

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICROSOFT CORPORATION,
Petitioner,

v.

PROXENSE, LLC,
Patent Owner.

IPR2024-00846
Patent 8,886,954 B1

Before THU A. DANG, KEVIN F. TURNER, and DAVID C. McKONE,
Administrative Patent Judges.

McKONE, *Administrative Patent Judge.*

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

A. Background and Summary

Microsoft Corp. (“Petitioner”) filed a Petition (Paper 2, “Pet.”) requesting *inter partes* review of claims 1–29 of U.S. Patent No. 8,886,954 B1 (Ex. 1001, “the ’954 patent”). Pet. 1. Proxense, LLC (“Patent Owner”) filed a Preliminary Response (Paper 7, “Prelim. Resp.”). The Board instituted an *inter partes* review of the challenged claims pursuant to 35 U.S.C. § 314. Paper 8 (“Inst. Dec.”).

After institution, Patent Owner filed a Patent Owner Response (Paper 10, “PO Resp.”), Petitioner filed a Reply (Paper 14, “Reply”), and Patent Owner filed a Sur-reply (Paper 17, “Sur-reply”). The parties then presented oral arguments via a (video) Hearing (August 18, 2025), and the Board entered a Hearing transcript into the record (Paper 31, “Tr.”).

For the reasons set forth in this Final Written Decision pursuant to 35 U.S.C. § 318(a), we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 1–29 are unpatentable.

B. Related Matters

The parties advise us that the ’954 patent is involved in three district court cases, including *Proxense, LLC v. Microsoft Corp.*, Case No. 6:23-cv-00319 (W.D. Tex.). Pet. 107; Paper 5, 2. Petitioner also has filed petitions for *inter partes* review of patents related to the ’954 patent, including IPR2024-00775 (challenging U.S. Patent No. 8,352,730 B2 (“the ’730 patent”); terminated after Patent Owner request for adverse judgment) and IPR2024-00776 and IPR2024-01335 (both challenging U.S. Patent No. 9,298,905 B1 (“the ’905 patent”); both dismissed or terminated after Patent Owner’s request for adverse judgment). The ’730 patent also was the

subject of *Samsung Electronics America, Inc. v. Proxense LLC*, IPR2021-01444 (PTAB) (institution denied). The '954 patent also was the subject of *Google LLC v. Proxense, LLC*, IPR2024-00233 (PTAB) (final written decision determining all challenged claims unpatentable), *Microsoft Corp. v. Proxense, LLC*, IPR2024-01327 (PTAB) (institution denied), and *Apple Inc. v. Proxense, LLC*, IPR2024-01334 (PTAB) (petitioner joined to IPR2024-00233). Pet. 107; Paper 5, 2. The '730 patent also was the subject of *Apple Inc. v. Proxense, LLC*, IPR2024-00232 (terminated after Patent Owner's request for adverse judgment).

Patent Owner states that patents related to the '954 patent are the subject of *ex parte* reexaminations in Application No. 90/015,052 ("the '052 reexam"), reexamining the '730 patent (currently pending), Application No. 90/015,053, reexamining the '905 patent (reexamination certificate cancelling all claims), and Application No. 90/015,054, reexamining U.S. Patent No. 10,698,989 (reexamination certificate cancelling all claims). Paper 24, 3–4.

C. The '954 Patent

The '954 patent discloses systems for "authentication responsive to biometric verification of a user being authenticated," using "an integrated device [that] includes a persistent storage to persistently store[] a code such as a device identifier (ID) and biometric data for a user in a tamper-resistant format." Ex. 1001, 1:60–65. The '954 patent states that "[c]onventional user authentication techniques," such as requiring input of a password, were deficient because they "require[d] the user to memorize or otherwise keep track of the credentials" and "it can be quite difficult to keep track of them all." *Id.* at 1:26–35. Other techniques, such as "provid[ing] the user with an

access object . . . that the user can present to obtain access,” were inadequate because “authentication merely proves that the access object itself is valid; it does not verify that the legitimate user is using the access object.” *Id.* at 1:36–46. According to the ’954 patent, there was a need in the art for a system for “verifying a user that is being authenticated that does not suffer from [such] limitations” and “ease[s] authentications by wirelessly providing an identification of the user.” *Id.* at 1:52–56.

Figure 2 of the ’954 patent is reproduced below.

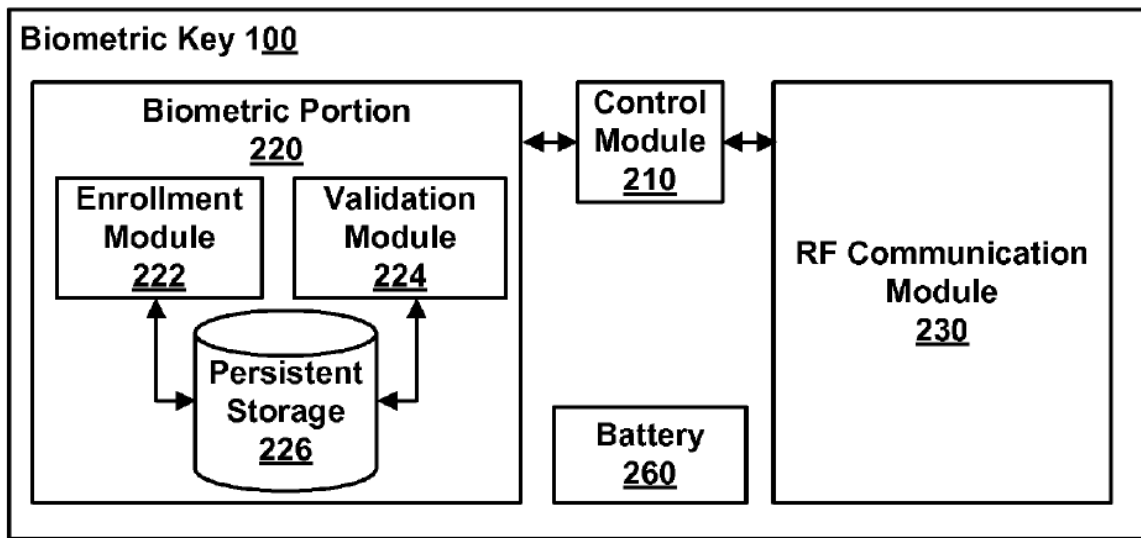


FIG. 2

Figure 2 is a block diagram of the functional modules of a biometric key. *Id.* at 3:28–30. Enrollment module 222 registers a user with biometric key 100 by persistently storing biometric data associated with the user (e.g., a digital image of the retina, fingerprint, or voice sample) in persistent storage 226. *Id.* at 4:64–5:21. Enrollment module 222 registers biometric key 100 with a trusted authority by providing a code, such as a device ID, to the trusted authority or, alternatively, the trusted authority can provide a code to biometric key 100. *Id.* at 5:1–5. The code is stored in persistent

storage 226. *Id.* at 5:36–38. “Persistent storage 226 is itself, and stores data in, a tamper-proof format to prevent any changes to the stored data.” *Id.* at 5:29–31. “Tamperproofing increases reliability of authentication because it does not allow any changes to biometric data (i.e., allows reads of stored data, but not writes to store new data or modify existing data).” *Id.* at 5:31–34. In a fingerprint embodiment, validation module 224 uses scan pad 120 (shown in Figure 1) to capture scan data from the user’s fingerprint and compares the scanned data to the stored fingerprint to determine whether the scanned data matches the stored data. *Id.* at 5:6–15.

The interaction of biometric key 100 with other system components is illustrated in Figure 3, reproduced below.

