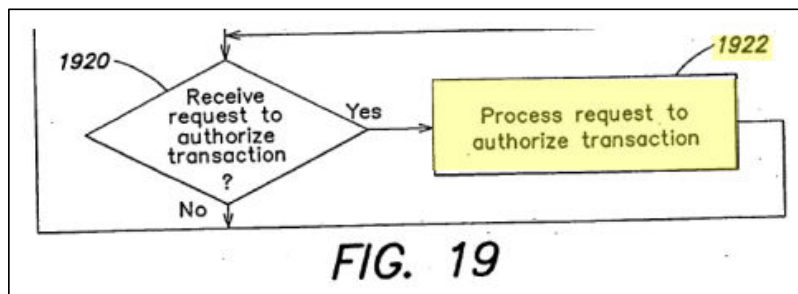
Burger's Pocket Vault Use Method Encompasses the '954 Patent's Method

Petition

Burger's Pocket Vault can be used as a "wallet replacement" to execute a transaction. MSC-1005, FIGS. 19, 24, 25, ¶[93]. When a request to authorize a transaction has been made, Burger's network server implements the operations depicted in FIGS. 24 and 25 (reproduced below). MSC-1005, FIG. 19, ¶[0474]; MSC-1003, ¶[65].

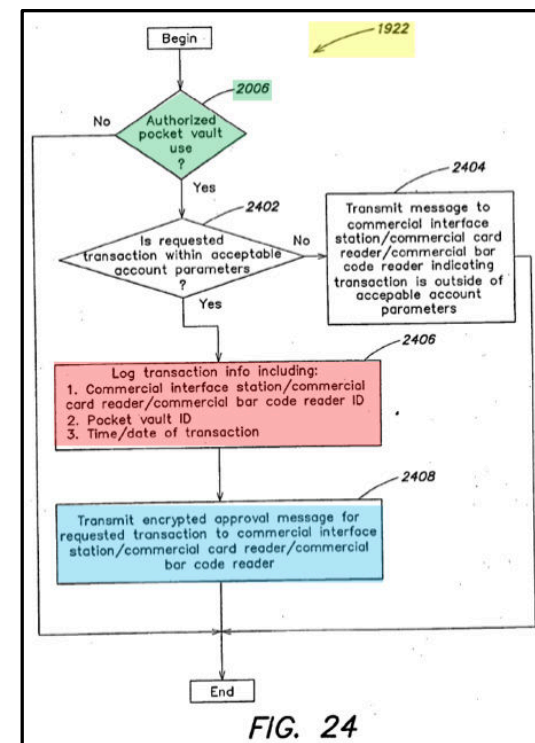
Pet., 14-15.

Burger



MSC-1005, FIG. 19; Pet., 14.

Burger



MSC-1005, FIG. 24; Pet., 15.

30

Burger

MSC-1005.

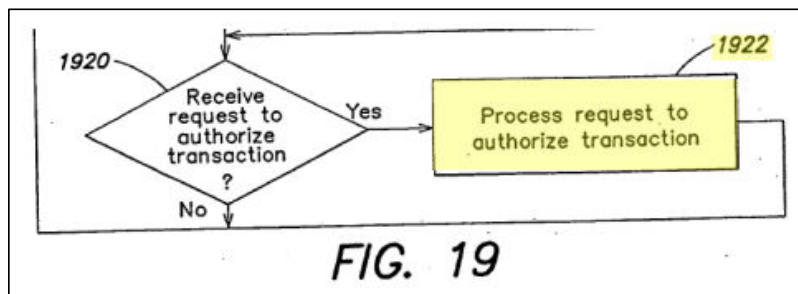
Burger's Pocket Vault Use Method Encompasses the '954 Patent's Method

Burger

[0474] 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.

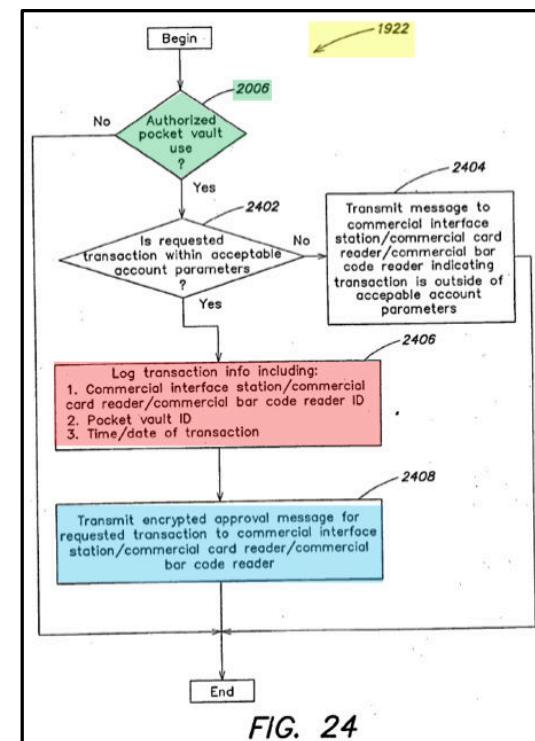
MSC-1005, ¶[474]; Pet., 14.

Burger



MSC-1005, FIG. 19; Pet., 14.

Burger



MSC-1005, FIG. 24; Pet., 15.

31

Burger

MSC-1005.

