No. 25-

In the Supreme Court of the United States

CPC PATENT TECHNOLOGIES PTY LTD.,
Petitioner,

v.

APPLE INC.,
Respondent.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Federal Circuit

PETITION FOR A WRIT OF *CERTIORARI*

MELISSA M. HAULCOMB
K&L GATES LLP
70 W MADISON ST.
SUITE 3300
CHICAGO, IL 60602

GEORGE C. SUMMERFIELD
Counsel of Record
K&L GATES LLP
SUITE 3708, PARK PLACE
1601 NANJING ROAD WEST
JING AN DISTRICT
SHANGHAI 200040 CHINA
+86 21.2211.2051
george.summerfield@klgates.com

Counsel for Petitioner

March 19, 2026

QUESTION PRESENTED

Whether the Federal Circuit can affirm a PTAB decision without opinion in contravention of the clear statutory requirement of an "opinion" when reviewing such decisions.

LIST OF PARTIES TO THE PROCEEDING

CPC Patent Technologies Pty Ltd., *Petitioner*

Apple Inc., *Respondent* (stock ticker symbol: AAPL)

RULE 29.6 STATEMENT

Petitioner CPC Patent Technologies Pty Ltd. is a wholly-owned subsidiary of Charter Pacific Corp. Ltd., which is an Australian corporation. No publicly held corporation owns 10% or more of its stock.

LIST OF PROCEEDINGS

- *CPC Pat. Techs. Pty Ltd. v. Apple, Inc.*, No. 24-1365, United States Court of Appeals for the Federal Circuit. Judgement entered Nov. 10, 2025.

- *Apple, Inc. v. CPC Pat. Techs. Pty Ltd.*, No. IPR2022-00600, Patent Trial and Appeal Board. Decision entered Oct. 13, 2023.

- *CPC Pat. Techs. Pty Ltd. v. ASSA Abloy AB*, Nos. 24-1492, 24-1493, United States Court of Appeals for the Federal Circuit. Judgement entered Nov. 10, 2025.

- *ASSA Abloy AB v. CPC Pat. Techs. Pty Ltd.*, No. IPR2022-01093, Patent Trial and Appeal Board. Decision entered Jan. 31, 2024.

- *ASSA Abloy AB v. CPC Pat. Techs. Pty Ltd.*, No. IPR2022-01094, Patent Trial and Appeal Board. Decision entered Jan. 31, 2024.

ABBREVIATIONS

'039 Patent	U.S. Patent No. 8,620,039
Apple	Respondent Apple, Inc.
Apple IPR	*Apple Inc. v. CPC Pat. Techs. Pty Ltd.*, No. IPR2022-00600
ASSA Abloy IPRs	*ASSA Abloy AB v. CPC Pat. Techs. Pty Ltd.,* IPR2022-01093 & -01094
CPC	Petitioner CPC Patent Technologies Pty, Ltd.
The Defining Limitation	The limitation "***defining***, dependent upon the received card information, a memory location in a local memory external to the card" appearing in the claims of the '039 Patent
IPR	*Inter Partes* Review
Federal Circuit	United States Court of Appeals for the Federal Circuit
FWD	Final Written Decision
PTAB	Patent Trial and Appeal Board
PTO	United States Patent and Trademark Office

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Court Rules

Other Authorities

PETITION FOR WRIT OF *CERTIORARI*

CPC respectfully requests a writ of *certiorari* to review the judgment without opinion of the Federal Circuit in *CPC Pat. Techs. Pty Ltd. v. Apple, Inc.,* No. 24-1365, 2025 WL 3135224 (Fed. Cir. Nov. 10, 2025) (App. 1a).

DECISION BELOW

The Federal Circuit decision below reviewed the FWD by the PTAB in the Apple IPR. The Federal Circuit issued a one-word affirmance without opinion, relying on its local rule 36. *CPC*, 2025 WL 3135224 (App. 1a).

JURISDICTION

The Federal Circuit entered its judgment on November 10, 2025. On February 9, 2026, this Court granted Petitioner's Application to extend the time to file a Petition until March 19, 2026. This Petition is therefore timely filed pursuant to S. Ct. R. 13. This Court has jurisdiction under 28 U.S.C. § 1254(1).

STATUTORY PROVISION INVOLVED

"The United States Court of Appeals for the Federal Circuit shall review the decision from which an appeal is taken on the record before the Patent and Trademark Office. Upon its determination the court ***shall issue*** to the Director its mandate ***and opinion***, which shall be entered of record in the Patent and Trademark Office and shall govern the further proceedings in the case." 35 U.S.C. § 144 (emphasis added).

INTRODUCTION

This is a story of two appeals – one appeal in which the Federal Circuit ***vacated*** consolidated PTAB opinions predicated upon the assumption that merely "associating" data in a memory location satisfies a claim limitation that requires "defining" a memory location, and the other appeal in which the Federal Circuit ***affirmed*** a decision on the same patent predicated on the same assumption. The two decisions are difficult, if not impossible, to reconcile. However, the Federal Circuit was not ultimately forced to reconcile them, as it rendered a one-word affirmance in the second appeal without opinion. CPC petitions this Court for *certiorari* in that second appeal.

This is the second time that CPC has approached this Court to address the viability of Federal Circuit Rule 36 when appeals from the PTAB are at issue. CPC approaches this Court again because there can be no real debate that, when applied to review of a PTAB decision, such rule, which begins with the language "[t]he court may enter a judgment of affirmance ***without opinion***," is facially inconsistent with 35 U.S.C. § 144, which requires that the Federal Circuit issue "its mandate ***and opinion***" when reviewing decisions of the PTO, of which the PTAB is a part. As this case demonstrates, allowing the Federal Circuit to avoid its statutory obligation to render an "opinion" by promulgating a rule excusing it from doing so can result in seemingly inconsistent decisions with no explanation attempting to resolve that inconsistency.

And, in any event, as this Court made clear in *Desert Palace, Inc. v. Costa*, "where, as here, the words of the statute are unambiguous, the 'judicial inquiry is complete.'" 539 U.S. 90, 98 (2003) (citation omitted). The term "opinion" (both in the statute requiring it and in the rule avoiding it) are unambiguous. This Court should grant *certiorari* to confirm what the controlling statute unambiguously says – that the Federal Circuit ***must*** issue an opinion when reviewing a PTAB decision.

STATEMENT OF THE CASE

CPC is the owner by assignment of the '039 Patent, which relates to credit card security, and in particular, biometric verification of the user. *CPC Pat. Techs. Pty Ltd. v. ASSA Abloy AB*, Nos. 2024-1492, 24-1493, 2025 WL 3134960, at *1 (Fed. Cir. Nov. 10, 2025) (App. 77a). The patent "purports to introduce a particular way of storing the biometric data during enrollment of any given user: '[t]he biometric signature is stored at a memory address ***defined by the ("unique") card information*** on the user's card as read by the card reader of the verification station.'" *Id.* (emphasis added) (citation omitted) (App. 78a). Claim 1 of the '039 Patent reads as follows, with the language at issue in this Petition highlighted:

> A method of enrolling in a biometric card pointer system, the method comprising the steps of:
>
> receiving card information;
>
> receiving the biometric signature;

> ***defining, dependent upon the received card information, a memory location in a local memory external to the card*;**
>
> determining if the defined memory location is unoccupied; and
>
> storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

Id. (emphasis added) (App. 78a-79a).

On October 13, 2023 the PTAB issued its FWD in the Apple IPR. *Apple, Inc. v. CPC Pat. Techs. Pty Ltd.*, No. IPR-2022-00600, 2023 WL 6878760 (P.T.A.B. Oct. 13, 2023) (App. 2a). On January 31, 2024, the PTAB issued its FWDs in the ASSA Abloy IPRs. *ASSA Abloy AB v. CPC Pat. Techs. Pty Ltd.*, No. IPR2022-01093, 2024 WL 378066 (P.T.A.B Jan. 31, 2024) (App. 94a); *ASSA Abloy AB v. CPC Pat. Techs. Pty Ltd.*, No. IPR2022-01094, 2024 WL 378074 (P.T.A.B. Jan. 31, 2024) (App. 163a).

In all three IPRs, the PTAB construed "defining" to mean "set" or "establish." *See CPC*, WL 3134960 at *2 (App. 80a); *Apple,* 2023 WL 6878760 at *15 (App. 43a). The PTAB nonetheless found that prior art references at issue in each proceeding, which merely taught an association of card information with biometric data, disclosed the Defining Limitation. *See, e.g., Apple,* 2023 WL 6878760 at *9 (a prior art enrollment system "creates the entry in the player ID database corresponding to th[e] player, ***associating***

the data corresponding to a first and second authentic [*sic*] authenticator with this entry") (emphasis added) (App. 28a); *CPC*, 2025 WL 3134960 at *2 (in a prior art biometric verification system "fingerprint data [is] associated with corresponding user numbers" in memory) (citation omitted) (App. 80a). The PTAB found all challenged claims invalid in each of the three IPRs, and CPC appealed.

On November 10, 2025, the same panel of the Federal Circuit issued its rulings in all three appeals. The panel reversed the FWDs in the ASSA Abloy IPRs, finding that merely storing card information "in association with" fingerprint data in the same memory location does not mean that the former defines where the latter is stored. *See CPC*, 2025 WL 3134960 at *3 (App. 83a). The court explained its ruling as follows:

> [T]o associate two pieces of data with one another does not necessarily mean that one piece of data sets, or otherwise establishes, the location of the other piece of data . . . the Board did not meaningfully grapple with the '039 patent's additional constraint that the ***card information*** determines (*i.e.*, establishes) ***the*** memory location of the biometric data.

Id. (emphasis in original).

In the case of the Apple IPR, however, the same panel issued a one-word affirmance. *CPC,* 2025 WL 3135224 (App. 1a). This was despite the PTAB having relied upon a prior art teaching that an enrollment system "creates the entry in the player ID database

corresponding to th[e] player, ***associating*** the data corresponding to a first and second authentic authenticator with this entry." *See Apple,* 2023 WL 6878760 at *9 (emphasis added) (App. 28a). While the two results are facially inconsistent with one another, the Federal Circuit was not required to address that inconsistency, as it did not write an opinion.[1]

REASONS FOR GRANTING THE PETITION

The afore-discussed inconsistency between the two appellate decisions involving the same patent illustrates the problems that can result from a rule that allows for an affirmance of PTAB decisions without opinion. Had the Federal Circuit written an opinion in the Apple IPR appeal, it could have explained away the inconsistency. On the other hand, a written opinion may well have confirmed that the two rulings were inconsistent, providing CPC with a basis for seeking rehearing at the very least.