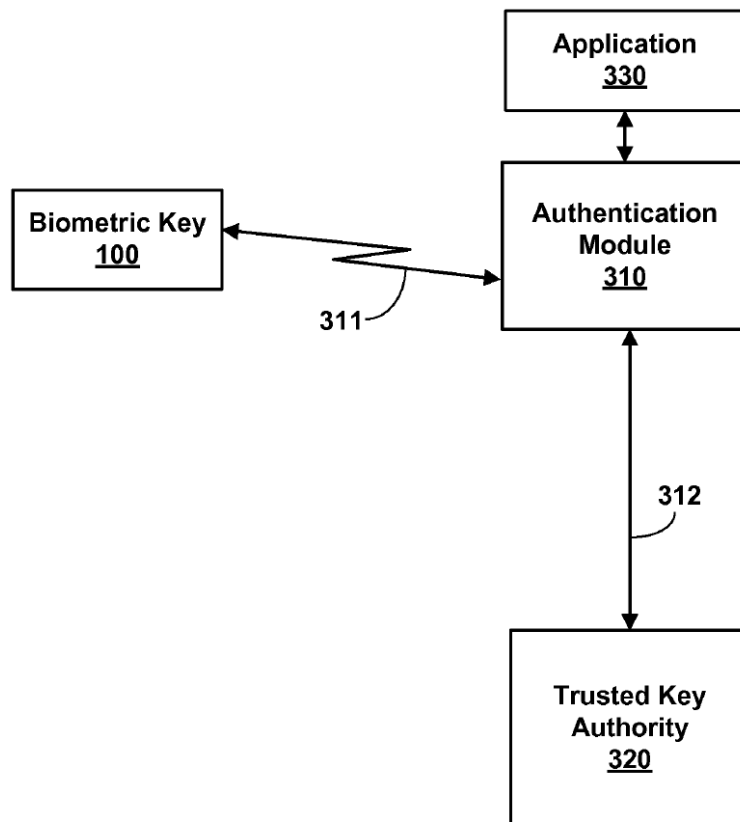


FIG. 3

Figure 3 is “a block diagram illustrating a system for providing authentication information for a biometrically verified user.” *Id.* at 3:31–33. Authentication module 310 is coupled to biometric key 100 via line 311 (a wireless medium) and with trusted key authority 320 via line 312 (a secure data network such as the Internet). *Id.* at 6:1–5. Authentication module 310 requires the device ID code (indicating successful biometric verification) from biometric key 100 before allowing the user to access application 330. *Id.* at 6:5–11. Authentication module 310 provides the device ID code from biometric key 100 to trusted key authority 320 to verify that it belongs to a legitimate key. *Id.* at 6:11–14; *see also id.* at 6:37–43 (“In one embodiment, trusted key authority 320 verifies that a code from a biometric key is legitimate. To do so, the trusted key authority 320 stores a list of codes for legitimate biometric keys In one embodiment, trusted key authority 320 can also store a profile associated with a biometric key.”). Authentication module 310 then sends a message to application 330 to allow the user access to the application responsive to a successful authentication by trusted key authority 320. *Id.* at 6:15–17.

“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, . . . and the like.” *Id.* at 6:19–24. Trusted key authority 320 can be operated by an agent, such as “a government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness.” *Id.* at 7:30–33. “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.” *Id.* at 7:33–36.

Claim 1, reproduced below,¹ is illustrative of the claimed subject matter:

1. A method comprising:
 - [1.1] 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;
 - [1.2] responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;
 - [1.3] comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;
 - [1.4] 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
 - [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.

¹ We add bracketed alphanumeric characters corresponding to those Petitioner uses in the Petition.

D. Evidence

Petitioner relies on the references listed below.

Name	Reference	Date	Exhibit No.
Burger	US 2005/0050367 A1	Mar. 3, 2005 (filed Sept. 30, 2004)	1005
Robinson	US 2003/0177102 A1	Sept. 18, 2003	1006
Orsini	US 2004/0049687 A1	Mar. 11, 2004	1021

Petitioner also relies on the Declaration of Patrick Traynor, Ph.D. (Ex. 1003) and the Supplemental Declaration of Dr. Traynor (Ex. 1033).

E. The Asserted Grounds of Unpatentability

We instituted a trial under the following grounds (Inst. Dec. 8):

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

II. ANALYSIS

A. Claim Construction

We construe a claim

using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b),

² The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”), amended 35 U.S.C. § 103. Because the ’954 patent has an effective filing date before the effective date of the relevant provision of the AIA, we cite to the pre-AIA version of § 103.

including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.

37 C.F.R. § 42.100(b); *see also Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

Independent claims 1, 12, 16, and 22 each recite “a third party that operates a trusted authority.”³ In our Institution Decision, we preliminarily construed this term “based on the ordinary meaning . . . , namely, ‘a trusted authority that is an entity separate from the parties to a transaction.’” Dec. 11. We declined to construe any other terms, including “access message.” *Id.* at 11–12.

As to our construction of “third party that operates a trusted authority,” “Patent Owner does not dispute this construction,” but does “dispute[] the implicit construction of the *transaction* and the *principal parties* thereto.” PO Resp. 2. Patent Owner argues that, rather than challenging our construction of “third party that operates a trusted authority,” “Patent Owner is merely attempting to construe the *transaction* and the *principal parties* thereto, which limit the scope of ‘third-party

³ The parties also refer to this term as “third party trusted authority.” The ’730 patent, a parent of the ’954 patent, was the subject of *Samsung Electronics America, Inc. v. Proxense LLC*, IPR2021-01444 (PTAB) (institution denied). *See* Ex. 1007 (IPR2021-01444, Paper 11 (PTAB Feb. 28, 2022) (“Samsung DDI”). In the Samsung DDI, the Board construed “third-party trusted authority” to mean “a trusted authority that is an entity separate from the parties to a transaction.” Ex. 1007, 15. Patent Owner appears to contend that “third party that operates a trusted authority,” recited in the ’954 patent claims, has the same meaning as “third-party trusted authority,” recited in the ’730 patent claims. Petitioner does not appear to dispute this. We treat these terms as equivalent.

trusted authority.” *Id.* Specifically, Patent Owner argues, “[t]he claims . . . 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.” *Id.* at 3; *accord id.* at 5 (“‘Third-party trusted authority,’ therefore, cannot be construed to encompass third parties to transactions other than those in which the principal parties are a user being allowed access and an application being accessed, and the underlying transaction is allowing a user access to an application.”), 7 (“[T]he ‘third-party trusted authority’ is limited to a third-party with respect to a user being allowed access to an application and the application being accessed.”).

In our Final Written Decision in IPR2024-00233 (Paper 35, “’233 FWD”), we “maintain[ed] our construction of ‘a third party that operates a trusted authority,’ namely, ‘a trusted authority that is an entity separate from the parties to a transaction,’” and made clear that “[s]uch a transaction is not limited to those in which the application being accessed is a party.” ’233 FWD, 15. In reaching this conclusion, we found that “the plain language of claim 1 does not limit the parties to a transaction between the user and an application, or require that one of the parties to a transaction be the application ultimately accessed.” *Id.* at 11. We further found nothing in the intrinsic evidence that departed from the ordinary meaning, either through lexicography or disavowal of the full claim scope. *Id.* at 12–14 (citing Ex. 1001⁴, 2:35–48, 5:65–67, 6:8–34, 6:45–55, 6:64–7:4, 8:12–16, Figs. 3, 4, 7). Thus, in IPR2024-00233, we essentially rejected the modifications to our construction that Patent Owner advances in the Patent Owner Response.

⁴ The ’954 patent is Exhibit 1001 in both this proceeding and in IPR2024-00233.

In the Sur-reply, which post-dated the '233 FWD, Patent Owner states that “[t]he claims at issue have been construed in [the '233 FWD]” and, “[w]ithout forfeiting any right of appeal, Patent Owner believes that construction is binding upon these proceedings.” Sur-reply 1.

For the same reasons, and based on the same evidence, given in the '233 FWD, we maintain our construction of “a third party that operates a trusted authority,” namely, “a trusted authority that is an entity separate from the parties to a transaction,” and make clear that such a transaction is not limited to those in which the principal parties are the user being allowed access and the application being accessed.

Based on the complete record, we do not find it necessary to provide express claim constructions for any other terms. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (noting that “we need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy’”) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

B. Obviousness of Claims 1, 2, 4, 5, 7–13, 15, 16, 18–24, and 26–29 over Burger

Petitioner contends that claims 1, 2, 4, 5, 7–13, 15, 16, 18–24, and 26–29 would have been obvious over Burger. Pet. 22–89. For the reasons given below, Petitioner has made a sufficient showing.

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are “such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” We resolve the question of obviousness on the basis of

underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) if in evidence, objective evidence of nonobviousness, i.e., secondary considerations.⁵ *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

1. Level of skill in the art

Neither party takes a position on the level of ordinary skill in the art. The description of the technology in the Specification, as well as the cited prior art, suggests that a skilled artisan would have been an experienced electrical or computer engineer.

2. Scope and content of the prior art – overview of Burger

Burger describes a method and system “for producing, distributing, storing, and using the typical contents of a person’s wallet, as well as the multiple, separate transaction authorization devices, e.g., RFID tags, owned by the person.” Ex. 1005 ¶ 93. “[T]he device may be more appropriately referred to as a multi-purpose, ‘point-of-transaction’ device.” *Id.* ¶ 94. Figure 1, reproduced below, illustrates an example:

⁵ The record does not include allegations or evidence of objective indicia of nonobviousness.