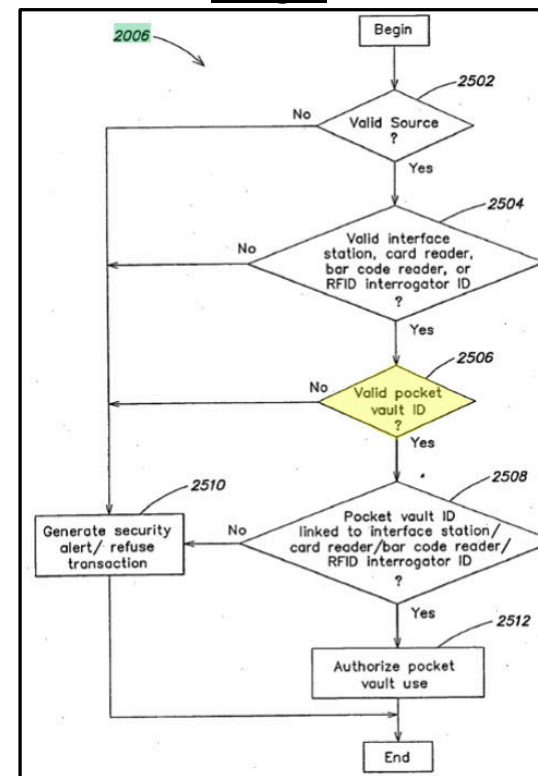
Burger's Pocket Vault Use Method Encompasses the '954 Patent's Method

Petition

As shown above, in response to the request to authorize a transaction, the network server determines whether the Pocket Vault is authorized. MSC-1005, FIGS. 24, 25; ¶¶[0511]-[513]. To determine whether the Pocket Vault is authorized, it is determined (1) whether the point of sale terminal or other entity with which a transaction is being attempted is connected to a valid source, and (2) whether the ID of the interface station, card reader, barcode reader or RFID interrogator is valid, and is properly linked to the source to which is connected. MSC-1005, FIG. 25; ¶¶[0520]-[523]. If the network server determines that there is a valid source and the ID is valid, the network server proceeds to determine whether the Pocket Vault ID is valid, and upon, doing so, determines that the Pocket Vault is authorized. MSC-1005, FIG. 25; ¶¶[0524]-[529], [182]; MSC-1003, ¶[66].

Pet., 16-17.

Burger



MSC-1005, FIG. 25; Pet., 16-17.

32

Burger

MSC-1005.

Burger's Pocket Vault Use Method Encompasses the '954 Patent's Method

Burger

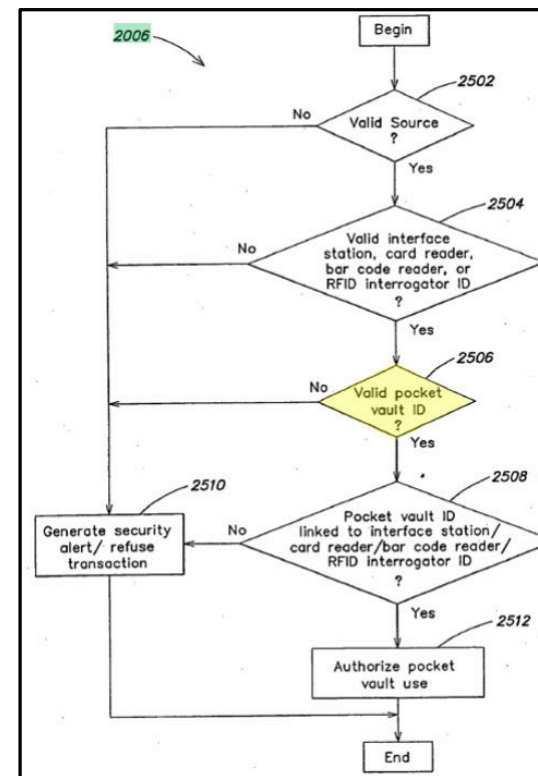
[0520] FIG. 25 is a flow diagram illustrating an example of a routine that may be employed to implement the step 2006 of the routines 1904 (FIG. 20), 1914 (FIG. 22), and 1922 (FIG. 24).

[0521] As shown, the routine 2006 begins at a step 2502, wherein it is determined whether the point of sale terminal or other entity with which a transaction is being attempted is connected to a valid source (e.g., an authorized telephone line or an authorized internet protocol (IP) address).

[0525] When, at the step 2504, it is determined that the ID of the entity proposing the transaction is valid, the routine 2006 proceeds to a step 2506, wherein it is determined whether the Pocket Vault ID (if available) is valid. It should be appreciated that, when a card reader 106, a barcode reader 107, an RF signal receiver, or an RFID interrogator is employed, it is possible that the ID from the Pocket Vault will not be transmitted to the network server 114. Therefore, the step 2506 may be skipped in such a situation.

[0527] When, at the step 2506, it is determined that the Pocket Vault ID (when) is valid or is not required, the routine 2006 proceeds to a step 2508, wherein it is determined whether the Pocket Vault ID (if available) is linked to the ID

Burger



MSC-1005, ¶¶[520]-[527]; Pet., 17.

MSC-1005, FIG. 25; Pet., 16-17.