I. The Court's Intervention is Required to Address the Federal Circuit's Practice of Affirmances Without Opinion in Contravention of Statute

The Federal Circuit's jurisdiction includes any appeal from a decision of the PTAB. 28 U.S.C. § 1295(a)(4)(A). Section 144 of the Patent Statute,

[1] In its opinion in the ASSA Abloy IPR appeals, the Federal Circuit raised as a "housekeeping" matter its affirmance of the Apple IPR ruling that the challenged claims were unpatentable "in view of a different prior art combination" in its ruling on appeal on the Apple IPR. *See CPC*, 2025 WL 3134960 at *2 (App. 82a). That opinion is therefore unhelpful in resolving the facial inconsistencies between the two proceedings.

which governs appellate review of IPR proceedings, reads as follows:

> The United States Court of Appeals for the Federal Circuit shall review the decision from which an appeal is taken on the record before the Patent and Trademark Office. Upon its determination the court ***shall*** issue to the Director its mandate and ***opinion***, which shall be entered of record in the Patent and Trademark Office and shall govern the further proceedings in the case.

35 U.S.C. § 144[2] (emphasis added).

As this Court stated in *Desert Palace*, "where, as here, the words of the statute are unambiguous, the 'judicial inquiry is complete.'" 539 U.S. at 98 (citation omitted). Ironically, the Federal Circuit, quoting that same language, stated that it did "not rely on the legislative history in this case because our judicial inquiry was complete once we determined that the statutory language unambiguously resolves" the issue before it. *Duncan v. Office of Compliance*, 541 F.3d 1377, 1380 (Fed. Cir. 2008) (citing *Desert Palace,* 539 U.S. at 98). Here, the controlling statute unambiguously calls for the Federal Circuit to issue an "opinion" when reviewing a PTAB decision.

In determining the meaning of a statutory provision, a court looks "first to its language, giving the words used their ordinary meaning." *Moskal v.*

---

[2] In 1984, Section 144 was amended to include the requirement that the Federal Circuit issue a "mandate and opinion." Pub. L. No. 98-620, title IV, § 414(a), 98 Stat. 3363 (1984).

United States, 498 U.S. 103, 108 (1990) (citations omitted). The plain meaning of "opinion" is a court's "expression of the reasons why a certain decision (the judgment) was reached in a case." Opinion, Black's Law Dictionary 985 (5th ed. 1979). "Opinions announce the decision(s) reached by [a court] and explain the reasons for those results." McLauchlan, W.P., *Opinions, Assignment and Writing Of*, The Oxford Companion to the Supreme Court of the United States 705 (2005). Reading Section 144 as requiring expressed reasoning promotes the objectives of the Federal Circuit to "provide nationwide uniformity in patent law," and to "make the rules applied in patent litigation more predictable." *See* H.R. Rep. No. 97-312 at 20 (1981); *see also* S. Rep. No. 97-275 at 2 (1981). "In the area of patents, it is especially important that the law remain stable and clear." *Bilski v. Kappos*, 561 U.S. 593, 613 (2010) (Stevens, J., concurring).

Further, the term "shall" is "used in laws, regulations, or directives to express what is mandatory." Shall, Webster's Third New Int'l Dictionary of the English Language 2085 (1976). Thus, according to the plain language of Section 144, upon review of a FWD in an IPR proceeding from the PTAB, the Federal Circuit is statutorily mandated to express the reasons why it reached that decision.

Nonetheless, several years after the current iteration of Section 144 was enacted, the Federal Circuit propounded Rule 36. *See* The Seventh Annual Judicial Conference of the United States Court of Appeals for the Federal Circuit, 128 F.R.D. 409, 420 (1989). Fed. Cir. Rule 36(a)(1) provides that "[t]he

court may enter a judgment of affirmance ***without opinion***, citing this rule, when it determines that any of the following conditions exist and an opinion would have no precedential value: (1) the judgment, decision, or order of the trial court appealed from is based on findings that are not clearly erroneous" (emphasis added).

Facially, the option not to issue an opinion relying on Rule 36 is inconsistent with the statutory mandate to issue an opinion pursuant to Section 144. As evidence of this inconsistency, the Rule 36 Order issued by the Federal Circuit below, which is exemplary of all such orders, includes only a single word expressing the decision of the court – "affirmed." *CPC,* 2025 WL 3135224 (App. 1a). Per Rule 36, this Order does not contain any opinion, which is irreconcilable with the plain language of Section 144.

Beyond this express statutory requirement, Chief Judge Markey, the first person to hold that title on the Federal Circuit – the court now operating with it local Rule 36, expressed the importance of issuing opinions, noting that the court does "not just render a ***one-worded decision*** and go away." The First Annual Judicial Conference of the United States Court of Appeals for the Federal Circuit, 100 F.R.D. 499, 511 (1983) (emphasis added). "[Y]ou would never know what the law is otherwise." *Id.*

Unsurprisingly, Chief Judge Markey was not alone. Justice Brennan observed that the writing of opinions "restrains judges and keeps them accountable to the law and to the principles that are the source of judicial authority." Brennan, W.J., *In*

Defense of Dissents, 37 Hastings L.J. 427, 435 (1986). Judge Leventhal noted that "there is accountability in the giving of reasons," but grave questions are presented when "a court uses 'judgments' and 'orders' to dispense with any indication of reasons." Leventhal, H., *Appellate Procedures: Design, Patchwork, and Managed Flexibility*, 23 UCLA L. Rev. 432, 438 (1976). Justice Cardozo noted that reason-giving generates a body of coherent, predictable law. Cardozo, B.N., *Nature of the Judicial Process* 30 (1921). There can be little that undoes predictability like facially inconsistent decisions.

So, the statute is clear – the Federal Circuit is required to issue an "opinion" when reviewing a PTAB decision, *i.e.*, a disclosure of the reasons why the court reached its decision. However, in contravention of the statutorily mandated requirement to issue an opinion, and the benefit therefrom, a Rule 36 summary affirmance "simply confirms" that the adjudicative body below "entered the correct judgment" and "does not endorse or reject any specific part" of the "reasoning" under review, let alone ensuring any consistency thereof with prior decisions. *See Phil-Insul Corp. v. Airlite Plastics Co.*, 854 F.3d 1344, 1355 (Fed. Cir. 2017) (citation omitted). The existence of the Federal Circuit's Rule 36, and the one-word affirmances that result therefrom, warrant the intervention of this Court to correct the Federal Circuit's practice that so clearly contravenes statute.

II. This is the Appropriate Case for Addressing this Issue Given the Facial Inconsistency Between the Two Decisions in Question

CPC is cognizant of the myriad petitions that have previously challenged the legitimacy of Federal Circuit Rule 36. CPC submits, however, that none of those prior petitions involved a situation in which two appellate decisions from the panel addressed what amounts to the same issue on the same patent, but reached diametrically opposed results. As if to emphasize Judge Markey's concern regarding the need to avoid one-word rulings, in the instant case, given such a ruling, one can only guess as to how the Federal Circuit's two inapposite decisions on the same patent are a consistent application of the law.[3] And, to echo the sentiments of Justice Cardozo, requiring an opinion in this case would only help to generate a body of predictable law by either resolving the facial inconsistency between the two appellate decisions, or highlighting that inconsistency, and allowing the parties to address them.

CONCLUSION

Rule 36's provision of an appellate affirmance of a PTAB decision without opinion is facially inconsistent with Section 144, which mandates that

[3] The Federal Circuit's reference to "different prior art" in its decision in the ASSA Abloy IPR is hardly a satisfactory explanation. *CPC*, 2025 WL 3134960 at *2 (App. 82a). The prior art in both cases taught ***associating*** data – not using one data set to define a storage location for another. That the references had different authors is hardly the point.

the Federal Circuit issue an opinion when reviewing a decision of the PTAB. CPC respectfully requests that this Court grant *certiorari* and remand this matter to the Federal Circuit with instructions to issue a written opinion.

Respectfully submitted,

GEORGE C. SUMMERFIELD
Counsel of Record
K&L GATES LLP
Suite 3708, Park Place
1601 Nanjing Road West
Jing An District Shanghai 200040
China
+86 21.2211.2051
george.summerfield@klgates.com

MELISSA M. HAULCOMB
K&L Gates LLP
70 W Madison Street
Suite 3300
Chicago, Illinois 60602

Counsel for Petitioner

March 19, 2026

APPENDIX

TABLE OF APPENDICES

Page

APPENDIX A — JUDGMENT OF THE UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT, NO. 24-1365, FILED NOVEMBER 10, 2025

UNITED STATES COURT OF APPEALS,
FEDERAL CIRCUIT

2024-1365

CPC PATENT TECHNOLOGIES PTY LTD.,

Appellant

v.

APPLE INC.,

Appellee

November 10, 2025

Appeal from the United States Patent and Trademark Office, Patent Trial and Appeal Board in No. IPR2022-00600.

(Prost, Wallach, and Chen, Circuit Judges).

JUDGMENT

Per Curiam

THIS CAUSE having been heard and considered, it is ORDERED and ADJUDGED:

AFFIRMED. *See* Fed. Cir. R. 36.

APPENDIX B — JUDGMENT OF THE PATENT TRIAL AND APPEAL BOARD, NO. IPR2022-00600, DATED OCTOBER 13, 2023

PATENT TRIAL AND APPEAL BOARD

IPR2022-00600
Patent 8,620,039 B2

APPLE INC.,

Petitioner,

v.

CPC PATENT TECHNOLOGIES PTY, LTD,

Patent Owner.

Dated October 13, 2023

Before SCOTT A. DANIELS, AMBER L. HAGY and FREDERICK C. LANEY, Administrative Patent Judges.

JUDGMENT

Final Written Decision Determining All Challenged Claims Unpatentable

35 U.S.C. § 318(a)

DANIELS, Administrative Patent Judge.

Appendix B

I. INTRODUCTION

Apple Inc., ("Apple" or "Petitioner") filed a Petition requesting *inter partes* review ("IPR") of claims 1, 2, 19, and 20 of U.S. Patent No. 8,620,039 B2 (Ex. 1001, "the '039 patent"). Paper 1 ("Pet"). CPC Patent Technologies PTY, Ltd., ("CPC" or "Patent Owner") filed a Preliminary Response to the Petition. Paper 7 ("Prelim. Resp.").

On October 17, 2022, we instituted trial for claims 1, 2, 19, and 20 of the '039 patent on all grounds of unpatentability alleged in the Petition. Paper 8 ("Decision to Institute" or "Inst. Dec."). After institution of trial, Patent Owner filed a Patent Owner Response. Paper 12 ("PO Resp.). Petitioner timely filed a Reply. Paper 13 ("Pet. Reply). Subsequently, Patent Owner filed a Sur-Reply to address certain arguments raised in Petitioner's Reply. Paper 15 ("PO Sur-Reply).

A hearing for this proceeding was held on July 18, 2023. The transcript of the hearing has been entered into the record. Paper 21 ("Tr.").

We have jurisdiction under 35 U.S.C. § 6(c). This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a).