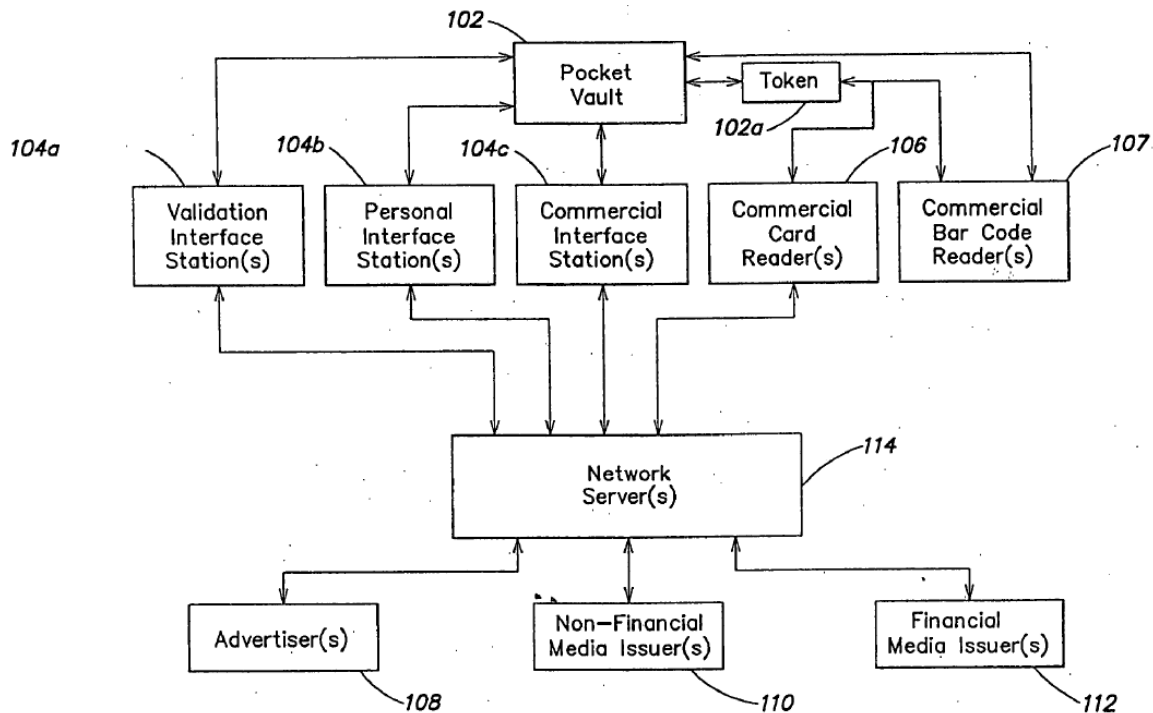


FIG. 1

Figure 1 is a block diagram of a network system in which a portable electronic authorization device (a “pocket vault”) is used. *Id.* ¶ 51.

In network system 100, pocket vault 102, associated token 102a, and network server 114 communicate with interface stations 104a–104c, commercial card readers 106, and commercial bar code readers 107. *Id.* ¶¶ 96–98, 100. Network server 114 also is coupled to advertiser computers 108, non-financial media issuers 110, and financial media issuers 112. *Id.* ¶ 98. Pocket vault 102 can be equipped to generate token 102a such that the token has transactional information such as an actual or simulated magnetic stripe or bar code so that the token can be used by the user to engage in a transaction through card reader 106 or bar code reader 107. *Id.* ¶ 103. A trust relationship may be established between pocket vault 102 and network server 114; for example, a unique encrypted chip ID of pocket vault 102 may be registered with network server 114. *Id.* ¶ 114.

Figure 2 is reproduced below:

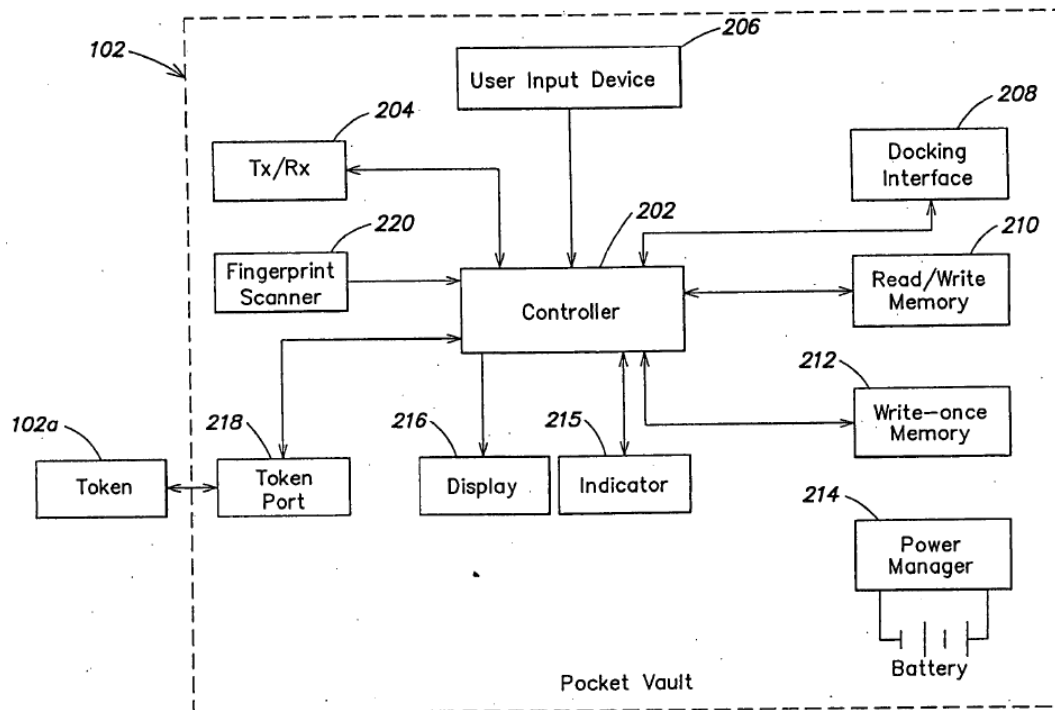


FIG. 2

Figure 2 is a block diagram of pocket vault 102. *Id.* ¶ 52. Pocket vault 102 includes controller 202, memory 210, write-once memory 212, and fingerprint scanner 220.⁶ *Id.* ¶ 118. Controller 202 includes a software-programmable and encryption protected or hard-wired unique chip ID that is released from pocket vault 102 only after fingerprint scanner 220 successfully authenticates the identity of the pocket vault's holder. *Id.* ¶ 122. Memory 210 can store various media and personal information (debit/credit cards, drivers licenses, passports, building security, etc.). *Id.* ¶¶ 127–129. Write-once memory 212 stores the user's fingerprints (or other biometric data). *Id.* ¶ 182. When the user applies a finger to fingerprint scanner 220, pocket vault 102 is authenticated by comparing the

⁶ Burger contemplates other forms of biometric data, such as “retina scan, a speech pattern analysis, keystroke rhythm, etc.” *Id.* ¶ 112.

fingerprint from scanner 220 to the fingerprint stored in fingerprint memory 212. *Id.* ¶¶ 178–184, 209–210, Figs. 7A, 8A. When it is determined that pocket vault 102 has been properly authenticated, pocket vault 102 transmits an encrypted message with the unique pocket vault chip ID to an interface unit such as interface stations 104a–104c. *Id.* ¶¶ 186, 474, Figs. 7A, 8A, 19.

Figures 24 and 25 are reproduced below:

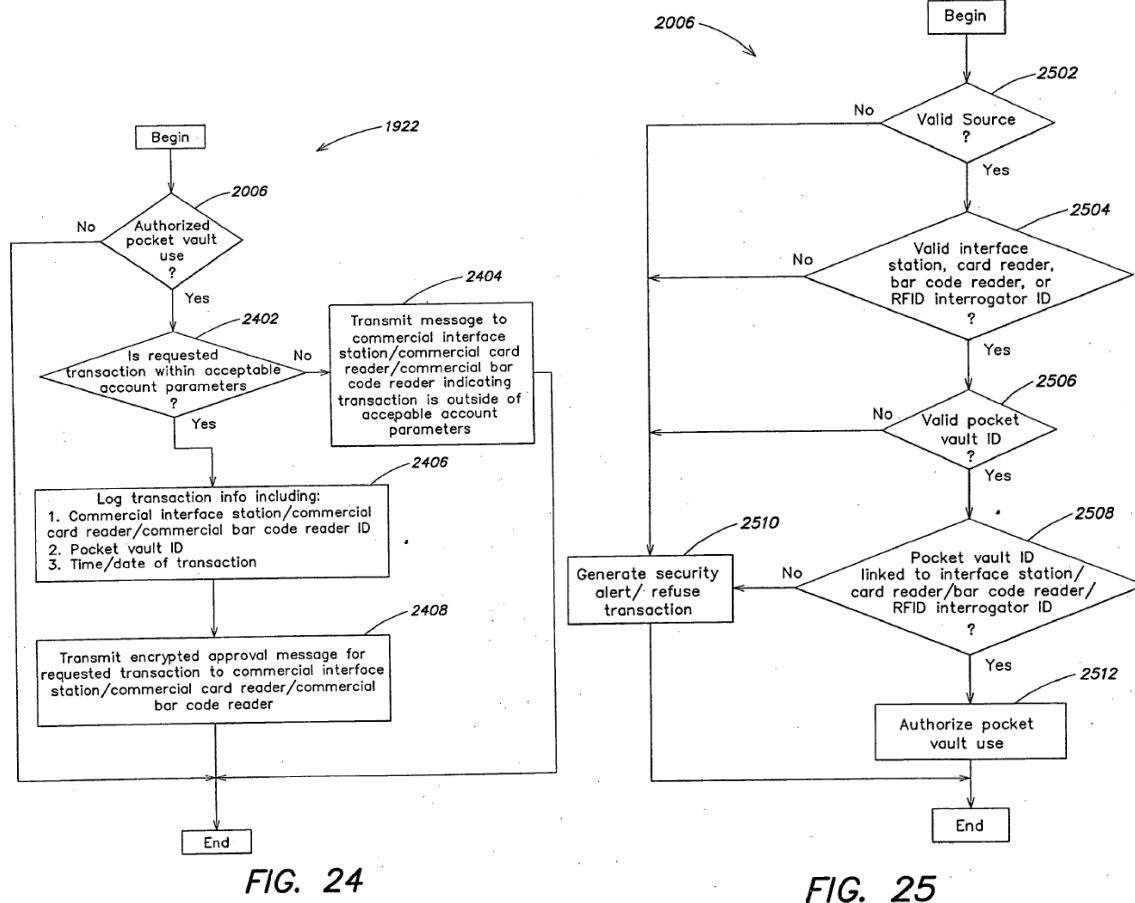


Figure 24 is a flow diagram of a process to request authorization of a transaction. *Id.* ¶ 74. Figure 25 is a flow diagram of the “authorized pocket vault use?” step 2006 of Figure 24. *Id.* ¶ 75. After network server 114 receives a request to authorize a transaction from an interface unit, the network server determines that the entity with which the user is attempting to transact (e.g., a point-of-sale terminal) is valid and properly linked

(steps 2502–2504) and determines that the pocket vault ID is valid (step 2506). *Id.* ¶¶ 473–474, 511–512, 520–525, Figs. 19, 24, 25. Network server 114 then determines that the pocket vault ID is linked to the ID of the commercial interface station 104, card reader 106, or barcode reader 107 and, if so, determines that the pocket vault use is authorized (steps 2508, 2512). *Id.* ¶¶ 527, 529. The network server then determines “whether the requested transaction is within acceptable account parameters (e.g., as set by the media issuer)” and, if so, logs the transaction and transmits an encrypted approval message to the entity with which the transaction is being attempted (e.g., interface station 104, card reader 106, barcode reader 107). *Id.* ¶¶ 514–518.

In one example, network server 114 may serve as a repository for information regarding advertisers 108, and may serve as a conduit for advertisers to target particular classes of pocket vault holders and channel information to them. *Id.* ¶ 117. Figure 10A, reproduced below, illustrates an example:

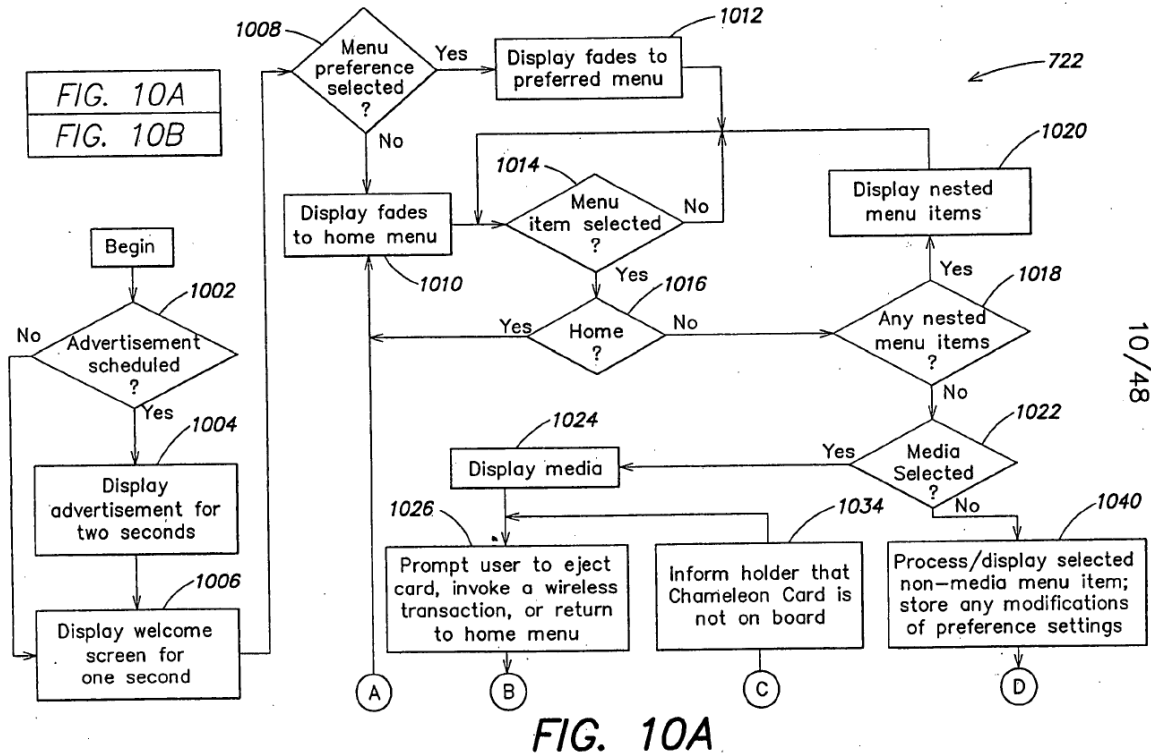


FIG. 10A

Figure 10A is a flow diagram of an authorized holder routine executed by controller 202 of pocket vault 102. *Id.* ¶¶ 57, 60, Fig. 2. Advertiser 108 can make arrangements with the company operating network server 114 to have certain advertisements uploaded to pocket vault 102 when it interfaces with personal interface station 104b. *Id.* ¶ 237. When it is determined that an advertisement is scheduled for display on pocket vault 102 (step 1002), the scheduled advertisement is displayed (e.g., for two seconds) (step 1004). *Id.* ¶¶ 237–238, Fig. 26I.

In another example, the user uses pocket vault 102 to access a hotel room. *Id.* ¶ 679. In this example, the user secures a room using a credit card, and

the prospective hotel guest may link to the network server 114 (while staying within the hotel's website), and follow onscreen 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).

Id. Pocket vault 102 can then encode token 102a with magnetic stripe coding to unlock the hotel room. *Id.*

3. *Differences, if any, between claims 1, 2, 4, 5, 7–13, 15, 16, 18–24, and 26–29 and Burger; reasons to modify*

a) *Claim 1: uncontested limitations*

Petitioner contends that Burger teaches a method for verifying a pocket vault holder during authentication of the pocket vault used in transactions involving financial and non-financial media. Pet. 22–23 (citing Ex. 1005 ¶¶ 2, 10, 127–128; Ex. 2003 ¶ 89). We agree.

As to claim limitation 1.1,

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,

we agree with Petitioner and find that Burger’s pocket vault 102 is “an integrated device.” *Id.* at 23 (citing Ex. 1005 ¶¶ 94–95, 118, 134, Fig. 2; Ex. 1003 ¶ 90). We also agree with Petitioner and find that write-once memory 212, a storage element that is not capable of being subsequently altered, persistently stores biometric data of the user, and that other hard-wired memory stores a pocket vault ID and encryption/decryption information. *Id.* at 24–27 (citing Ex. 1005 ¶¶ 112, 114, 118, 127, 129, 154, 182, 551–552, Fig. 2; Ex. 1003 ¶¶ 22–23, 91–96). Dr. Traynor testifies that it would have been obvious to implement the hard-wired memory as

protected, write-once memory so that sensitive information that is not subject to change (e.g., device ID, encryption information) is kept secure and not tampered with. Ex. 1003 ¶ 98. We credit this uncontroverted testimony.

As to claim limitation 1.2, “responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan,” we agree with Petitioner and find that the user applying a finger to Burger’s fingerprint scanner 220 (or other physical action pursuant to a different type of biometric data) is a request for a biometric verification of the user and that responsive to this request, fingerprint scanner 220 scans the applied fingerprint and controller 202 receives the scan data. Pet. 28–30 (citing Ex. 1005 ¶¶ 112, 135, 178–182, Figs. 2, 7A; Ex. 1003 ¶¶ 99–100).

We agree with Petitioner and find that Burger’s description of pocket vault 102 comparing the biometric data stored in write-once memory 212 to the scan data from fingerprint scanner 220 teaches claim limitation 1.3, “comparing the scan data to the biometric data to determine whether the scan data matches the biometric data.” *Id.* at 30–31 (citing Ex. 1005 ¶¶ 182–184, Figs. 2, 7A; Ex. 1003 ¶ 101).

Patent Owner does not contest that Burger teaches limitations 1.1–1.3 of claim 1.

b) Claim 1: “third party that operates a trusted authority” and “application”

The parties dispute whether Burger teaches a “third party that operates a trusted authority,” as recited in claim limitation 1.4 (emphasis added), 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.