33

ISSUE 1

Burger discloses a “third-party trusted authority”

Burger Discloses the “Third-party Trusted Authority”

Burger Teaches that the Network Server is a “Trusted Authority”

[0114] As discussed below, great care may be taken to ensure that only authorized individuals are permitted to validate Pocket Vaults 102 by having their authentication information (e.g., their fingerprint data or PIN codes) stored therein. Therefore, after it has been confirmed that the holder's authentication information has been properly stored in the Pocket Vault 102, a trust relationship may be established between the network server 114 and the Pocket Vault 102. This relationship may involve, for example, the registration of a unique encrypted chip ID of the Pocket Vault 102 with the network server 114 through a secure Internet connection, the distribution of a digital certificate (e.g., a PKI certificate) to the Pocket Vault 102, and the grant of authority to the Pocket Vault 102 to permanently store the Pocket Vault holder's authentication information.

MSC-1005, ¶[114]; MSC-1003, ¶[109]; Pet. 8, 37.

[0146] 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

...

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

...

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).

MSC-1005, ¶[146]; MSC-1003, ¶[109]; Pet. 37.

35

Burger Discloses the “Third-party Trusted Authority”

Burger Teaches that the Network Server is a “Trusted Authority”

[0116] Because of the creation of the above-described trust relationships, each Pocket Vault 102 and each interface station 104 may communicate securely with the network server 114, as well as with any other networked devices or sites that require a high level of trust. Also, the existence of these trust relationships enable individual Pocket Vaults 102 to accept other services provided by the network servers 114,

MSC-1005, ¶[116]; MSC-1003, ¶[109]; Pet. 37-38.

Burger Discloses the “Third-party Trusted Authority”

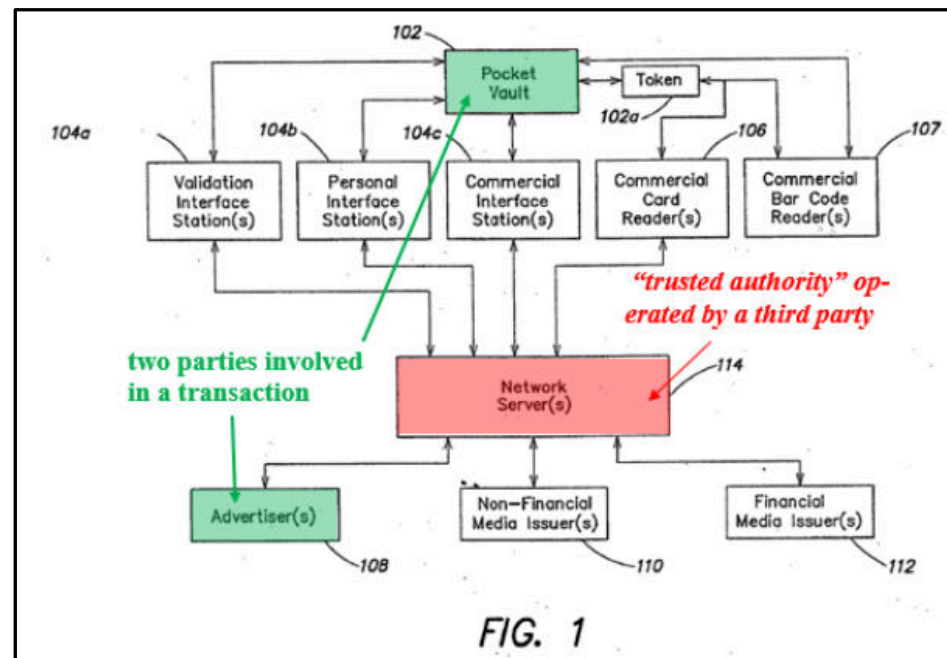
Burger’s Network Server is a “trusted authority operated by a third party”

Petition

1005, ¶¶[146], [0531]-[0543], FIG. 27. In both cases, the party that runs the network server is the “third party that operates a trusted authority.” MSC-1005, ¶¶[146], [237], [0531]-[0543], FIG. 27. The network server (or the company running it) is a separate entity from the user/Pocket Vault and the financial media issuers 112/non-financial media issuers 110/advertisers 108, and thus would have been understood by a POSITA to be a “third party.” MSC-1005, FIG. 1; MSC-1003, ¶[108].

Pet., 36-37, 40; MSC-1003, ¶¶[108], [111].

Burger



MSC-1005, FIG. 1.

Burger Discloses the “Third-party Trusted Authority”

Burger Teaches that the Network Server is Operated by a “Third Party”

thereto. 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.

MSC-1005, ¶¶98; MSC-1003, ¶¶107; Pet. 36.

mation stored on the network server 114. The advertiser 108 (FIG. 1) may, for example, have made arrangements with the company operating the network server 114 to have

MSC-1005, ¶¶237; MSC-1003, ¶¶107, [117]; Pet. 36-37, 39.