For the reasons that follow, we determine that Petitioner has met its burden of showing by a preponderance of the evidence that claims 1, 2, 19, and 20 are unpatentable.

Appendix B

A. Real Parties in Interest

Petitioner states that Apple Inc. is the real party in interest. Pet. 57. Patent Owner states that CPC Patent Technologies PTY, Ltd., is the real party in interest. Paper 3.

B. Related Matters

The parties indicate that the '039 patent has been asserted against Petitioner in *CPC Patent Technologies PTY Ltd. v. Apple Inc.*, Case No. 6:21-cv-00165, in the U.S. District Court for the Western District of Texas. Pet. 57; Paper 3.

Petitioner indicates that it has filed additional petitions for *inter partes* review challenging two other patents held by Patent Owner, IPR2022-00601 for U.S. Patent No. 9,269,208, and IPR2022-00602 for U.S. Patent No. 9,665,705. Pet. 57. Final Written Decisions in these IPRs were entered on September 27, 2023.

C. The '039 Patent (Ex. 1001)

The '039 patent, titled "Card Device Security Using Biometrics," describes a biometric card pointer (BCP) system intended to more efficiently and securely permit a user to store biometric information during an enrollment process, and in future verification processes access their account using an identification (ID) card and biometric information such as a fingerprint. Ex. 1001, 2:51-3:11.

Appendix B

The '039 patent explains that in the enrollment phase "[t]he card user's biometric signature is automatically stored the first time the card user uses the verification station in question (this being referred to as the enrolment phase)." *Id.* at 2:62-64. The '039 patent explains further that "[t]he biometric signature is stored at a memory address defined by the ('unique') card information on the user's card as read by the card reader of the verification station." *Id.* at 2:64-67. Following the enrollment phase, the '039 patent describes that

> [a]ll future uses (referred to as uses in the verification phase) of the particular verification station by someone submitting the aforementioned card requires the card user to submit both the card to the card reader and a biometric signature to the biometric reader, which is verified against the signature stored at the memory address defined by the card information thereby determining if the person submitting the card is authorised to do so.

Id. at 3:4-11.[1] For both enrollment and future verification, the use of the ID card at a verification station "is identical from the card user's perspective, requiring merely input of the card to the card reader, and provision of the biometric

1. The words "enrolment," "authorise," and "authorisation" are the British spellings of "enrollment," "authorize," and "authorization." *See*, *e.g.*, https://www.merriam-webster.com/dictionary/authorisation, last visited Sept. 23, 2022. We will use the American spelling of these words except when quoted from the '039 patent.

signature ([e.g.] thumb print or retinal scan etc.) to the biometric reader." *Id.* at 3:12-15.

Figure 4 of the '039 patent is reproduced below.

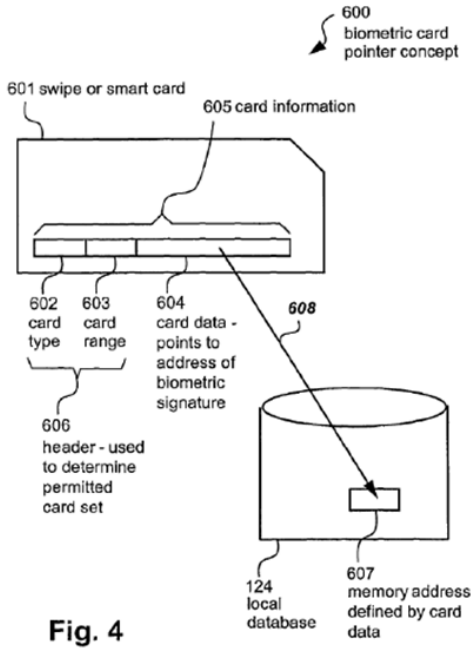


Fig. 4

Figure 4 of the '039 patent illustrates swipe or smart card 601 including card information 605 encompassing fields for card type 602, card range 603, and card data 604. The '039 patent describes that "the card data 604 acts as the memory reference which points, as depicted by an arrow 608, to a particular memory location at an address 607 in the local database 124." *Id.* at 7:31-35. Information 605 can be encoded on a magnetic strip on the card, for

example. *Id.* at 7:28-29. The '039 patent explains that for a specific user "[i]n an initial enrolment phase, . . . [t]he card data 604 defines the location 607 in the memory 124 where their unique biometric signature is stored." *Id.* at 7:43-49. And the '039 patent explains further that "in later verification phases, . . . [t]his signature is compared to the signature stored at the memory location 607 in the memory 124, the memory location 607 being defined by the card data 604 read from their card 601 by the card reader 112." *Id.* at 7:50-56.

Figures 6 and 7, reproduced below, depict the differences between enrollment process 207 shown in Figure 7 and verification process 205 shown in Figure 6.

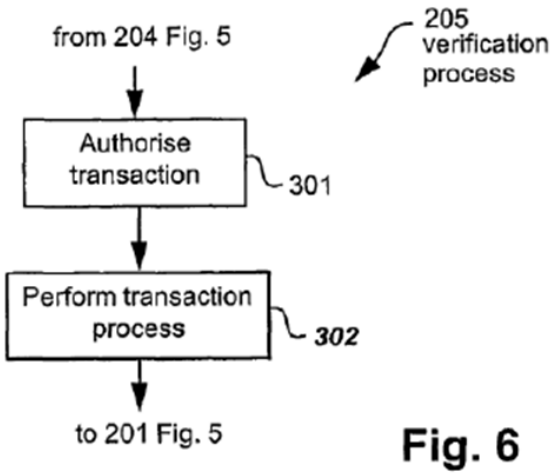


Fig. 6

Appendix B

Figure 6 illustrates verification process 205, which occurs after the enrollment process, illustrated, below, in Figure 7.

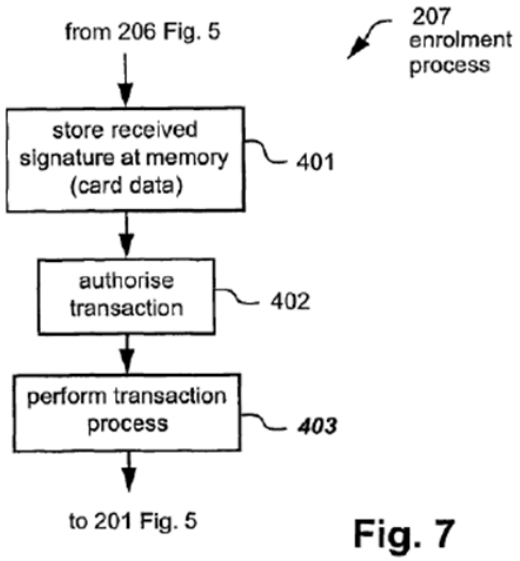


Fig. 7

Figure 7 of the '039 patent illustrates enrollment process 207 where the system at "step 401 stores the biometric signature received by the step 203 in the memory 124 at a memory address defined by the card data 604." *Id.* at 9:64-66 (referring to elements 203 and 124 described in Figure 5).

Appendix B

A difference between verification process 205 and enrollment process 207 is that the enrollment process includes step 401, which *stores* the biometric signature "at a memory address defined by the card data 604," whereas in verification process 205 "step 204 *reads* the contents stored at a single memory address defined by the card data 604" and compares the stored biometric signature with the input biometric signature. *Id.* at 9:65-66, 8:24-26.

D. Illustrative Claim

Claims 1 and 19 are independent. Each of claims 2 and 20 depends, respectively, from independent claims 1 and 19. Claim 1, including disputed limitations highlighted in italics, illustrates the claimed subject matter and is reproduced below:

> 1. [1Pre] A method of enrolling in a biometric card pointer system, the method comprising the steps of:
>
> [1a] receiving card information;
>
> [1b] receiving the biometric signature;
>
> [1c] *defining, dependent upon the received card information, a memory location in a local memory external to the card;*
>
> [1d] determining if the defined memory location is unoccupied; and
>
> [1e] storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

Ex. 1001, 12:29-38. Limitations [1a]-[1e] are similarly recited in independent claim 19 in the context of "a processor to execute a method of enrolling in a biometric card pointer system." *Id.* at 15:25-16:11. For example, limitation [19a] recites "code for receiving card information." *Id.* at 16:3.

E. Prior Art and Asserted Ground

Petitioner asserts that claims 1, 2, 19, and 20 would have been unpatentable based on the following ground:

Ground	Claim(s) Challenged	35 U.S.C. §[2]	Reference(s)/ Basis
1	1, 2, 19, 20	103(a)	Bradford,[3] Foss,[4] [5] and Yamane

2. The Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112-29, 125 Stat. 284, 296-07 (2011), took effect on September 16, 2011. The changes to 35 U.S.C. §§ 102 and 103 in the AIA do not apply to any patent application filed before March 16, 2013. Because the application for the patent at issue in this proceeding has an effective filing date before March 16, 2013, we refer to the pre-AIA version of the statute.

3. Ex. 1004, US Patent No. 6,612,928 Bl (Sept. 2, 2003).

4. Ex. 1005, US Pub. Appl. No. 2005/0127169 A1 (pub. Jun. 16, 2005).

5. Ex. 1006, US Pub. Appl. No. 2001/0014883 A1 (pub. Aug. 16, 2001).

Petitioner relies on the testimony of Andrew Sears, Ph.D. Ex. 1003. Patent Owner relies on the testimony of William Easttom, Ph.D. Ex. 2001.