Petitioner argues that, after pocket vault 102 authenticates the user's biometric data, pocket vault 102 wirelessly sends an encrypted message including the pocket vault chip ID, ultimately to network server 114, which acts as a third-party trusted authority. Pet. 32–34 (citing Ex. 1005 ¶¶ 97, 99–101, 113–114, 122–123, 146, 183–184, 186, 209–210, Figs. 1, 7A; Ex. 1003 ¶¶ 96–99). Petitioner argues that network server 114 maintains a list of current pocket vault holders, identified by chip ID and linked to the list of holders and, thus, establishes a trust relationship between it and pocket vault 102. *Id.* at 44–45 (citing Ex. 1005 ¶¶ 114, 116, 146, Fig. 4; Ex. 1003 ¶ 109). We find that Petitioner's evidence shows that Burger teaches these aspects of claim limitation 1.4, and Patent Owner does not contest this.

Petitioner argues that network server 114 acts as a third party that operates a trusted authority in three example transactions described in Burger, a credit card transaction, an advertisement displayed at the pocket vault, and an electronic hotel room key. For each of these examples, the parties' disagreement centers around an identification of the application to be accessed and the party, beyond the user, who is the other primary party to the transaction. Because the parties' disputes are as to the transactions as wholes, we evaluate claim limitation 1.4 along with claim limitation 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.”

*(1) third party that operates a trusted authority; first theory
(credit card transactions)*

In Petitioner's first asserted example transaction, as to claim limitation 1.5, Petitioner argues that, after Burger's network server 114 authenticates the user's pocket vault ID, the user is granted access to pocket vault 102 and can select a transaction from a displayed menu. Pet. 42–44 (citing Ex. 1005 ¶¶ 95–96, 103, 125, 155–158, 189, 236–238, 320, Figs. 7B, 10A, 19; Ex. 1003 ¶ 114). Burger describes, for example, that “Pocket Vault 102 may be equipped to generate the token 102a such that the token 102a has transactional information regarding a media (e.g., an actual or simulated magnetic stripe or a bar code) produced thereon.” Ex. 1005 ¶ 103. “[T]he token 102a may be used by the Pocket Vault holder to engage in a transaction wherein an entity swipes the magnetic stripe portion of the token 102a through a card reader 106 or scans the bar code on the token 102a using a bar code reader 107.” *Id.* In cases where the retailer needs to see the credit or debit card number, “the holder may, for example, repeat the biometric input to the Pocket Vault 102 to reveal the card account number,” and “[i]f placed in the personal interface station 104c, such account numbers may be automatically revealed.” *Id.* ¶ 320; *see also id.* ¶¶ 157–158).

In this example, Petitioner argues, pocket vault 102, or token 102a coupled to it, displays credit card information to be used by a retailer in a transaction. Pet. 42–43 (citing Ex. 1005 ¶¶ 95, 155–158, 320; Ex. 1003 ¶ 114). Dr. Traynor testifies that it would have been obvious that pocket vault 102 would have received an access message from network server 114 in order for pocket vault 102 to grant access to the user and display credit card information. Ex. 1003 ¶ 115.

In an “alternative mapping” of this example, Petitioner argues that the encrypted approval message from network server 114 can be transmitted to an interface station (e.g., 104c, 106, 107). Pet. 45–48 (citing Ex. 1005 ¶¶ 101, 182–186, 517–527, Figs. 24, 25; Ex. 1003 ¶ 116). Dr. Traynor testifies that it would have been obvious that the encrypted approval message from network server 114 could be sent to the pocket vault 102 in addition to or instead of interface stations 104c, 106, 107. Ex. 1003 ¶ 116.

In either mapping of Petitioner’s first example, and pursuant to claim limitation 1.5, the “application” that is accessed is “a file” or computer software that stores credit card information. Pet. 52–53 (citing Ex. 1005 ¶¶ 94–96, 125–129, 155–158, 189, 242, 517–527, Figs. 7B, 10A, 19, 26H–26K). As to claim limitation 1.4, Petitioner argues that the first party to the transaction is the user of pocket vault 102, the second party is either the retailer or financial media issuer 112 (e.g., a bank or credit card company), and the third party, a third party that operates a trusted authority, is network server 114 and the party that operates it. *Id.* at 34–35, 38–39 (citing Ex. 1005 ¶¶ 95, 158, 320, 511–513, Figs. 19, 24, 25, 27; Ex. 1003 ¶ 110).

As to Petitioner’s first mapping of this example, the pocket vault presenting via magnetic stripe or displaying a credit card number to a retailer, Patent Owner argues that “[n]either the Petition nor Dr. Traynor offer anything more than a conclusory statement devoid of any articulated reasoning and rational underpinning” for why it would have been obvious for the pocket vault to receive an access message before displaying sensitive credit or debit card information to conduct a transaction. PO Resp. 7–8.

We find that, after Burger’s network server 114 authenticates a user’s pocket vault ID, the user is granted access to pocket vault 102 and can select a transaction from a displayed menu, including use of a credit card.

Ex. 1005 ¶ 242, Fig. 26H. It is straightforward and logical that the user's subsequent access to that credit card information, either by displaying it or through token 102a, is because network server 114 sent a communication to pocket vault 102 indicating that it successfully authenticated the pocket vault. Ex. 1003 ¶ 115. This is the obvious inference a skilled artisan would have drawn from Burger's description of authenticating the pocket vault and subsequently allowing credit card information to be used. Thus, we find that, in this example, the operator of network server 114 is a third party that operates a trusted authority, the principle parties to the transaction are the user of pocket vault 102 and the retailer, and a message from network server 114 to pocket vault 102 allowing the credit card to be used (displayed or encoded in the token) is an access message allowing the user access to the application (file with credit card information). Accordingly, we find that this example of Burger teaches claim limitations 1.4 and 1.5.

As to Petitioner's alternative mapping, network server 114 transmitting an encrypted approval message to an interface station (or to pocket vault 102 in Petitioner's modification of this example), Patent Owner argues that an approval message in the context of Burger is an indication that funds have been secured after an authorization process has been conducted and it is determined that the transaction is within acceptable parameters set by the issuing bank. PO Resp. 8–14 (citing Ex. 1005 ¶¶ 320, 473–474, 511, 514, 517–518, Fig. 24; Ex. 2010 (PayPal article, "How online payment processing works"); Ex. 2011 (Stripe article, "How credit card transaction processing works: A quick guide"); Ex. 2012 (PayPal article, "How PayPal helps sellers process and accept credit card payments"); Ex. 2013 (Stripe article, "Card authorization explained: How it works and what businesses need to know")). Thus, Patent Owner argues, "the transaction of 'obtaining

payment information or authorization for charging a credit card or bank account’ solely is performed by the Pocket Vault and the Pocket Vault Server 114,” and the financial media issuer is not a participant or party to the transaction. Sur-reply 4. In this example, Patent Owner argues, the transaction is between only two parties and lacks a third party. *Id.*

Petitioner responds by clarifying that, in this example, “the ‘second party’ is a financial media issuer 12, such as a bank or credit card company” and “the ‘third party’ is a party that operates the network server.” Reply 10. Petitioner argues that Patent Owner “conflates the ‘approval’ for charging a financial account in a transaction, with an approval to use sensitive information to ultimately conduct a financial transaction—the latter of which was articulated in the Petition.” *Id.* at 10–11 (citing Pet. 45). Here, it is Petitioner who is conflating its two separate mappings of this example. Patent Owner’s argument is directed to Petitioner’s alternative mapping, in which the network server 114 determines whether a “requested transaction [is] within acceptable account parameters” and, if so, transmits an “encrypted approval message for [the] requested transaction to commercial interface station/commercial card reader/commercial bar code reader.” Ex. 2005 ¶¶ 514, 517–518, Fig. 24 (2402, 2408). We agree with Patent Owner that this appears to be a transaction in which network server 114 determines whether the transaction is within the financial institution’s parameters and sends an authorization message to the pocket vault indicating that funds can be transferred. Petitioner does not explain persuasively why the financial institution is the second party to the transaction and the network server is a third party, since the network server appears to be playing the role of the financial institution. Thus, Petitioner has not shown that the alternative mapping of this example teaches claim limitations 1.4 and 1.5.