DR. TRAYNOR'S USE CASE EXAMPLE

Burger supports a Retail Use Case
that Renders Claim 1 Obvious

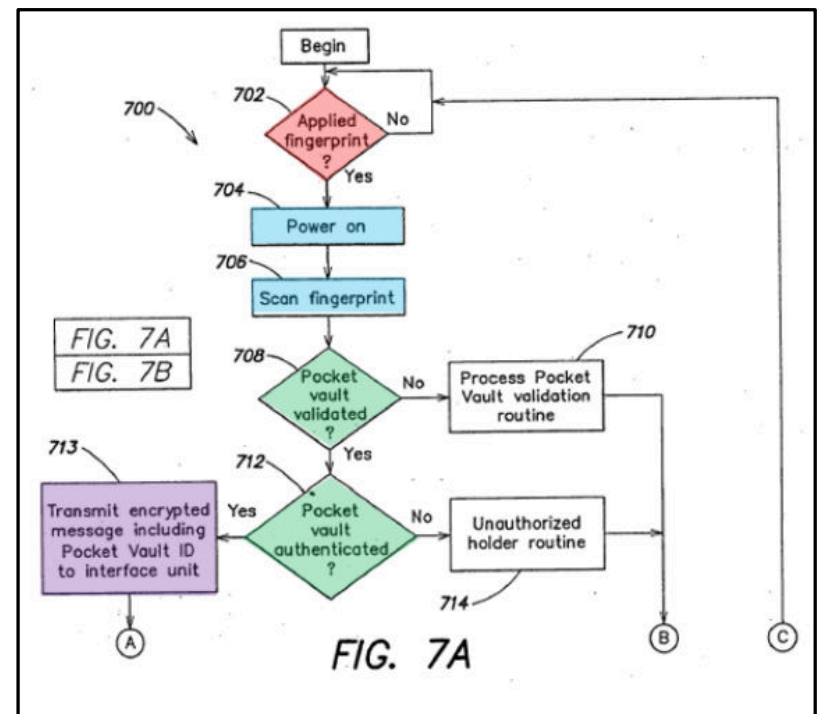
Retail Use Case

Dr. Traynor's 1st Declaration

69. When a user is interested in using the Pocket Vault 102 for a transaction (e.g., when the user is at a grocery store or retail store), the user places the user's finger on the Pocket Vault scanner (see red annotated diamond in FIG. 7A below). MSC-1005, FIG. 7A, ¶¶[320], [158], [95]. The Pocket Vault activates and then obtains a biometric scan (e.g., fingerprint or retina scan) (see blue annotated rectangles in FIG. 7A below) of the user and checks to see if a matching record is stored in the Pocket Vault memory (see green annotated diamonds in FIG. 7A below). MSC-1005, FIG. 7A. In response to determining that the scanned biometric data matches the stored biometric data, the Pocket Vault then transmits its Pocket Vault ID to the network server 114 (see purple annotated rectangle in FIG. 7A below). MSC-1005, FIG. 7A. A check is then performed to ensure that the components used to interface the Pocket Vault 102 with the other components in the network 100 (either wirelessly or directly) are in place and operating correctly. MSC-1005, FIGS. 7A, 7B, ¶[187].

MSC-1003, ¶[69].

BURGER



MSC-1003, ¶[69]; MSC-1005, FIG. 7A.

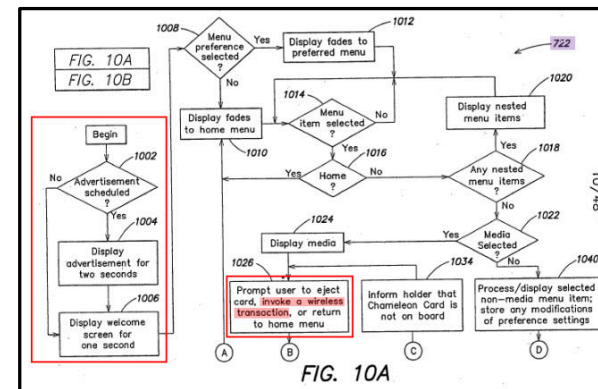
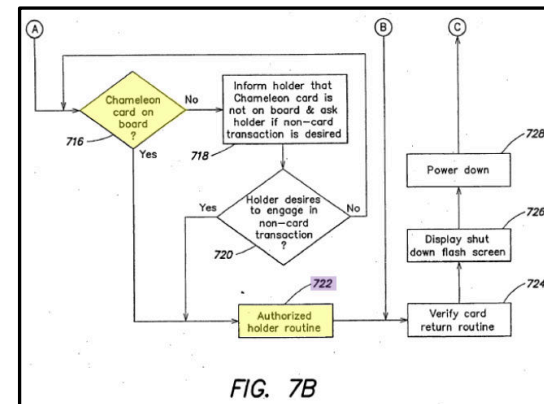
Retail Use Case

Dr. Traynor's 1st Declaration

70. Next, the Pocket Vault holder is granted access to contents of the Pocket Vault 102, and if the Pocket Vault includes a token 102a (also referred to as Chameleon Card), an Authorized Holder Routine (step 722) is performed (see yellow annotations in FIG. 7B below) in which a welcome screen and ads are displayed and a user can select, through a displayed menu, a desire for executing a transaction using the Pocket Vault (see red annotations in FIG. 10A below). See e.g., MSC-1005, step 722 in FIG. 7B, step 1026 in FIG. 10A; steps 1920, 1922 in FIG. 19; ¶¶[320], [189], [158], [95], [96], [125], [236]-[238], [155]-[158].

MSC-1003, ¶[70].

BURGER



MSC-1003, ¶[70]; MSC-1005, FIGS. 7B, 10A.