II. ANALYSIS

A. Legal Standards

A patent 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. 35 U.S.C. § 103(a); *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). "[W]hen a patent claims a structure already known in the prior art that is altered by the mere substitution of one element for another known in the field, the combination must do more than yield a predictable result." *KSR*, 550 U.S. at 416 (citing *United States v. Adams*, 383 U.S. 39, 50-51 (1966)). The question of obviousness is resolved based on 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 ordinary skill in the art; and (4) when in evidence, objective evidence of non-obviousness. *Grahamv. JohnDeereCo.*, 383 U.S. 1, 17-18 (1966).[6]

The Supreme Court made clear that we apply "an expansive and flexible approach" to the question of

6. The parties do not present evidence or arguments regarding secondary considerations.

obviousness. *KSR*, 550 U.S. at 415. Whether a patent claiming the combination of prior art elements would have been obvious is determined by whether the improvement is more than the predictable use of prior art elements according to their established functions. *Id.* at 417. To support this conclusion, however, it is not enough to show merely that the prior art includes separate references covering each separate limitation in a challenged claim. *Unigene Labs., Inc. v. Apotex, Inc.*, 655 F.3d 1352, 1360 (Fed. Cir. 2011). Rather, obviousness additionally requires that a person of ordinary skill at the time of the invention "would have selected and combined those prior art elements in the normal course of research and development to yield the claimed invention." *Id.*

Accordingly, an obviousness determination generally requires a finding "that a person of ordinary skill in the art would have been motivated to combine or modify the teachings in the prior art and would have had a reasonable expectation of success in doing so." *Univ. of Strathclyde v. Clear-Vu Lighting LLC*, 17 F.4th 155, 160 (Fed. Cir. 2021) (citing *OSI Pharms.*, 939 F.3d at 1382 (quoting *Regents of Univ. of Cal. v. Broad Inst., Inc.*, 903 F.3d 1286, 1291 (Fed. Cir. 2018))). "Whether the prior art discloses a claim limitation, whether a skilled artisan would have been motivated to modify or combine teachings in the prior art, and whether she would have had a reasonable expectation of success in doing so are questions of fact." *Strathclyde*, 17 F.4th at 160. In determining whether there would have been a motivation to combine prior art references to arrive at the claimed invention, it is insufficient to simply conclude the combination would have been obvious without

identifying any reason why a person of skill in the art would have made the combination. *Metalcraft of Mayville, Inc. v. The Toro Co.*, 848 F.3d 1358, 1366 (Fed. Cir. 2017). Moreover, in determining the differences between the prior art and the claims, the question under 35 U.S.C. § 103(a) is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious. *LittonIndus. Prods., Inc. v. Solid State Sys. Corp.*, 755 F.2d 158, 164 (Fed. Cir. 1985) ("It is elementary that the claimed invention must be considered as a whole in deciding the question of obviousness."); *see also Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1537 (Fed. Cir. 1983) ("[T]he question under 35 U.S.C. § 103 is not whether the differences themselves would have been obvious. Consideration of differences, like each of the findings set forth in *Graham*, is but an aid in reaching the ultimate determination of whether the claimed invention *as a whole* would have been obvious.").

As a factfinder, we also must be aware "of the distortion caused by hindsight bias and must be cautious of arguments reliant upon ex post reasoning." *KSR*, 550 U.S. at 421. Applying these general principles, we consider the evidence and arguments of the parties.

B. Level of Ordinary Skill in the Art

The level of skill in the art is "a prism or lens" through which we view the prior art and the claimed invention. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). "This reference point prevents . . . factfinders from using their own insight or, worse yet, hindsight,

to gauge obviousness." *Id.* Moreover, "the inquiry into whether any 'differences' between the invention and the prior art would have rendered the invention obvious to a skilled artisan necessarily depends on such artisan's knowledge." *Koninklijke Philips N.V. v. Google LLC*, 948 F.3d 1330, 1337 (Fed. Cir. 2020) (citing *Dow Jones & Co. v. Ablaise Ltd.*, 606 F.3d 1338, 1349, 1353 (Fed. Cir. 2010) (affirming the district court's grant of summary judgment of invalidity in part because the obviousness "analysis requires an assessment of the '. . . background knowledge possessed by a person having ordinary skill in the art'")).

Factors pertinent to a determination of the level of ordinary skill in the art include: (1) educational level of the inventor; (2) type of problems encountered in the art; (3) prior art solutions to those problems; (4) rapidity with which innovations are made; (5) sophistication of the technology; and (6) educational level of workers active in the field. *Env't Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 696-697 (Fed. Cir. 1983) (citing *Orthopedic Equip. Co. v. All Orthopedic Appliances, Inc.*, 707 F.2d 1376, 1381-82 (Fed. Cir. 1983)). Not all such factors may be present in every case, and one or more of these or other factors may predominate in a particular case. *Id.* Moreover, these factors are not exhaustive but are merely a guide to determining the level of ordinary skill in the art. *Daiichi Sankyo Co. Ltd, Inc. v. Apotex, Inc.*, 501 F.3d 1254, 1256 (Fed. Cir. 2007).

In determining a level of ordinary skill, we also may look to the prior art, which may reflect an appropriate skill level. *Okajima*, 261 F.3d at 1355.

Additionally, the Supreme Court informs us that "[a] person of ordinary skill is also a person of ordinary creativity, not an automaton." *KSR*, 550 U.S. at 421.

In our Institution Decision we determined, in accordance with Petitioner's proposal, that a person of ordinary skill in the art at the time of the '039 patent

> would have had at least a bachelor's degree in computer engineering, computer science, electrical engineering, or a related field, with at least one year of experience in the field of human-machine interfaces and device access security. Additional education or experience might substitute for the above requirements.

Inst. Dec. 9 (quoting Pet. 4). Patent Owner does not dispute the level of ordinary skill in the art. PO Resp. 5.

Because there is no express dispute as to the level of ordinary skill in the art, and because Petitioner's assessment is consistent with the '039 patent and the asserted prior art, we maintain our reliance on Petitioner's proposed level of ordinary skill in the art as set forth above.

C. Claim Construction

We construe claims using the principles set forth in *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312-17 (Fed. Cir. 2005) (en banc), and related cases. 37 C.F.R. § 42.100(b) (2021). Under that precedent, the words of a claim are generally given their "ordinary and customary meaning,"

which is the meaning the term would have to a person of ordinary skill at the time of the invention, in the context of the entire patent including the specification. *Phillips*, 415 F.3d at 1312-13.

1. Dependent upon

Petitioner indicates that the parties agreed in the district court litigation that "dependent upon," recited in claim 1 and 19, should be given its "[p]lain and ordinary meaning, defined as 'contingent on or determined by.'" Pet. 6 (citing Ex. 1032, 2). Patent Owner agrees, adding that "a memory location in a local memory which *corresponds* to, but is not contingent upon or determined by, the received card information is not 'dependent upon' under Apple's claim construction." PO Resp. 7 (emphasis added). Patent Owner contends, however, that despite this agreed upon meaning, the arguments in the Petition are not consistent with the plain and ordinary meaning. *Id.*

For purposes of understanding claim 1, given the plain and ordinary meaning of "dependent upon," limitation 1[c] would read:

> **[1c]** ***defining, [contingent upon or determined by] the received card information, a memory location in a local memory external to the card;***

Because neither party disputes the agreed upon meaning of "dependent upon," we will consistently apply the plain and ordinary meaning of "dependent upon" as "contingent on or determined by."

2. Biometric card pointer system

Petitioner also notes that the District Court construed "biometric card pointer system" recited in both claims 1 and 19 "as a '[n]onlimiting preamble term with no patentable weight.'" *Id.* (citing Ex. 1033, 1). Neither party, on this record, disputes this construction, and therefore, to the extent necessary, we rely on the District Court's construction.

3. Defining

We note that Patent Owner proposes also, not a specific claim construction, but an interpretation that we should understand "defining" as meaning "setting" or "establishing." *See* PO Resp. 5-8 (Patent Owner arguing that "Petitioner repeatedly characterizes '*defining*, dependent upon the received card information' term with respect to *Bradford* as 'to find' or 'identifying.'"). Because the parties do not specifically construe the term "defining," we address this issue in the context of the claim language as a whole, and the '039 specification, in our analysis below.

D. Ground 1: Claims 1, 2 19, and 20—Alleged Obviousness over Bradford (Ex. 1004) in view of Foss (Ex. 1005), and further in view of Yamane (Ex. 1006)

On the complete record now before us, Petitioner has shown by a preponderance of the evidence that claims 1, 2, 19, and 20 would have been obvious over Bradford, Foss, and Yamane.

Appendix B

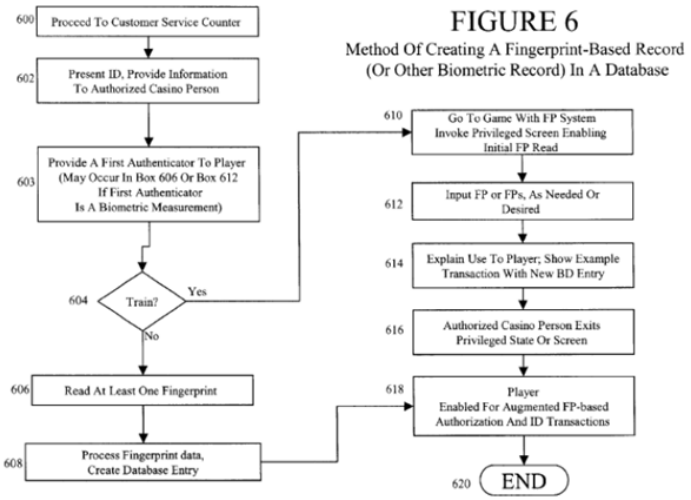
1. Bradford (Ex. 1004)

Titled "Player Identification using Biometric Data in a Gaming Environment," Bradford relates to player authentication systems and gaming machines using biometric data, which "allow a player to quickly and easily authenticate documents while remaining at game machines, [and] authenticate electronically based transfers into and out of accounts at game machines." Ex. 1004, Abstract, code (57).

Bradford discloses a gaming authentication system that uses at least two authenticators to identify a player, explaining "[t]he first authenticator may be one of many types, with a typical first authenticator being a player ID card, a voucher with a unique, encoded, and preferably encrypted numerical ID on it, a unique alphanumeric sequence, or an RFID tag." *Id.* at 3:6-10. Bradford discloses that "[t]he second authenticator will be based on a biometric reading. The present invention may use any biometric reading, although those providing reasonably high degrees of uniqueness are clearly preferred. It is expected that at the present time, the predominant biometric used will be based on fingerprints." *Id.* at 3:21-26.

Bradford further discloses a method for entering biometric data entry into a player ID database. *Id.* at 14:21-22. Bradford explains that "[a] player identification database is also used, where an entry corresponding to a player comprises at least one record (typically, exactly one record), and the record has fields containing data, information, or pointers." *Id.* at 3:28-31. Bradford's Figure 6 is reproduced below.

Appendix B



Bradford's Figure 6, titled "Method of Creating a Fingerprint-Based Record [] in a Database," is a flow chart illustrating steps for creating a fingerprint, or other biometric data, as an entry in a database record. The process begins with a player going to a customer service counter at step 600 and then presenting identification and requesting an account at step 602. *Id.* at 14:23-28. At step 603, the player may be provided with a first authenticator, such as an ID card or voucher. *Id.* at 15:16-20. If a player desires training "[t]he attendant goes to a game with the present invention installed on it" where the player's biometric information is entered at step 612. *Id.* at 15:42-58.

Depending on whether a player needs training on how to operate a game at step 604, the player's biometric data, e.g., fingerprint data, is input to the database at either steps 606-608, or step 612. Once the first and second

authenticators are stored, the player is enabled at step 618 to be subsequently verified and to operate a desired game device. *Id.* at 16:40-47.

2. Foss (Ex. 1005)

Foss is titled "Stored Value Card Account Transfer System" and describes various systems and methods for transferring funds between stored value card accounts of first and second customers. Ex. 1005, Abstract, code (57). Referring to Figure 8, Foss discloses in one embodiment "an enrollment process at merchant terminal 704 for enabling a primary account holder (i.e., an existing customer 610) to enroll additional new customer(s) in the family stored value card program." Ex. 1005 ¶ 86. Foss's Figure 8 is reproduced below.