*(2) third party that operates a trusted authority; second theory
(advertising)*

In another example, Petitioner argues, Burger describes that pocket vault 102 receives and displays, on its screen, an advertising message from advertiser 108 via network server 114. Pet. 39–41 (citing Ex. 1005 ¶¶ 117, 146, 189–195, 236–238, 541, Figs. 1, 10, 11; Ex. 1003 ¶¶ 111–112), 48–51 (citing Ex. 1005 ¶¶ 110, 194, 236–237, 242, Figs. 7B, 10A, 14, 26H–26K). Burger states that “network server 114 may also serve as a repository for information regarding media issuers or advertisers” and “may serve as a conduit for advertisers to target particular classes of Pocket Vault holders, and channel information to them.” Ex. 1005 ¶ 117. In Burger’s example of Figure 7, after network server 114 has authenticated pocket vault 102 (Fig. 7A, steps 702–713), and the pocket vault user seeks to engage in a non-financial transaction (Fig. 7B, step 720), an authorized holder routine is executed (Fig. 7B, step 722, Fig. 10A). Ex. 1005 ¶¶ 178–186, 189, 194, 236. As shown in Figure 10A, reproduced above, if advertiser 108 makes arrangements with the company operating network server 114, advertising information can be uploaded to pocket vault 102 when the user interfaces pocket vault 102 with interface station 104b, after which the advertisement is displayed, e.g., for two seconds. *Id.* ¶¶ 237–238, Fig. 10A (steps 1002–1004).

Dr. Traynor testifies that it would have been obvious that, for pocket vault 102 to display an advertisement, it would have received an access message from network server 114 conditioned on network server 114 authenticating the pocket vault ID. Ex. 1003 ¶ 117. We credit this testimony, as it is consistent with the process of Figures 7 and 10.

In this example, and pursuant to claim limitation 1.5, the “application” that is accessed is a file, computer software, or a website containing advertising data that are displayed. Pet. 52. As to claim limitation 1.4, Petitioner argues that the first party to the transaction is the user of pocket vault 102, the second party is advertiser 108, and the third party, a third party that operates a trusted authority, is network server 114 and the party that operates it. *Id.* at 36, 41–42 (citing Ex. 1003 ¶ 113).

Patent Owner argues that the claims require that, in a transaction allowing the user access to an application, the principal parties must be the user being allowed access and the application being accessed. PO Resp. 15. Because the parties to the advertising transaction in Petitioner’s theory are the user and the advertiser, Patent Owner argues that this is not a transaction between the user and the application being accessed. *Id.* at 16. As we conclude in the above Claim Construction section, however, the claimed transaction is not limited to those in which the principal parties are the user being allowed access and the application being accessed. Thus, Patent Owner’s argument is unpersuasive.

Patent Owner also argues that, even if the claims contemplate a transaction between a user and an advertiser (we determine that they do), Petitioner has equated the third party that operates a trusted authority and the application being accessed. *Id.* at 16–17. According to Patent Owner, Burger states that network server 114 may contract with the advertisers and may act as a conduit for advertisers by storing and delivering adds. *Id.* at 17–19 (citing Ex. 1005 ¶¶ 98, 104, 111, 117, 237, 538); *see also* Sur-reply 7–8 (citing Ex. 1005 ¶¶ 98, 117, 237, 538). Thus, Patent Owner argues, network server 114 is the application being accessed, and cannot also be the

third party that operates a trusted authority. PO Resp. 19–20. According to Patent Owner,

advertisements are stored on Pocket Vault Server 114 and downloaded to Pocket Vault software on the Pocket Vault device. Accordingly, the transaction of accessing advertisements is performed only between the Pocket Vault Server 114 and the Pocket Vault. Therefore, there are only two participants in the transaction of accessing advertisement.

Sur-reply 8.

Petitioner responds that nothing in the '954 patent states that the third party that operates a trusted authority cannot be an active participant in the transaction. Reply 14–15. Thus, Petitioner argues, simply because network server 114 stores information to facilitate an advertising transaction between a user and an advertiser does not mean that network server 114 is a principal party to that transaction. *Id.* at 15. We have previously explained that active participation in a transaction, alone, does not make an entity a party to that transaction; instead, we evaluate a party's relationship to the transaction to determine whether it is a principal party or a third party. Dec. 10–11.

Petitioner also argues that it identifies different software, that running on pocket vault 102, as the application being accessed, and that Patent Owner's argument improperly conflates that software with software running on network server 114. Reply 15–16. Under Petitioner's theory, after the pocket vault is authenticated, and the pocket vault receives a message from the network server to that effect, the pocket vault displays (the user accesses) an advertisement that has been scheduled on the pocket vault. Pet. 39–40 (“[A]n advertiser may send information to the network server, which is then forwarded onto a Pocket Vault for display upon successful authentication of the user and Pocket Vault ID.”) (citing Ex. 1005 ¶¶ 117, 146, 237, 541,

Fig. 1). Although acknowledging that software on the pocket vault should not be conflated with software on the network server, Patent Owner argues that “Pocket Vault Server 114 is still the application being accessed as well as the purported third party that operates a trusted authority.” Sur-reply 9.

We agree with Petitioner. Petitioner has shown that Burger teaches an advertising transaction between advertiser 108 and the user of pocket vault 102, with the user accessing (viewing) the advertisement on the pocket vault after network server 114 authenticates pocket vault 102 and sends an access message to pocket vault 102 notifying it of the authentication. Pet. 39–40. We find that, in this transaction, the advertiser and the user of the pocket vault are the principal parties to the transaction and the operator of network server 114 is a third party that operates a trusted authority. Although network server 114 may store and transmit advertisements on behalf of advertiser 108 or otherwise act as a conduit for advertisements, witnessing and helping to facilitate the transaction does not make network server 114 a principal party to that transaction.

On the complete record, we find that Burger’s advertising example teaches claim limitations 1.4 and 1.5.

*(3) third party that operates a trusted authority; third theory
(electronic hotel room key)*

In a third example, Petitioner argues that Burger describes a user downloading a hotel room key to pocket vault 102, and using pocket vault 102 to unlock a guest room. Pet. 52–53 (citing Ex. 1005 ¶¶ 94, 102, 128–129, 679–680).

With reference to Figure 1 of Burger, reproduced above, building access cards (e.g., electronic hotel room keys) is an example of media from

non-financial media issuers 110 stored on pocket vault 102 and requiring authentication to access. Ex. 1005 ¶¶ 128–129, 679. Information such as “building security ID” is added to pocket vault 102, e.g., when docked to personal docking station 104b, through a secure connection to network server 114. *Id.* ¶ 102. According to a “typical scenario involve[ing] distribution of hotel room key cards to hotel guests who make room reservations over the Internet,” described in Burger,

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. . . . 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 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 include an icon for the hotel room key (e.g., the hotel’s logo) When the room key card icon is selected, the Pocket Vault 102 may encode the Chameleon Card with the magnetic stripe coding to unlock the guest’s hotel room.

Id. ¶ 679.

Petitioner argues that, in this example, and pursuant to claim limitation 1.5, the “application” that is accessed is a keyless lock and the transaction is obtaining authorization to enter a secure building or facility. Pet. 52; Reply 16. As to claim limitation 1.4, Petitioner argues that the first party to the transaction is the user of pocket vault 102, the second party is non-financial media issuer 110 (e.g., hotel room key issuer), and the third party, a third party that operates a trusted authority, is network server 114 and the party that operates it. Pet. 35–36; Reply 16.

As noted above, claim limitation 1.5 recites (emphasis added) “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.” Focusing on this language, in response, Patent Owner argues that, in Burger’s hotel room key example, the hotel room key card is received/downloaded from the hotel’s website and not network server 114. PO Resp. 20–21. According to Patent Owner, “[a]s the hotel key is not received from network server 114 acting as a third-party trusted authority, it cannot be equated to an access message without rendering the claim language requiring receipt of the access message *from the third-party trusted authority* meaningless.” *Id.* at 21. In other words, Patent Owner argues that, because pocket vault 102 receives the hotel room key from the hotel’s website, it does not receive it “from the trusted authority” as recited in claim limitation 1.5. *Id.*

Petitioner responds that Burger describes pocket vault 102 receiving the hotel room key from network server 114 along with an encrypted approval message indicating that pocket vault 102 has been authenticated. Reply 17–18 (citing Ex. 1005 ¶¶ 182–186, 517–527, 679, Figs. 24, 25).

We agree with Petitioner. Burger describes the hotel guest linking to network server 114 while staying within the hotel’s website when obtaining a hotel room key card. Ex. 1005 ¶ 679. As with the advertising example, non-financial media issuers 110 may enlist network server 114 to store non-financial media (e.g., hotel keys) and upload the non-financial media to pocket vault 102 when the pocket vault next synchronizes with the network server. *Id.* ¶ 467. Moreover, as indicated above, Burger expressly states that a “building security ID” is added to pocket vault 102 “through a secure

connection to the network server 114.” *Id.* ¶ 102. Thus, in accordance with Petitioner’s arguments for the hotel key example, and contrary to Patent Owner’s, we find that pocket vault 102 receives an electronic hotel room key and an encrypted approval message from network server 114.

In the Sur-reply, Patent Owner argues that, if pocket vault 102 receives the hotel room key card from network server 114, network server 114 would be both the application accessed and the third party that operates a trusted authority. Sur-reply 11. This argument is unpersuasive for the same reasons given above for Patent Owner’s substantially similar argument regarding network server 114 storing and uploading advertisements.

On the complete record, we find that Burger’s electronic hotel room key example teaches claim limitations 1.4 and 1.5.