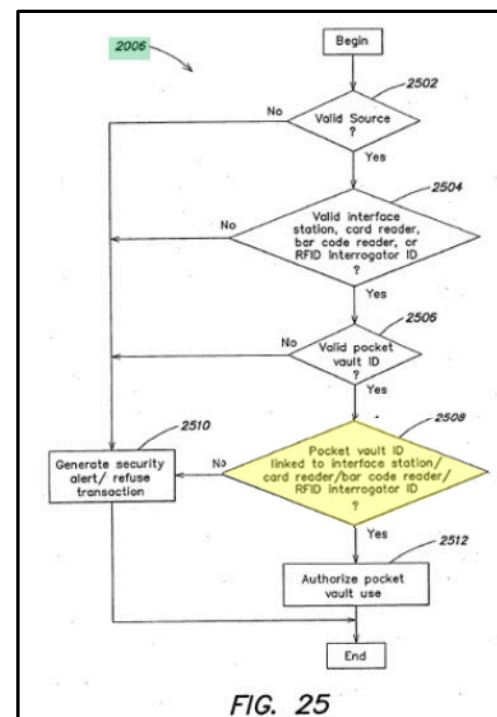
Retail Use Case

Dr. Traynor's 1st Declaration

71. The network server 114 then determines whether the Pocket Vault is authorized to be used, e.g., by checking whether the transmitted Pocket Vault ID matches a stored ID in the network server 114, and then transmits an approval message for the transaction. MSC-1005, FIGS. 19 (steps 1920, 1922), 24 (steps 2006, 2406, 2408), 25 (Steps 2506), ¶¶[0511]-[529], [182].

MSC-1003, ¶[71].

BURGER



MSC-1003, ¶[71]; MSC-1005, FIG. 25.

Retail Use Case

Dr. Traynor's 1st Declaration

71. The network server 114 then determines whether the Pocket Vault is authorized to be used, e.g., by checking whether the transmitted Pocket Vault ID matches a stored ID in the network server 114, and then transmits an approval message for the transaction. MSC-1005, FIGS. 19 (steps 1920, 1922), 24 (steps 2006, 2406, 2408), 25 (Steps 2506), ¶¶[0511]-[529], [182].

MSC-1003, ¶[71].

BURGER

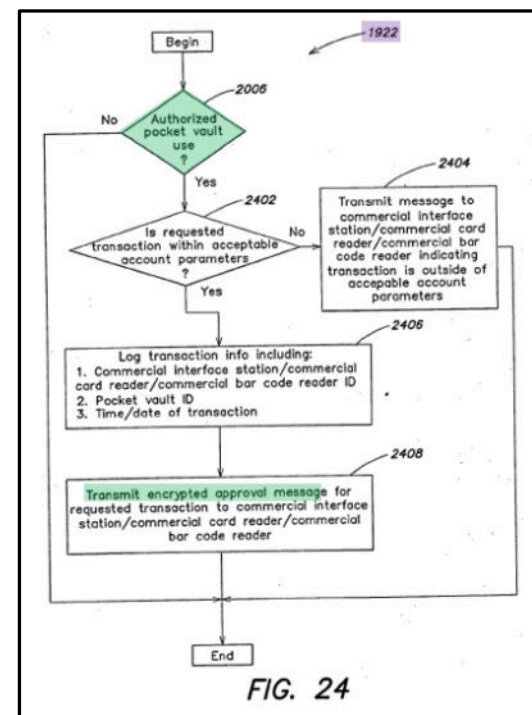


FIG. 24

MSC-1003, ¶[71]; MSC-1005, FIG. 24.

Retail Use Case

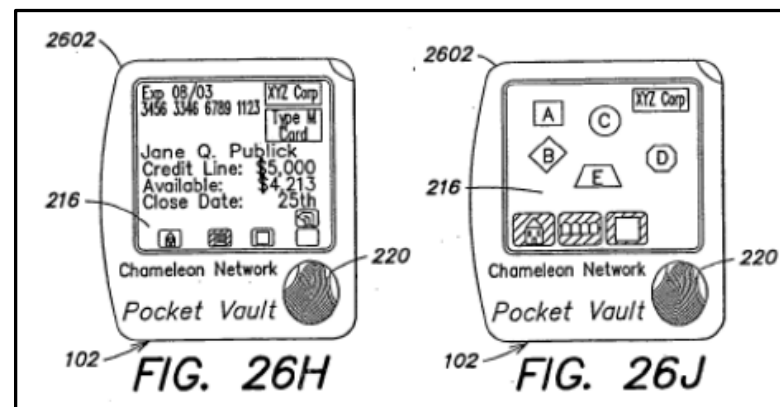
Dr. Traynor's 1st Declaration

screen. In the example of FIG. 26J, the preferred menu immediately shows, perhaps, a selected group of the holder's most frequently used menu items." MSC-1005, ¶[242]. A retailer may verify authenticity by matching the information displayed on the token 102a (or Pocket Vault 102) with that revealed in a swipe or other token reading process." MSC-1005, ¶[158].

73. In the above-described manner, a user or Pocket Vault holder would be able to securely use the Pocket Vault to execute a transaction, such as a financial transaction with a retailer.

MSC-1003, ¶¶[72]-[73].

BURGER



MSC-1003, ¶¶[72]-[73]; MSC-1005, FIGS. 26H, 26J.

Retail Use Case

Dr. Traynor's 1st Declaration

Transaction	First Party	Second Party	Third Party that Operates a Trusted Authority	Trusted Authority	Application
Purchase at Retail Store	Pocket Vault Holder	Retailer	Party Operating the Network Server	Network Server 114, as a whole, or, in some cases, a portion (a controller 402 or database 406) of network server.	Software on Pocket Vault for Providing Credit Card Information

MSC-1003, ¶¶[68]-[73], [105]-[106]; Pet. 17-20, 34-36.