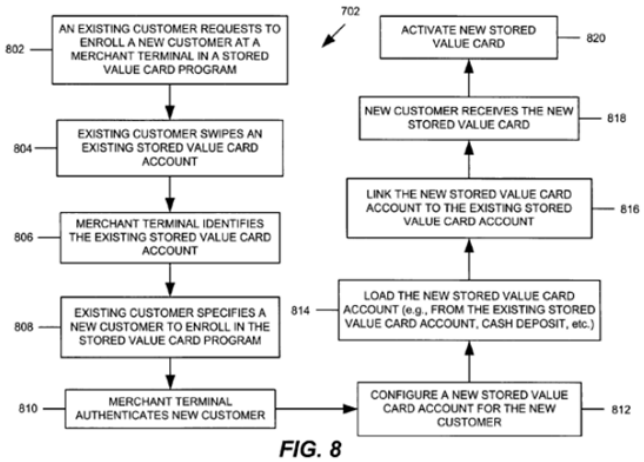


FIG. 8

Foss's Figure 8 is a flow chart illustrating steps for an existing customer having an existing stored value card

and account to initiate enrollment of a new customer at steps 802-808. *Id.* ¶¶ 86-90. Foss explains that "[a]t block 806, merchant terminal 704 identifies the stored value card account associated with the existing customer 610. The stored value card account may be identified based on the data read from magnetic stripe 710 via card reader 706." *Id.* ¶ 88.

Foss describes step 804 as part of a process by which existing customer 506 can swipe their card and begin an enrollment process for new additional customers, e.g., a family member. *Id.* ¶ 85. Foss's Figure 11 is reproduced below.

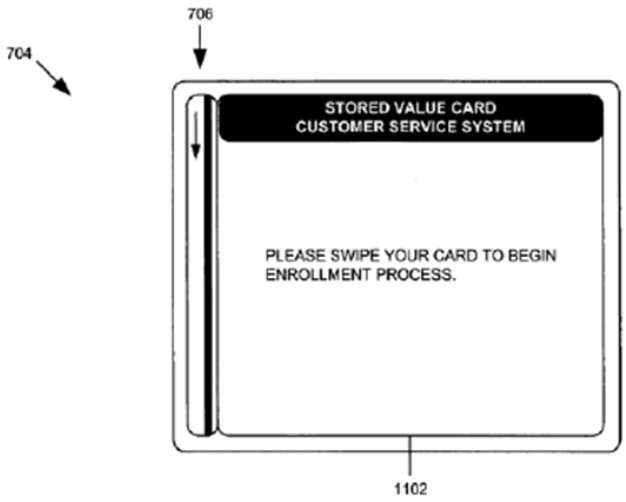


FIG. 11

Foss's Figure 11 "illustrates another input screen 1102 which prompts the existing customer 610 to swipe the existing stored value card 508." *Id.* ¶ 88. Foss explains

that the new customer's account is added to the primary customer's account, and, after authentication of the new customer at step 810, Foss describes that a new stored value card is loaded with some monetary value and linked to the existing stored value card account at steps 814, 816. *Id.*; *see also id.* at ¶ 90 ("At block 814, the existing customer 610 has the option of loading the new secondary stored value card account . . . with funds.").

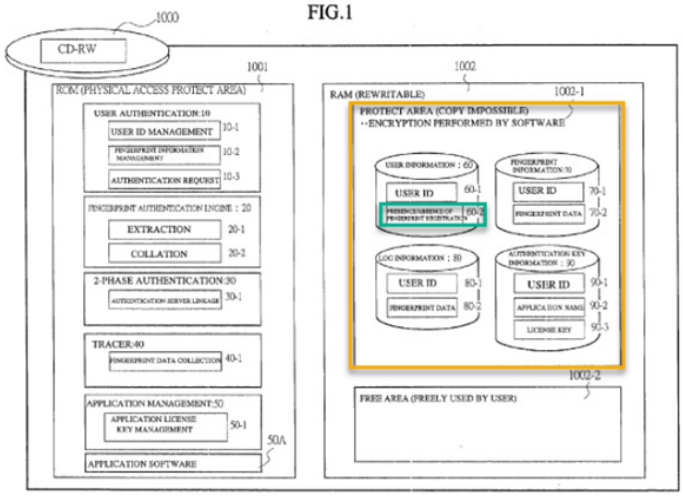
3. Yamane (Ex. 1006)

Yamane is titled "Portable Recording Medium and Method of Using Portable Recording Medium" and discloses, for example, a CD-RW that requires identification of an authorized user before a user can access software stored on the CD-RW. Ex. 1006, Abstract. Yamane discloses specifically a user authentication program implemented as "software for performing a process of deciding a proper user on the basis of user fingerprint information input from the outside and fingerprint information which is registered in advance." *Id.* ¶ 33.

Considering Yamane's Figure 1, as annotated by the Board and reproduced below, Yamane describes user information 60 and fingerprint information 70 stored in a protect area 1002-1 (highlighted yellow) of rewritable area 1002 of CD-RW 1000. *Id.* ¶ 39.

Appendix B

FIG.1

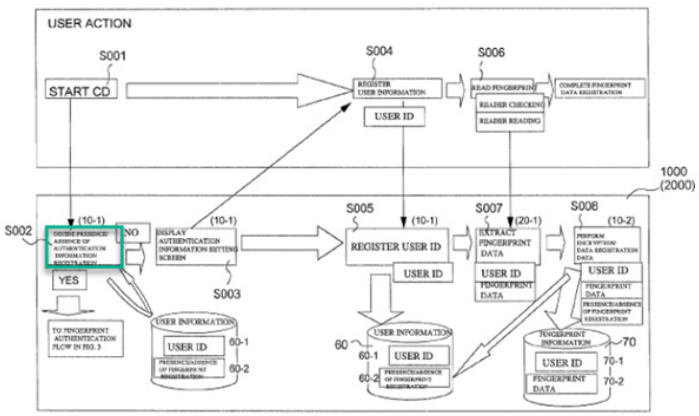


Yamane's Figure 1 illustrates user information 60 including User ID 60-1 and fingerprint registration presence/absence flag 60-2 (highlighted green). *Id.* ¶ 40. Referring to Figure 2, Yamane explains that

> [t]he user ID management function 10-1 of the user authentication program 10 decides whether a fingerprint has been registered or not with reference to the fingerprint registration presence/absence flag 60-2 of the user information 60 (step S002). If the fingerprint has not been registered, an authentication information setting screen for urging a user to register a fingerprint is shown to the user (step S003).

Id. ¶ 52. Yamane's Figure 2 as annotated by the Board is reproduced below.

FIG.2



Yamane's Figure 2 illustrates diagrammatically that following step S001, the start-up of CD, step S002 (highlighted green) detects the presence/absence of authentication information including presence/absence of fingerprint data 60-2. *Id.*

4. Independent Claim 1

(a) Petitioner's Arguments

Petitioner contends that a person of ordinary skill in the art would have understood Bradford, Foss, and Yamane in combination to teach all of the limitations of claim 1. *See* Pet. 5, 9.

Appendix B

i. Limitation [1Pre] – "A method of enrolling in a biometric card pointer system, the method comprising the steps of:"

Petitioner argues that even if the preamble is limiting, Bradford teaches such a method because Bradford describes enrolling a new user (a "player [seeking to use gaming devices] currently without an entry in [a] player ID database") in the player ID database, the enrollment including "creation of an entry having biometric data in [the] player ID database." Pet. 9-12 (citing Ex. 1004, 3:50-54, 14:21-28, 15:16-24, 15:37-38, 15:48-58, 16:5-7, 16:21-32, 16:40-47, 22:25-56, Fig. 6). Petitioner explains that completion of Bradford's enrollment provides the player with "an entry in the player ID database corresponding to the player, having a first authenticator and a second authenticator useable by the player." *Id.* at 12 (citing Ex. 1004, 16:21-25, 16:40-47).

Petitioner argues that Bradford performs enrollment in "a biometric card pointer system" as claimed because "*Bradford* describes creating a player ID that is accessed using a player ID card" that includes the player's first authenticator, and the player ID (after enrollment) resides in the player ID database in which the enrolled players' entries include records having "fields containing data, information, or pointers. The records have fields corresponding to a first authenticator and a second authenticator, providing authenticator data therein or pointers to authenticator data." Pet. 9, 12-14 (citing Ex. 1004, 3:6-23, 3:28-36, 3:50-58, 5:36-54, 6:3-13, 15:16-20, 16:40-45, Fig. 6; Ex. 1003 ¶¶ 64-69).

Appendix B

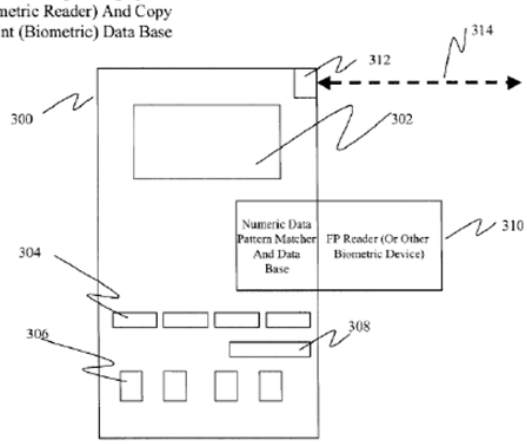
ii. Limitation [1a] – receiving card information.

According to Petitioner, Bradford describes a magnetic strip card that may be inserted and read by a magnetic strip card reader to provide data of a "first authenticator" of a player. Pet 14-15 (citing Ex. 1004, 3:9-15, 6:4-6, 6:13-27, 8:22-31, 8:51-56; Ex. 1003 ¶¶ 70-72). In Bradford, the first authenticator is provided to the player during enrollment. *Id.* at 11-12 (citing Ex. 1004, 14:25-43, 15:16-24, 15:37-38, 15:48-63, 16:1-5, 16:26-32, Fig. 6).

Petitioner relies in part on Bradford's Figure 3, reproduced below, showing a "General Gaming Device" 300 having "first authenticator readers" 304. *Id.* at 14-15.