In sum, in each of the three examples in Burger that Petitioner relies on, we find that Burger teaches claim limitations 1.4 and 1.5. Thus, on the complete record, Petitioner has shown that Burger teaches each limitation of claim 1.

c) Remaining claims

Independent claim 12 is directed to an integrated device with modules that perform functions similar to the steps of claim 1. Independent claim 16 is a method with steps substantially similar to those of claim 1. Independent claim 22 is a system with components that perform functions similar to the steps of claim 1. Petitioner’s arguments and evidence for claims 12, 16, and 22 are similar to, and largely incorporate, its arguments and evidence for claim 1. Pet. 62–65, 67–78, 80–83. Patent Owner presents its arguments for claims 1, 12, 16, and 22 together. PO Resp. 7, 17, 19, 21. For the reasons

given for claim 1, Petitioner has shown that Burger teaches each limitation of claims 12, 16, and 22.

Claim 2 depends from claim 1; claim 13 depends from claim 12. As to claims 2 and 13, we find that the pocket vault ID of Burger's pocket vault is transmitted to the network server over a wireless or cellular network. Ex. 1005 ¶¶ 99, 114, 122, 147, Fig. 7A; Ex. 1003 ¶ 120; Pet. 53, 65. Thus, Burger teaches the additional limitation of claims 2 and 13.

Claim 4 depends from claim 1. We find that Burger teaches the pocket vault sending an ID to the network server when biometric scan data from the user matches stored biometric data. Ex. 1005 ¶¶ 122, 135, 178–184, 349, 358, 553; Ex. 1003 ¶¶ 121–122; Pet. 54. Thus, Burger teaches the additional limitation of claim 4.

Claim 5 depends from claim 1; claim 26 depends from claim 22. We find that Burger teaches various examples of biometric data, including fingerprint and retinal scan data. Ex. 1005 ¶¶ 112, 135; Ex. 1003 ¶ 123; Pet. 55, 88. Thus, Burger teaches the additional limitation of claims 5 and 26.

Claims 7 and 9 depend from claim 1; claims 19 and 21 depend from claim 16; claims 27 and 29 depend from claim 22. We find that Burger describes keyless locks, financial accounts, and computer software as example applications. Ex. 1005 ¶¶ 3, 95–96, 105, 109, 127–129, 139, 149, 155–158, 182–186, 236–238, 242, 250, 255, 318–332, 511–529, 559, 679; Ex. 1003 ¶¶ 124–125; Pet. 56–58, 79, 89. Thus, Burger teaches the additional limitation of claims 7, 9, 19, 21, 27, and 29.

Claim 8 depends from claim 1. Claim 20 depends from claim 16. Claim 28 depends from claim 22. We find that Burger gives medical information cards as an example application. Ex. 1005 ¶¶ 3, 126–127;

Ex. 1003 ¶ 126; Pet. 57–58, 79, 89. Thus, Burger teaches the additional limitation of claims 8, 20, and 28.

Claim 10 depends from claim 1; claim 18 depends from claim 16. We find that Burger’s description of establishing a trust relationship between network server 114 and pocket vault 102 over a secure Internet connection teaches the additional limitation of claims 10 and 16. Ex. 1005 ¶ 114; Ex. 1003 ¶ 128; Pet. 58, 78–79.

Claim 11 depends from claim 1. We find that Burger, in its description of the process of registering a pocket vault with network server 114, teaches the additional limitations of claim 11. Ex. 1005 ¶¶ 101, 462–464, 476–481, 562, 573, 585, Figs. 19, 20; Ex. 1003 ¶¶ 129–132; Pet. 59–62.

Claim 15 depends from claim 12. We find that it would have been obvious to include an LED in Burger’s pocket vault to be activated for requesting a biometric scan, in light of Burger’s description of LEDs for displaying information and a beep to indicate that a biometric scan is complete. Ex. 1005 ¶¶ 131, 204, 206, 232, 355, 384, 585, 598, Fig. 2; Ex. 1003 ¶ 143; Pet. 66–67. Thus, Burger teaches the additional limitation of claim 15.

Claims 23 and 24 depend from claim 22. We find that Burger teaches the additional limitations of claims 23 and 24. Ex. 1005 ¶¶ 101, 184, 185, 464, 476–482, 562, 573, 575, 585, Figs. 20, 32; Ex. 1003 ¶¶ 164–169; Pet. 83–88.

Patent Owner does not present separate arguments for the dependent claims.

In sum, Burger teaches each limitation of claims 2, 4, 5, 7–13, 15, 16, 18–24, and 26–29.

4. Conclusion of obviousness

As detailed above, we find that Burger teaches each limitation of claims 1, 2, 4, 5, 7–13, 15, 16, 18–24, and 26–29. The record does not contain evidence of objective indicia of nonobviousness. Upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence that claims 1, 2, 4, 5, 7–13, 15, 16, 18–24, and 26–29 would have been obvious over Burger.

C. Obviousness of Claims 3, 14, and 17 over Burger and Robinson

Petitioner contends that claims 3, 14, and 17 would have been obvious over Burger and Robinson. Pet. 89–97. Claim 3 depends from claim 1 and adds “registering an age verification for the user in association with the device ID code.” Claim 14 depends from claim 12 and claim 17 depends from claim 16. Claims 14 and 17 add limitations similar to that of claim 3.

Robinson relates to a tokenless system and method for age verification using biometric information and a system identification number (“SID”). Ex. 1006 ¶ 5. Figure 3 of Robinson is reproduced below:

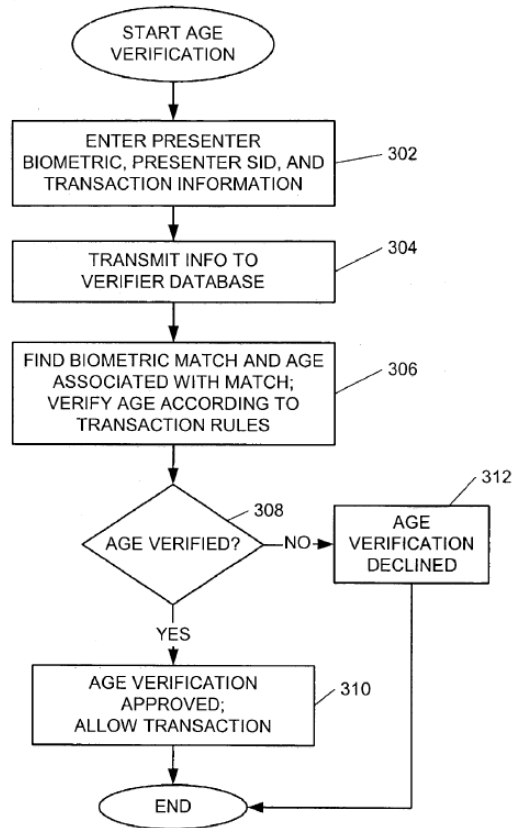


FIG. 3

Figure 3 is a flowchart of a process for age verification with remote biometric matching. *Id.* ¶ 22.

A presenter enters their SID and biometric sample (e.g., fingerprint, retinal scan, face geometric scan, voice print) at a point of verification (“POV”) device, and transaction information, such as a rule by which the presenter’s age can be evaluated, is entered (step 302). *Id.* ¶¶ 14, 30, 54. The presenter SID, biometric information, and transaction information are sent to a verifier database (step 304), which compares the biometric information to stored biometric information (step 306) and evaluates the presenter’s age. *Id.* ¶¶ 30, 55. If the presenter’s age is verified (step 308), the verifier database approves the presenter’s access to purchasing age-

restricted goods and/or services, or entry to an age-restricted area (step 310). *Id.* ¶ 57.

Petitioner contends that “it would have been obvious to a [person of ordinary skill in the art] to incorporate the age verification method of Robinson in Burger so that Burger’s system can be used by businesses interested in conducting transactions that require age-verification.” Pet. 93. Petitioner argues that it would have been predictable to include Robinson’s age-verification feature in Burger’s system in light of Robinson’s explanation that merchants and their employees face penalties if they sell age-restricted goods (e.g., alcohol or tobacco) to underage individuals. *Id.* at 94–95 (citing Ex. 1006 ¶ 5; Ex. 1003 ¶¶ 79–80). Dr. Traynor testifies that there would have been “a reasonable expectation of success because it merely involves combining known elements in a manner that would have been easily implemented and obvious to” a skilled artisan. Ex. 1003 ¶ 80. We credit Dr. Traynor’s uncontroverted testimony and find that a skilled artisan would have had reasons, with rational underpinning, to combine the teachings of Burger and Robinson.

As to claims 3, 14, and 17, Robinson describes a user registering a biometric sample, identity-verifying information (SID), and age-verifying information with a database of an age-verification system. Pet. 95–96 (citing Ex. 1006 ¶¶ 14–15, 28, 43, 48; Ex. 1003 ¶¶ 175–178). We find that a skilled artisan would have combined the teachings of Burger and Robinson, such that Robinson’s age-verifying information would have been stored in the database of Burger’s network server 114. *Id.* at 95 (citing Ex. 1003 ¶ 176). Patent Owner does not provide separate arguments for claims 3, 14, and 17. PO Resp. 22.