Retail Use Case

Dr. Traynor's 1st Declaration

115. It would have been obvious that an application in the Pocket Vault would have received an access message from the controller 402 of the network server (*"receiving, at an application, an access message from the trusted authority"*) to allow users access to the application after the controller 402 and database 406 of the network server authenticated the Pocket Vault ID that was sent to the network server 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.

MSC-1003, ¶¶115]; Pet. 45, 46.

Burger

manually keyed in. There is no way for this embossing to disappear when it is not needed and appear at just the right time, either with a standard card or a Smartcard. As a result, such numbers are generally in view and this visibility may lead to fraud. In one embodiment, the Pocket Vault 102 may be programmed to conceal this number, unless prompted to the contrary by the holder. A retailer may confirm the kind of credit or debit being presented and the full name on the card, without having to see or be told the account number. On the rare occasion when the number itself is needed, the holder may, for example, repeat the bio-metric input to the Pocket Vault 102 to reveal the card account number. If placed in the personal interface station 104c, such account numbers may be automatically revealed (e.g., through detection of an encrypted cookie on the interface station computer 304 of the personal interface station 104c).

MSC-1005, ¶¶320]; MSC-1003, ¶¶69], [114], [119]; Pet. Rep., 11.

PETITION EXAMPLE 1

Burger's Supports a Financial Media Issuer
Scenario that Renders Claim 1 Obvious

Example 1 According to Burger's Disclosure

Dr. Traynor's 1st Declaration

Transaction	First Party	Second Party	Third Party that Operates a Trusted Authority	Trusted Authority	Application
Obtaining payment information or authorization for charging a credit card or bank account	Pocket Vault Holder	Financial media issuer 112 (e.g., bank or credit card company)	Party operating the network server	The network server 114, as a whole, or, in some cases, a portion (a controller 402 and database 406) of the network server	File or computer software (when a user is involved in a financial transaction with a retailer or credit card company)

MSC-1003, ¶¶[105]-[107], [118]; Pet. 34-36, 52.

PETITION EXAMPLE 2

Burger's Supports a Non-Financial
Media Issuer Scenario that Renders
Claim 1 Obvious

Example 2 According to Burger's Disclosure

Dr. Traynor's 1st Declaration

Transaction	First Party	Second Party	Third Party that Operates a Trusted Authority	Trusted Authority	Application
Obtaining authorization to enter a secure building or facility	Pocket Vault Holder	Non-financial media issuer 110 (e.g., hotel card key issuer, library, building management for company)	Party operating the network server	The network server 114, as a whole, or, in some cases, a portion (a controller 402 and database 406) of the network server	A room key (showing the hotel logo) is downloaded and displayed, and the Pocket Vault can be used to unlock the guest's hotel room

MSC-1003, ¶¶[105]-[107], [118]; Pet. 34-36, 52.

50

Burger's Hotel Example Renders Claim 1 Obvious

Petitioner Reply (Paper 14)

It is clear from the foregoing disclosure that Burger teaches that the user links with the network server 114 to download the key. *Id.* And while linking with the network server 114, the network server 114 sends an encrypted approval message when the Pocket Vault ID is authenticated, as previously explained. MSC-1005, ¶¶[517]-[527], [182]-[186], FIGS. 24, 25. Burger even offers as an option that the network server 114 can store information, such as a website, issued and provided by media issuers (such as a non-financial issuer like a hotel), and provide the website for access to the user, e.g., to download a room key. MSC-1005, ¶¶[365], [371], [381], [467], [539], [556], [559], [560]. Accordingly, Proxense's assertion that because a user, in some cases, downloads the key from a website (and not the network server) is wrong. As noted above and consistent with

Paper 14, 17.

Burger

sensitive media to individual operators. The following typical scenario involves distribution of hotel room key cards to hotel guests who make room reservations over the Internet. Using a hotel's secure web site, the prospective guest, who is also a Pocket Vault holder, may secure a room for a specific time period by providing a credit card number. This step may or may not involve use of a credit card stored on the Pocket Vault 102. If it does involve use of a Pocket Vault credit card, this card may, for example, be accessed while the Pocket Vault 102 is interfaced with the holder's personal interface station 104b. 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). After downloading is complete, the display 216 of the Pocket Vault 102 may

MSC-1005, ¶[679]; Paper 14, 17; Pet., 36, 53, 57.

PETITION EXAMPLE 3

Burger's Supports an Advertising
Scenario that Renders Claim 1
Obvious

Example 3 According to Burger's Disclosure

Dr. Traynor's 1st Declaration

Transaction	First Party	Second Party	Third Party that Operates a Trusted Authority	Trusted Authority	Application
Obtaining advertisement content or related information	Pocket Vault Holder	Advertiser(s) 108	Party operating the network server	The network server 114, as a whole, or, in some cases, a portion (a controller 402 and database 406) of the network server.	A file or computer software containing advertising data is accessed and data therein is displayed. A particular website is accessed and displayed to display advertisement data.

MSC-1003, ¶¶[105]-[107], [118]; Pet. 34-36, 52.

The Network Server is a TPTA Separate from the Application

Petitioner Reply (Paper 14)

Nothing in the '954 patent prevents the third-party trusted authority to store information associated with the first and second party to a transaction. Indeed, if ...
device involved in a transaction. In Burger, simply because the network server 114 stores some information to facilitate a transaction with an advertiser does not mean that the network server 114 is one of the two parties in a transaction involving an advertiser and a user that receives and views advertisements from the advertiser. MSC-1005, ¶¶[111], [117], [237]. Such an understanding is consistent with the Board's decision in IPR2024-00232, which explains that the third-party trusted authority may be an active participant in facilitating a transaction. IPR2024-00232,

Paper 14, 14-15.