FIGURE 3

General Gaming Device Having A Fingerprint Reader (Or Other Biometric Reader) And Copy Of A Player Fingerprint (Biometric) Data Base



Appendix B

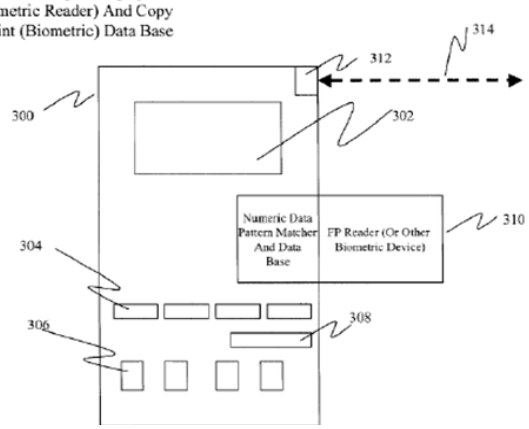
Bradford's general gaming device 300 includes, among other things, first authentication readers 304 and fingerprint reader 310. Ex. 1003, Fig. 3.

iii. Limitation [1b] – receiving the biometric signature.[7]

As shown above in Figure 3, Bradford describes a fingerprint reader 310 for receiving a fingerprint "biometric signature." Pet. 16 (citing Ex. 1004, 7:45-47, 8:22-28, 8:56-65, 10:30-40, Fig. 3; Ex. 1003 ¶¶ 64-65, 73-78). Petitioner relies in part on Bradford's Figure 3, reproduced below, illustrating "General Gaming Device" 300 having an "FP Reader (Or Other Biometric Device)" 310."

FIGURE 3

General Gaming Device Having A Fingerprint Reader (Or Other Biometric Reader) And Copy Of A Player Fingerprint (Biometric) Data Base



7. As recited in claim 1, "the biometric signature" does not have antecedent basis. For purposes of our Decision, we assume this is incorrect and should be understood as "a biometric signature."

Appendix B

Bradford's general gaming device 300 includes, among other things, first authentication readers 304 and fingerprint reader 310. Ex. 1003, Fig. 3.

iv. Limitation [1c] – defining, dependent upon the received card information, a memory location in a local memory external to the card.

Petitioner argues that Bradford discloses "a memory location, i.e., the second authenticator data field storing the second authenticator data [(biometric information, such as fingerprint data)], in a database, i.e., the player ID database." Pet. 23-24 (citing Ex. 1004, 6:3-30, 6:49-64, 15:59-63, 17:47-51, 17:18-22, 23:36-40). The biometric information is entered into Bradford's player ID database during enrollment—during which the two-level authentication system "creates the entry in the player ID database corresponding to th[e] player, associating the data corresponding to a first and second authentic authenticator with this entry." Ex. 1004, 16:40-45; *see* Pet. 19-20 (citing Ex. 1004, 3:27-36, 14:21-28, 14:42-43, 15:16-23, 15:42-16:7, 16:21-26, 16:40-47, 23:36-40, Figs. 3, 6).

Petitioner argues that Bradford's first authenticator can be stored on "magnetic-strip cards" provided to the player during enrollment, or may be "an already existing player ID card." Pet. 18, 20-21, 24, 26 (citing Ex. 1004, 5:30-54, 6:3-13, 6:18-20, 13:23-33, 15:16-20).

Petitioner acknowledges that

> *Bradford* indicates the player entry is retrieved during the enrollment process because the

> player's second authenticator data is added to the player entry. *Bradford*, 15:60-63. *Bradford* does not indicate *how* the player entry is retrieved at the game device during enrollment.

Pet. 30 (citing Ex. 1003 ¶¶ 96-98). Petitioner then turns to Foss, explaining that

> *Foss* teaches "an enrollment process . . . for enabling a primary account holder (i.e., an existing customer 610) to enroll additional new customer(s) in the family stored value card program." . . . [t]o initiate enrollment, the customer is prompted "to swipe the **existing** stored value card" to "**continue** the **enrollment** process." The system "identifies the stored value card account associated with the existing customer 610. The stored value card account may be identified based on the data read from magnetic stripe 710 via card reader 706 . . . "

Id. at 27-28 (quoting Ex. 1005 ¶¶ 86, 88; citing Ex. 1003 ¶ 92) (citations omitted). Petitioner argues "[t]hus, *Foss* teaches, during an enrollment process, identifying an account associated with a user by reading account information stored on a magnetic stripe of a card." *Id.* at 28 (citing Ex. 1003 ¶¶ 93-94).

Petitioner argues that "*Bradford* in combination with *Foss* teaches that during *enrollment*, a user record stored in a database is retrieved by reading a card having unique user information thereon." *Id.* at 26 (citing Ex. 1003 ¶¶ 90-94). Petitioner asserts that a person of ordinary skill in the art would have looked to Foss because in

Bradford "the enrollment process is not complete when the attendant and player move to the game device. The player entry needs to be retrieved for associating the biometric information." *Id.* at 29 (citing Ex. 1003 ¶¶ 95-98). Petitioner argues that "a very well-known and simple method of retrieving an account record is swiping a card with the account information, as indicated by *Foss*." *Id.* (citing Ex. 1003 ¶¶ 92-98).

Finally with respect to claim limitation 1(c), Petitioner submits that Bradford in combination with Foss teaches the defined memory location is "in a local memory external to the card" because Bradford's player ID database (which includes the enrolled players' ID entries) is stored locally at a game device. Pet. 19, 21, 31-33 (citing Ex. 1004, 8:51-65, 9:57-63, 14:21-28, 14:42-43, 15:16-23, 15:42-16:7, 16:21-26, 16:40-47, Figs. 3, 6; Ex. 1003 ¶¶ 83-85, 100-102).

v. Limitation [1d] – determining if the defined memory location is unoccupied.

Petitioner next argues that "*Bradford* (as otherwise modified by *Foss*) as modified by *Yamane* teaches determining if a flag is set indicating a memory location is occupied/no longer occupied, as claimed [in claim 1]." Pet. 33-34. Petitioner points out that the '039 patent "envisions a method in which determining if the defined memory location is unoccupied is performed by checking the status of a flag that 'can be set to indicate that the memory location in question is occupied' and 'reset to indicate that the memory location in question is no longer occupied.'"

Pet. 33 (citing Ex. 1001, 9:25-37). Petitioner then relies on Yamane for disclosing a "process of registering the fingerprint information of a proper user on [a] CD-RW 1000" by first "determining whether a fingerprint has been registered by reference to a flag." Pet. 34-36 (citing Yamane ¶¶ 33, 39, 41, 45-47, 49, 52-54, Figs. 1-2).

Petitioner argues that "*Bradford* (as modified by *Foss*) as further modified by *Yamane* renders obvious Claim 1(d)" because "*Yamane* already teaches the purpose of its flag is to 'decide[] whether a fingerprint has been registered or not,' thus indicating the flag determines if fingerprint data has been stored or not." Pet 38 (quoting Ex. 1006 ¶ 52) (citing Ex. 1003 ¶¶ 104-105, 109). Petitioner argues that "*Bradford* teaches a player entry is enabled once the second authenticator data field is populated to include the second authenticator data." *Id.* (citing Ex. 1004, 17:47-50). Therefore, according to Petitioner, a person of ordinary skill in the art would have been motivated "to modify the process of creation of the player entry to set a flag to determine if the memory location comprising the second authenticator data field is occupied with the second authenticator data or if such needs to be completed." *Id.* (citing Ex. 1003 ¶¶ 108-111).

vi. Limitation [1e] – storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

Petitioner argues that "*Bradford*(as modified by *Foss*) as further modified by *Yamane* renders obvious Claim

1(e)." Pet 39-40 (citing Ex. 1003 ¶¶ 108-114). According to Petitioner, a person of ordinary skill in the art would modify Bradford based on Yamane's teachings such that

> the fingerprint data corresponding to the second authenticator data [in Bradford] is stored at a memory location comprising the second authenticator data field [taught by Bradford] . . . When the memory location is unoccupied, as determined by the flag [taught by Yamane] in the modified *Bradford* system, the fingerprint data is then input into and stored in the memory location comprising the second authenticator data field, as taught by *Bradford*.

Pet. 40 (citing Ex. 1003 ¶¶ 108-114). Petitioner argues that a person of ordinary skill in the art would have combined Bradford's and Yamane's teachings for the reasons discussed with respect to claim limitation 1(d). *Id.* (citing Ex. 1003 ¶ 114).

(b) Patent Owner's Arguments

Focusing initially on limitation 1[c], Patent Owner argues that Petitioner has failed to prove that Bradford, Foss, and Yamane, alone or in combination, render obvious claims 1 and 19 because the cited art does not teach "defining, dependent upon the received card information, a memory location in a local memory external to the card" as recited in the claims. PO Resp. 7 (citing Ex. 1001, 12:33-34). Specifically, Patent Owner argues that "a memory location in a local memory which corresponds to, but is

not contingent upon or determined by, the received card information is not 'dependent upon' under [Petitioner's] claim construction." *Id.* Also, with respect to limitations 1[d]-[e], Patent Owner asserts the prior art "does not teach 'determining if the defined memory location is unoccupied; and storing, if the memory location is unoccupied, the biometric signature at the defined memory location'" as required by these claims. *Id.* at 19.

Along with a focus on the claim limitations 1[c]-[e], Patent Owner presents additional arguments asserting that "a POSITA would not have looked to *Foss* in seeking to modify *Bradford*, and that "[a] POSITA would not seek to combine *Bradford* and *Yamane* as [Petitioner] suggests." *Id.* at 17-19, 23-25. We address these arguments in turn.

(c) Whether the combination of Bradford and Foss teaches limitation [1c]"defining, dependent upon the received card information, a memory location in a local memory external to the card"

Patent Owner argues that Bradford and Foss fail to teach the claimed "defining [a memory location]," which "a POSITA would consider . . . especially in the context of enrollment, to mean 'setting' or 'establishing,'" and "not finding or identifying something that has already been defined" and not "'pointing to' a memory location in which data is already stored," as Petitioner contends. PO Resp. 7-8 (citing Ex. 2001 ¶ 41); PO Sur-Reply 7. Patent Owner also asserts that a "temporal structure is implicit" in claim 1, which

> first requires card information be received . . . [a]fter, and only after, that card information is received can a memory location be defined. . . . [p]ut differently, **after** card information is received, the claim requires defining a memory location "contingent on" the received card information or that a defined memory location is "determined by" the received card information.

PO Resp. 8 (citing Ex. 2001 ¶¶ 42-43, 45; Ex. 2003, 15:12-16:6). Patent Owner submits that Dr. Sears, Petitioner's Declarant, admitted that claim 1's steps are framed by *a temporal structure* in which "the card information is obtained first, the memory location is defined by the card information second, and the biometric signature is stored in the defined memory location third." PO Sur-Reply 1-2 (citing Ex. 2003, 15:21-16:6; Ex. 1001, 12:29-38; PO Resp. 8; Pet. 26). Patent Owner observes that "Dr. Sears' admission . . . comports with the construction of the challenged claims put forth by Dr. Easttom, [Patent Owner's] expert. . . . [who] opined that the term 'defining' means 'setting' or 'establishing,' citing to the specification of the '039 Patent for support." *Id.* at 2 (citing Ex. 2001 ¶ 41; Ex. 1001, 2:64-67, 7:47-49); *see also* PO Resp. 7-8 ("in the context of the claim language, a memory location is set or established") (citing Ex. 2001 ¶¶ 41-43).