On the complete record, we find that Robinson teaches the additional limitations of claims 3, 14, and 17, and that a skilled artisan would have had reasons, with rational underpinning, for combining Burger and Robinson. The record does not contain evidence of objective indicia of nonobviousness. Upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence that claims 3, 14, and 17 would have been obvious over Burger and Robinson.

D. Obviousness of Claims 6 and 25 over Burger and Orsini

Petitioner contends that claims 6 and 25 would have been obvious over Burger and Orsini. Pet. 97–102. Claim 6 depends from claim 1 and adds “wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.” Claim 25 depends from claim 22 and adds substantially the same limitation.

Orsini describes a cryptographic system that includes a user system in communication with a trust engine. Ex. 1021 ¶ 62. The user system includes a biometric device that captures biometric information from the user and sends it to the trust engine. *Id.* ¶¶ 63, 67. The user system can include “a computer workstation, an interactive television, an interactive kiosk, a personal mobile computing device, such as a digital assistant, mobile phone, laptop, or the like, a wireless communications device, a smartcard, an embedded computing device, or the like.” *Id.* ¶ 65.

As to claims 6 and 25, Petitioner contends that a skilled artisan “would have implemented the Pocket Vault such that it comprises a mobile phone or laptop—devices that are similar and, in some cases, the same as modern personal digital assistants and palm top computers—as disclosed by

Orsini.” Pet. 99, 102 (citing Ex. 1021 ¶ 182; Ex. 1003 ¶¶ 181–182). Dr. Traynor testifies that this would have merely involved combining prior art elements according to known methods to yield predictable results. Ex. 1003 ¶¶ 84–88; Ex. 1005 ¶¶ 93–95, 118; Ex. 1021 ¶¶ 63, 65, 67; Pet. 99–101 (citing; Ex. 1003 ¶¶ 84–88). We credit Dr. Traynor’s uncontroverted testimony and find that a skilled artisan would have had reasons, with rational underpinning, to combine the teachings of Burger and Orsini.

Patent Owner does not provide separate arguments for claims 6 and 25. PO Resp. 22.

On the complete record, for the reasons articulated by Petitioner, we find that Orsini teaches the additional limitations of claims 6 and 25, and that a skilled artisan would have had reasons, with rational underpinning, for combining Burger and Orsini. The record does not contain evidence of objective indicia of nonobviousness. Upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence that claims 6 and 25 would have been obvious over Burger and Orsini.

*E. The ’052 Reexam*⁷

As noted above, the ’730 patent, a patent related to the ’954 patent, is the subject of the co-pending ’052 reexam. As noted above, Patent Owner requested (and was granted) adverse judgment in IPR2024-00232 and

⁷ In IPR2024-00233, Patent Owner sought Director Review (Paper 36 in IPR2024-00233) of our ’233 FWD, because our Final Written Decision allegedly was inconsistent with an Office Action in the ’052 reexam (Ex. 2016 in this proceeding). Director Review was denied in that case. Paper 38 in IPR2024-00233. That Office Action has since been superseded. Ex. 2017.

IPR2024-00775, resulting in the cancellation of all original claims of the '730 patent. Patent Owner, however, amended the claims in the '052 reexam (cancelling claims 1–17 and adding claims 18–34⁸), and, according to the reexamination Examiner, “the '954 Patent claim 1 shares similar scope relating to the access message limitation with claim 18 of the '730 Patent.” Ex. 2017 (July 29, 2025, Non-final Office Action in '052 reexam), 55⁹. The parties have entered papers from the '052 reexam as exhibits in this proceeding. *See* Exs. 1038, 2017, 2018.¹⁰

Although the current rejection of claims in the '052 reexam is non-final, and does not purport to be a final set of factual findings and conclusions, we nevertheless have considered the record from the '052 reexamination, in particular, the July 29, 2025, Non-final Office Action (Ex. 2017), and see no findings or conclusions inconsistent with our findings and conclusions in this Decision. The reexamination Examiner rejected then-pending claims 18–34 as anticipated by Burger, making findings similar to those we make here. Ex. 2017, 12–28. In fact, the reexamination

⁸ June 30, 2025, Supplemental Amendment in '052 reexam (Ex. 3001). Claims 18–34 have since been cancelled and claims 35–51 have been added. Ex. 1038.

⁹ We use the Examiner’s page numbering in the upper right corners of the document.

¹⁰ *See* C. Stewart, *Memorandum: PTAB consideration of prior findings of fact and conclusions of law* (Sept. 16, 2025) (“[I]f the Board reaches an initial or final decision on a finding of fact or conclusion of law that is different than the prior finding or conclusion of the Office, district court, or the ITC, the Board shall explain in the institution or final written decision why a different outcome is warranted. . . . To help make its assessment, the Board shall consider relevant materials submitted by the parties from the other proceeding (e.g., an opinion, a judgment, trial testimony, or other evidence)”).

Examiner “adopts the PTAB’s rationale from IPR2024-00846 for Granting Institution of Inter Partes Review [Paper 8] of related [’954 patent] dated November 18, 2024.” Ex. 2017, 55. Patent Owner admits that the Examiner “adopted specifically the rationale from the institution decision of this proceeding.” Tr. 26:3–5. For example, the Examiner concludes that

The claims do not require the parties to be a user and an application. Rather, claim 18 requires a third party trusted authority, where the access message is sent to the application from the agent (of the third party trusted authority). The parties could be the user and the application or could be, for example, the user and vendors, advertisers, non-financial media issuers and financial media issuers.

Ex. 2017, 56. With this understanding, the Examiner finds:

Burger discloses the network server is the third-party trusted authority between the user of the Pocket Vault (where the user utilizes the Pocket Vault to conduct the transaction) and advertisers, non-financial media issuers and financial media issuers as shown in Fig. 1. Thus, Burger can be viewed as having the parties be a user and the advertisers, non-financial media issuers and financial media issuers; or the user and the Pocket Vault (i.e., the application).

Id. at 57. Here, we see no material inconsistencies between our findings and conclusions and those of the Examiner.

At the hearing, Patent Owner admitted that “[t]he examiner in the CRU have adopted the Board’s claim construction,” and “didn’t see them make any inconsistent claim construction with the Board.” Tr. 26:10–12. Patent Owner further admits that “with regards to what Burger discloses, . . . the CRU hasn’t made any inconsistencies.” *Id.* at 26:17–18. Instead (for the first time at the oral argument) Patent Owner sought to argue that, in light of principles of compact prosecution, the Examiner’s decision to reject the pending claims under an anticipation ground, and not an obviousness

ground, implies that the Examiner determined that the claims were not obvious. *Id.* at 26:18–27:9. “Under the principles of compact prosecution, the examiner should review each claim for compliance with every statutory requirement for patentability in the initial review of the application and identify all of the applicable grounds of rejection in the first Office action to avoid unnecessary delays in the prosecution of the application.” Manual of Patent Examining Procedure (MPEP) § 2173.06(I). However, we see no requirement that the Examiner, when concluding that Burger discloses each limitation of claims 18–34, was required to make back-up obviousness rejections based on what Patent Owner might argue in the future.

In any case, Patent Owner has since cancelled claims 18–34 and added new claims 35–51. Ex. 1038. Thus, even if there were inconsistencies between the Examiner’s rejection of ’730 patent claims 18–34 and our analysis of claims 1–29 of the ’954 patent here (we see none), the Examiner’s rejection of claims that have since been cancelled has little relevance to this proceeding.

III. CONCLUSION¹¹

Petitioner has proved by a preponderance of the evidence that claims 1–29 of the ’954 patent are unpatentable.

¹¹ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner’s attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. See 37 C.F.R. § 42.8(a)(3), (b)(2).

The outcome for the challenged claims of this Final Written Decision follows. In summary:

Claim(s)	35 U.S.C. §	Reference(s)/ Basis	Claim(s) Shown Unpatentable	Claim(s) Not Shown Unpatentable
1, 2, 4, 5, 7–13, 15, 16, 18–24, 26–29	103(a)	Burger	1, 2, 4, 5, 7– 13, 15, 16, 18–24, 26–29	
3, 14, 17	103(a)	Burger, Robinson	3, 14, 17	
6, 25	103(a)	Burger, Orsini	6, 25	
Overall Outcome			1–29	

IV. ORDER

It is hereby:

ORDERED that 1–29 of the '954 patent are unpatentable;

FURTHER ORDERED that because this is a Final Written Decision, parties to the proceeding seeking judicial review of the Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:

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

IPR2024-00846
Patent 8,886,954 B1

PATENT OWNER:

David Hecht
James Zak
HECHT PARTNERS LLP
dhecht@hechtpartners.com
jzak@hechtpartners.com
zakx0017@umn.edu