54

Example 3 According to Burger's Disclosure

Merriam-Websters Dictionary

a "transaction" is "a communicative action or activity involving two parties or things that reciprocally affect or influence each other" or "an act, process, or instance of transacting."

MSC-1008, 1252; MSC-1003, ¶[113]; Pet. 41-42.

Dr. Traynor's 1st Declaration

disclosure, the party that operates the network server or the controller 402 and database 406 of the network server is "*a third-party that operates a trusted authority*" because there is a transaction involving the display of advertisement content and potential subsequent selection of the advertisement by a user, which is a communicative action or activity involving two parties or things that reciprocally affect or influence each other. For instance, the display of advertisement information impacts the user by conveying information to the user regarding the advertisement. The advertiser 108 also gets publicity, market exposure, and, if the user selects an advertisement, the advertiser can collect information on how useful or impactful the advertisement is. MSC-1012, 2:7-60, FIGS. 4, 8; MSC-1013,

MSC-1003, ¶[113]; Pet. 41-42.

Issue 2

Burger Renders Obvious the “access message”

[1.5] receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values sent to the third party and allowing the user access to the application.

Burger Renders Obvious an Access Message

Dr. Traynor's 1st Declaration

115. It would have been obvious that an application in the Pocket Vault would have received an access message from the controller 402 of the network server (*“receiving, at an application, an access message from the trusted authority”*) to allow users access to the application after the controller 402 and database 406 of the network server authenticated the Pocket Vault ID that was sent to the network server 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.

116. As an alternative mapping, the controller 402 of the network server also transmits an encrypted approval message in operation 2408 after the Pocket Vault 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)). MSC-1005, ¶¶[517]-[527], [182]-[186]. Because this encrypted approval message (*“access message”*) would have been received and processed by software related to the transaction (*“application”*) at the Pocket Vault in response to the Pocket Vault ID being successfully authenticated by the network server, Burger also discloses *“receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values sent to the third party and allowing the user access to the application”* in this additional way. Although operation 2408 indicates that

MSC-1003, ¶¶[115]-[116]; Pet., 45.

Burger's Pocket Vault Provides Security

Burger

[0116] Because of the creation of the above-described trust relationships, each Pocket Vault 102 and each interface station 104 may communicate securely with the network server 114, as well as with any other networked devices or sites that require a high level of trust. Also, the existence of these trust relationships enable individual Pocket Vaults 102 to accept other services provided by the network servers 114,

...

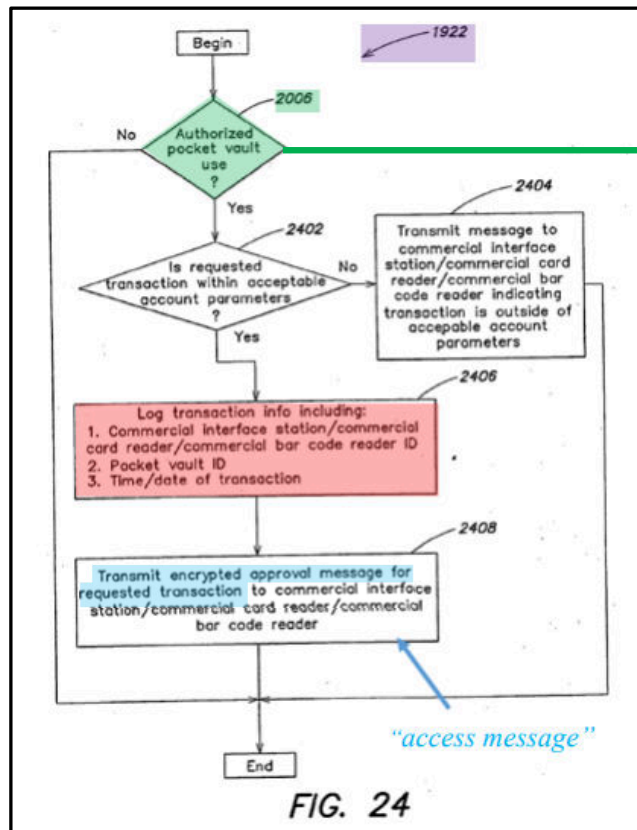
any of the interface stations 104a-c. Therefore, if a Pocket Vault 102 is lost or stolen, the Pocket Vault holder need only obtain a new Pocket Vault 102, and the entire contents of the lost Pocket Vault 102 can be uploaded thereto, in a single communication, in a matter of seconds. In addition, in the event that a validated Pocket Vault 102 is lost or stolen, the network server 114 may void the chip ID of that Pocket Vault 102, so that the Pocket Vault 102 cannot be used by a third party, even if the holder validation security (e.g., the bio-metric scanning or PIN entry requirement) is somehow breached. Voiding the chip ID of the Pocket Vault 102 may, for example, prevent the Pocket Vault 102 from assigning any media information to the associated Chameleon Card.

MSC-1005, ¶[116]; MSC-1003, ¶[109]; Pet. 37-38.