Despite not providing an explicit claim construction for "defining," most of Patent Owner's arguments center around the meaning of this word in the context of limitation [1c]. Therefore, we initially address the meaning of "defining" in the context of limitation [1c] as a whole.

Appendix B

i. The meaning of "defining"

Besides the agreed-upon construction of "dependent upon" as meaning "contingent upon or determined by," Patent Owner argues that "defining" also has a particular meaning, that is—"setting" or "establishing." PO Resp. 8. As issued, limitation [1c] reads:

> [1c] *defining*, *dependent upon* the received card information, a memory location in a local memory external to the card;

Ex. 1001, 12:33-34 (emphasis added). Given Patent Owner's proposed interpretation, we have:

> [1c] [setting or establishing], [contingent upon or determined by] the received card information, a memory location in a local memory external to the card;

We don't take issue with the alternative words specifically, but we observe that considering all the alternatives is repetitive and can lead to confusion because there are now 24, i.e., (4x3x2x1) permutations of the words/terms "setting," "establishing," "contingent upon," and "determined by," apparently deemed necessary to understand, what on its face, is not a particularly unwieldly claim recitation.

Claim limitation [1c] is best understood by reading the specification of the '193 patent, for example the Abstract, which reads:

Appendix B

> The disclosed Biometric Card Pointer arrangements store (207) a card user's biometric signature in a local memory (124) in a verification station (127) the first time the card user uses the verification station (127) in question. *The biometric signature is stored at a memory address (607) defined by the card information (605) on the user's card (601).* All future uses of the particular verification station (127) by someone submitting the aforementioned card (601) requires the card user to submit both the card and a biometric signature, which is verified against the signature stored at the memory address defined by the card information (605) thereby determining if the person submitting the card is authorized to do so.

Ex. 1001, Abstract, (57) (emphasis added).

We have no major issue with Patent Owner's interpretation of "defining" as also meaning "setting" or "establishing." Considering the abstract and the specification of the '039 patent, what "defining, dependent upon . . . " means as a whole, in the context of claim 1 and "a method of enrolling," is that during an *enrollment* process, the claimed "biometric signature," e.g., a fingerprint, is not yet stored in the memory and no memory location or address has been "set" or "established" for the fingerprint. When the fingerprint, and then the card, is provided to the system during enrollment, the card information provides data that establishes *where, e.g.*, at what memory location

or address, the system will *store* the fingerprint data.[8] *See* Tr. 61:14-16 (Patent Owner's counsel arguing that "[w]e are saying it's defining a memory location into which the biometric data is going to be stored"). In all subsequent *verification* processes, when a person submits their card and fingerprint, the submitted fingerprint "is *verified* against the [fingerprint] stored at the memory address defined by the card information thereby determining if the person submitting the card is authorised to do so." *Id.* at 3:8-11; *see also* Tr. 36:23-37:3 (Patent Owner's counsel explaining during oral argument that "[i]f we look at these claims the way they're supposed to be looked at, as two discrete processes, then defining the memory location becomes very clear. It's what you're doing in the first instance to figure out *where you're going to store* the biometric data, and that is what is dependent upon the card information") (emphasis added).

Notably, because of the use of the term "defined" in claim 1 and dependent claim 2, Petitioner does not agree with Patent Owner's interpretation that "defining" means "setting" or "establishing." Pet. Reply 1-12. Petitioner argues that "[Patent Owner's] construction requires that 'defining' in claim 1 be construed differently than 'defined by' in claim 2." *Id.* at 10.

We acknowledge Petitioner's position, and take note of Petitioner's use of the words "find" and "identifying" to

8. We use the terms "memory location" and "memory address" interchangeably because, in terms of computer memory, an "address" is well-understood as "[a] number specifying a location in memory where data is stored." MICROSOFT COMPUTER DICTIONARY, 5th Ed. (2002) Microsoft Press.

explain "define," but we do not have the same concerns.[9] Pet. Reply 3-5. In claim 1, following the "defining" step there is recited in past tense, "the defined memory location." Ex. 1001, 12:35, 39. Claim 2 recites "the memory location, . . . defined by the subsequently presented card information." *Id.* at 12:49-50. There is some merit to Petitioner's assertion here, because "defined" should be construed the same way in both claim 1 and claim 2. *See Phillips*, 415 F.3d at 1314 (explaining that "[b]ecause claim terms are normally used consistently throughout the patent, the usage of a term in one claim can often illuminate the meaning of the same term in other claims"). We appreciate the argument because claim 2 recites "defined by the *subsequently* presented card information," meaning that for verification, following enrollment, this is not the first time the card is being presented. However, in claim 2 "the memory location" is the object of the preposition "defined by . . . " And, a reasonable reading of "the memory location . . . defined by" in claim 2 could

9. In the context of these claims we do not understand "establish[ing]" and "identify[ing]" as any better or worse interpretations of "defining." Consider for example the following sentences:

> -The witness *identified* the defendant as the person she observed in the store.
>
> -The witness *established* the defendant as the person she observed in the store.

A reasonable reading of both sentences is quite similar—the witnesses' recollection is that she saw the defendant in the store. On the other hand, one would never state "the USPTO was identified in 1790," and would more likely say, "the USPTO was established in 1790."

also be understood grammatically similar to the past tense "defined memory location" in claim 1. Thus, consistent with claim 1, claim 2 can be understood as "the memory location . . . [established] by the subsequently presented card information." *Id.* Considering the meaning of the claims as a whole, as discussed above, Patent Owner's interpretation that "defining" means "setting" or "establishing" is not entirely inconsistent.

Importantly, and to make one thing clear, we do not understand that "defining . . . a memory location," or Patent Owner's alternative wording, "establishing" or "setting," means "[*creating*] . . . a memory location in a local memory." We bring this up because Patent Owner's counsel argued during the oral hearing that "there's nothing in Bradford that says you take that ID off the card *and create* the memory location based on that." Tr. 62:14-16 (emphasis added). Also, in the Patent Owner Sur-Reply, Patent Owner argues that "the memory location cannot already exist." PO Sur-Reply 2. While we might agree that "the memory location cannot [already be defined]," for the following reasons we do not agree that it "cannot already exist."

Coincident with the arguments raised by Petitioner above with respect to a consistent meaning of "defining," we point out that Patent Owner's interpretation of "defining" is somewhat of a moving target. Patent Owner argues that it is something more than "pointing to" or "finding," and perhaps means "creating." *See* PO Resp. 9 (Patent Owner arguing that "*Bradford*, notably, does not teach utilizing the first authenticator to create a player ID entry"). What Patent Owner's interpretation encompasses is not always clear. First, Patent Owner's

expert's interpretation is that "defining" means "setting" or "establishing." *See id.* (Patent Owner stating that its expert "Dr. Easttom opined that the term 'defining' means 'setting' or 'establishing.'"); *see also* Ex. 2001 ¶ 41. Second, whatever Patent Owner's counsel is asserting as to the meaning of "defining," Dr. Easttom has not advanced any interpretation or construction that "defining" means "creating" a database location. Thirdly, Patent Owner has not pointed to any recitation of the word "create" in the specification of the '039 patent; nor has Patent Owner provided any technical explanation or reference to the written description as to what "creating" a memory location entails.[10] If anything, as Petitioner argues, the specification uses the word "points" and "pointer" to describe how the memory address or location is defined. For example, as shown in Figure 4 below, the "card data points to" an existing location 607 in a database "defined by card data."

10. There is no technical or explanatory description in the '039 patent explaining *how* the card data creates or otherwise brings into existence a memory address. To the extent the written description lacks such technical explanation, we do not have jurisdiction to address the issue of enablement. *See* 35 U.S.C. § 112 ("The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.")

Appendix B

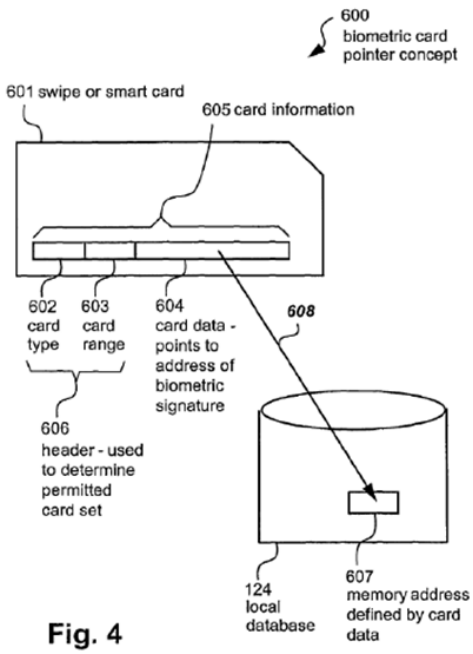


Fig. 4

Figure 4 states that as part of card information 605 the "card data [604] points to address of biometric signature." Ex. 1001, Fig. 4. Despite such disclosures throughout the specification, Patent Owner argues strenuously that "defining" does not mean simply "pointing to." PO Reply 7-17.

Regardless, we can give Patent Owner the benefit of the doubt that during an enrollment process the card data is provided for "setting" or "establishing" what memory location, or address, in the local database the fingerprint is to be stored. Even with this understanding, however, the card data does not actually *create* a memory location.

The memory location already exists, it has just not yet been "set" or "established" by the card data as the memory location at which the fingerprint data is stored.

As expressed by claim 1 itself, this is the logically correct conclusion. Claim limitation [1d] recites "determining if the defined memory location is unoccupied." Ex. 1001, 12:35. If the card data somehow *created* a memory location, then there would be no reason to determine if the memory location were unoccupied. Indeed, Patent Owner's counsel stated during oral argument with respect to "defining" that "[t]he only logical use of that term is that defining means *to identify* a memory location into which the biometric data is going to be stored." Tr. 61:5-7 (emphasis added). During the oral hearing Patent Owner's counsel was specifically asked about the memory location:

> [THE BOARD]: What is a memory location? Is it a physical address within the memory?
>
> [PATENT OWNER'S COUNSEL]: Yes, Your Honor. That's one good way of looking at it. So you look at the memory structure for any standard-type memory, and it's just identifying an address in the memory location stored here.

Id. at 33:15-20. Indeed, when questioned further, Patent Owner's counsel was reluctant to use the word "create":

> [THE BOARD]: So as far as timing, you're saying the timing has -- I mean, it goes back to the definition of defining, right? I mean, you're

> saying the card information has to be used in order to create the locations of that information that stored in the database.
>
> [PATENT OWNER'S COUNSEL]: To define it, I would say, Your Honor.
>
> [THE BOARD]: Well --
>
> [PATENT OWNER'S COUNSEL]: Creating it. The memory location exists. It's going to be figuring out where to use your -- the answer to your question earlier, where -- what physical address in the memory --

Id. at 47:3-14. This discussion reveals the linguistic tangle Patent Owner faces in distancing the claimed "defining" step from Bradford and Foss.