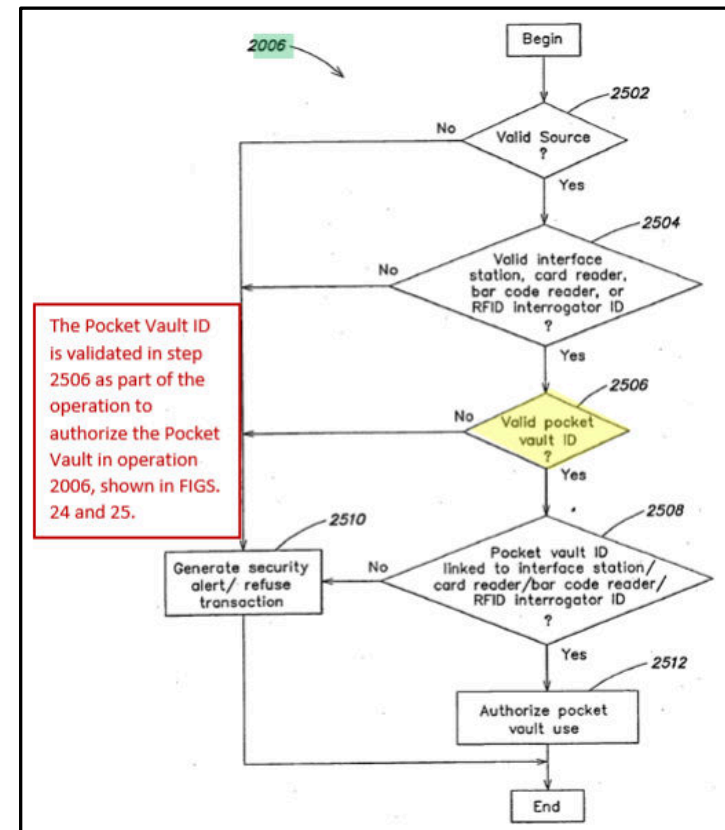
58

Burger Renders Obvious an Access Message

Burger teaches an encrypted approval message



MSC-1005, FIG. 24; Pet., 47-48..



MSC-1005, FIG. 25; Pet., 47-48..

Burger Renders Obvious the “access message”

Dr. Traynor’s 1st Declaration

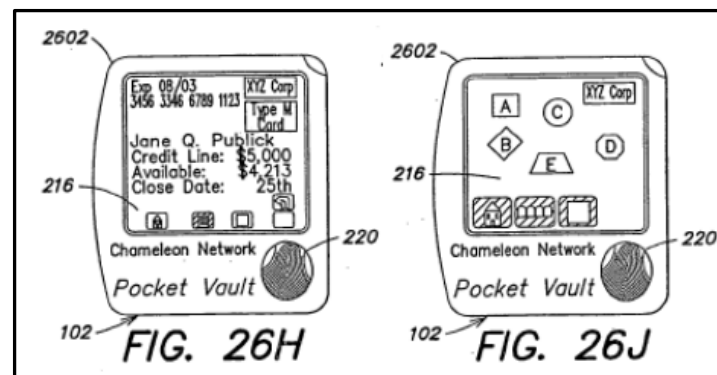
115. It would have been obvious that an application in the Pocket Vault would have received an access message from the controller 402 of the network server (“receiving, at an application, an access message from the trusted authority”) to allow users access to the application after the controller 402 and database 406 of the network server authenticated the Pocket Vault ID that was sent to the network server 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.

MSC-1003, ¶¶[115]; Pet., 45.

118. Note that the ’954 patent explains that an application may be a computer software, file, or financial account. MSC-1001, 6:18-24. Consistent with this description and in view of the above-noted examples, it would have been obvious to a POSITA that Burger renders obvious an “application” in the various ways noted in the table below.

MSC-1003, ¶¶[118]; Pet., 51.

Burger



MSC-1003, ¶¶[72]-[73]; MSC-1005, FIGS. 26H, 26J.

'954 Patent

Application 330 is a resource that can be accessed by a verified and authenticated user. Application 330 can be, for example, a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file, a financial account (e.g. a savings account, checking account, brokerage account, credit card account, credit line, etc.) and the like. In one embodiment, a file

MSC-1001, 6:18-24; Pet., 51.

Burger Renders Obvious an Access Message

It would have been obvious that Burger uses an Access Message in each of the Use Cases

Use Case	Transaction	First Party	Second Party	Third Party that Operates a Trusted Authority	Trusted Authority	Application
Retail	Purchase at Retail Store	Pocket Vault Holder	Retailer	Party operating the network server	The network server 114, as a whole, or, in some cases, a portion (a controller 402 and database 406) of the network server.	Software on Pocket Vault for Providing Credit Card Information
2	Obtaining authorization to enter a secure building or facility	Pocket Vault Holder	Non-financial media issuer 110 (e.g., hotel card key issuer, library, building management for company)	Party operating the network server	The network server 114, as a whole, or, in some cases, a portion (a controller 402 and database 406) of the network server.	A room key (showing the hotel logo) is downloaded and displayed, and the Pocket Vault can be used to unlock the guest's hotel room.
3	Obtaining advertisement content or related information	Pocket Vault Holder	Advertiser(s) 108	Party operating the network server	The network server 114, as a whole, or, in some cases, a portion (a controller 402 and database 406) of the network server.	A file or computer software containing advertising data is accessed and data therein is displayed. A particular website is accessed and displayed to display advertisement data.

Thank you

Questions?