Overall, in terms of "defining" and limitation [1c] as a whole, we understand that during an *enrollment* process, the claimed "biometric signature," e.g., a fingerprint, is not yet stored in the memory, and no memory location or address has been "defined," as in "set" or "established," in the memory for storing the fingerprint, until card information is received. Once the card information and fingerprint is received during enrollment, the card information provides data that establishes *where*, i.e., at what memory location or address, the system will *store* the fingerprint data.

ii. The temporal requirements of claim 1 and whether claim 1 "first requires card information be received . . . After, and only after, that card information is received can a memory location be defined"

Patent Owner contends that a "temporal structure is implicit" in claim 1, which "first requires card information be received . . . [a]fter, and only after, that card information is received can a memory location be defined." PO Reply 8 (citing Ex. 2001 ¶ 45).

We agree that there is a temporal aspect to claim 1. We agree that the biometric signature, e.g., a fingerprint, is not *stored*(step [1e]) until after receiving the card information (step [1a]). Ex. 1001, 12:29-38. This is because it is the card information that tells the system where, i.e., establishes (defines) a specified memory location to store the fingerprint at step [1c]. What we do not agree with, as Patent Owner appears to intend with this argument, is that a memory location does not already exist, or is somehow created only upon presentation of the card information. Indeed, as we explain below, the limitations of claim 1 do not exclude an existing user or player record entry from being a memory location in a database where the fingerprint is stored.

For one thing, claim 1 recites specifically "[a] method . . . *comprising* the steps of . . . " *Id.* at 12:29-30. It is well-settled that "comprising" is an open-ended term and

"[i]n the patent claim context the term 'comprising' is well understood to mean 'including but not limited to.'" *CIAS, Inc. v. All. Gaming Corp.*, 504 F.3d 1356, 1360 (Fed. Cir. 2007). Patent Owner has not pointed to any persuasive part of the specification of the '039 patent describing that a user or player record cannot exist prior to the use of the card for "defining . . . a memory location" where a biometric signature is to be stored. We agree that *prior* to use of the card *a memory location for storing a biometric signature* is not "established" or "set," but we do not agree that the memory location does not exist or that the language of claim 1 excludes the existence of a database record, and even a database record including user record information in the memory location.[11]

Secondly, during oral argument, Patent Owner's counsel confirmed that "enrollment" in the context of claim 1 requires the "receiving card information" to *identify* a memory location for storing a biometric signature:

> [THE BOARD]: But claim 1 doesn't say that the card data defines it. It says defining dependent upon the received card information. It's --
>
> PATENT OWNER'S COUNSEL]: Your Honor, going -- yes, Your Honor, but going back to the

11. "[I]n general, a patent claim reciting an apparatus 'comprising' various components merely means that the apparatus 'includ[es] but is not limited to' those components." *Rothschild Connected Devices Innovations, LLC v. Coca-Cola Co.*, 813 F. App'x 557, 562 (Fed. Cir. 2020) (nonprecedential) (citations omitted).

conversation you and I had during my argument in chief, if you look at what dependent upon means, it's contingent upon. *You can't have thememory location before you have the card data.*

. . .

[PATENT OWNER'S COUNSEL]: . . . But it is the card information that determines what the memory location is going to be. So when Ms. Bailey said that any time a card is used to locate information in memory, that is defining the memory location, that simply isn't true, according to the definition that [Petitioner] proposed. But more importantly, when we look at claim 1, it talks about an enrollment process. If defining were to include simply identifying information where the data is stored, according to the order of steps in claim 1, the biometric information isn't stored yet, so what would it be defining?

There's nothing to define at that point. There has been no storage of that biometric information, according to [Petitioner's] definition. *The only logical use of that term is that defining means to identify a memory location into which the biometric data is going to be stored.*

Tr. 59:11-61:14 (emphases added).

Keeping in mind the meaning of limitation [1c] based on the claim language and specification, the interpretation that stays true to the claim language and most naturally aligns with the patent's description of the invention is that, during an *enrollment* process, the claimed "biometric signature," e.g., a fingerprint, is not yet stored in the memory and no memory location or address has been established in the memory for the fingerprint. When the card is provided during enrollment, the card information provides data that establishes *where*, i.e., at what memory location or address, the system is *to store* the fingerprint data." Section II.4.(c)(i).

Therefore, based on our determination of the proper interpretation of "defining," we agree with Patent Owner's counsel that at limitation [1c] "according to the order of steps in claim 1, the biometric information isn't stored yet." Tr. 60:25-61:1. We also agree, based on all the evidence before us, and as Patent Owner's counsel argued, that "[t]here has been no storage of that biometric information, . . . *[t]he only logical use of that term is that defining means to identify a memory location into which the biometric data is going to be stored*." Tr. 61:5-7 (emphasis added). On the complete record before us, Patent Owner's explanation that "defining means to *identify* a memory location" is entirely consistent with Dr. Easttom's explanations, and our interpretation that the card information establishes *where*, i.e., a memory location or address, the system is to *store* the fingerprint data.

Therefore, based on the proper interpretation and understanding that the meaning of "defining" includes

"sets" or "establishes," we can agree with Patent Owner that "[a]fter, and only after, that card information is received can a memory location be defined" for the biometric signature. PO Reply 8 (citing Ex. 2001 ¶ 45).

(d) Obviousness of limitation [1c] based on Bradford and Foss

We note that the parties are somewhat in agreement about Bradford's disclosure, that is—Bradford discloses a casino attendant, for example, providing a player entry in the player ID database *prior* to a first use of the first authenticator, e.g., a player ID card. Pet. 11 (citing Ex. 1004, 14:25-43, Fig. 6, 15:37-38); *see also* PO Resp. 2 (Patent Owner asserting that "the experts for each party agrees, the database entry in the prior art (which Apple's expert characterized as 'the memory location') is created **before** card information is received").

However, we do not find that the player ID database being created prior to use of the player ID card in Bradford is excluded from the scope of claim 1. As discussed above, the temporal nature of claim 1 relates to "receiving card information," "receiving the biometric signature," and then "storing . . . the biometric signature" dependent, i.e., contingent on the card information. As we established, claim 1 does not recite, nor does "defining" mean, that a memory location cannot exist prior to use of the card as Patent Owner argues. What claim 1 requires is the initial "establishment" or "setting" of a memory location for storage of the fingerprint. As we discussed above, claim 1, including limitation [1c], would have been understood by

a person of ordinary skill in the art, to mean that during an *enrollment* process, the claimed "biometric signature," e.g., a fingerprint, is not yet stored in the memory, and no memory location or address has been established in the memory for the fingerprint. Once the card is provided during enrollment, the card information provides data that establishes *where*, i.e. at what memory location or address, the system is to store the fingerprint data.

Petitioner and Patent Owner also appear to agree that Bradford does not expressly disclose *how* a player entry is located or retrieved during an exemplary *enrollment* at a game device in the casino prior to recording the new player's fingerprints in the player ID database. *See* Pet. 26-27 (Petitioner arguing that "*Bradford* teaches the enrollment process that began at the customer service counter is continued and completed at the particular game device but is not express about *how* the previously-created player entry in the player ID database is located and accessed for completion on the particular game device"); *see also* PO Resp. 17-18 (Patent Owner arguing that "[Petitioner] is correct that *Bradford* does not teach how a player entry is retrieved during the creation of that player's ID entry").

To this end, Petitioner argues that "*Bradford* . . . is not express about how the previously-created player entry in the player ID database is located and accessed [during enrollment] for completion on the particular game device." Pet. 26-27. Petitioner submits that "*Foss* teaches, during an enrollment process, identifying an account associated with a user by reading account information

stored on a magnetic stripe of a card"—in other words, "a continuation of an enrollment process via presentation of a card to a card reader." Pet. 27-28 (citing Ex. 1005 ¶¶ 86, 88, Figs 7-8; Ex. 1003 ¶¶ 92-94). Petitioner asserts that based on Foss "[a] POSITA would have found it obvious that a convenient and expected method for locating the player entry associated with the player ID on the card would have been to read the player ID from the card via the card reader [(as described by Foss)] on the particular game device [(where enrollment occurs in Bradford)]." Pet. 27 (citing Ex. 1003 ¶¶ 92-94); *see also* Pet. Reply 19 ("The Petition maps 'receiving card information' by modifying *Bradford* via *Foss* to swipe *Bradford's* player ID card using *Bradford's* card reader.").

On the other hand, Patent Owner contends that "*Foss* does not cure the deficiencies of *Bradford* in failing to teach" the "defining" limitation. PO Resp. 9. Patent Owner contends Foss is deficient (and does not cure Bradford) for multiple reasons, which we discuss in turn below.

Patent Owner argues Foss is deficient because "*Foss* does not teach enrolling a single-user account by utilizing received card information to define a memory location"; "[i]nstead, *Foss* is directed towards expanding an existing customer account." PO Resp. 9-10 (citing Ex. 2001 ¶ 53; Ex. 1005 ¶¶ 85-86, 88, Figs. 7-8). Relatedly, Patent Owner argues Foss's description of swiping an existing card to enroll additional users (and create respective multi-user accounts) "would be illogical when applied to the enrollment of an individual account" because "unlike [Foss's] family card program, *there would be no existing account to reference* when enrolling an individual" (in

Bradford). PO Resp. 11 (emphasis added) (citing Ex. 1005 ¶ 88, Fig. 10).

Petitioner replies that the obviousness analysis relies on Foss "only . . . for clarification of receiving card data during an *enrollment* process" to "locat[e] a user's record to add additional information." Pet. Reply 23-24 (citing Pet. 2, 17, 25-30); *see* Pet. 26 ("*Bradford* in combination with *Foss* teaches that during enrollment, a user record stored in a database is retrieved by reading a card having unique user information thereon."); *see also id.* at 28 ("*Foss* teaches, during an enrollment process, identifying an account associated with a user by reading account information stored on a magnetic stripe of a card.") (citing Ex. 1003 ¶¶ 90-94).

Petitioner's declarant, Dr. Sears, explains in detail how Petitioner's obviousness analysis relies on Foss for using a card during an enrollment process to identify an account associated with a user by reading information stored on the card using a card reader. Ex. 1003 ¶¶ 90-98. Dr. Sears explains that the Bradford-Foss combination "modif[ies] *Bradford's* enrollment process to include swiping the player ID card at the game device to retrieve the associated player ID entry, as taught by *Foss*." *Id.* ¶ 95. Based on Dr. Sears' testimony, Petitioner concludes that, "[r]egardless of the type of account in which a user is enrolled, *Foss's* teachings regarding locating a user's record to add additional information is relevant to the same process being performed in *Bradford*." Pet. Reply 23.

We agree with Petitioner's assessment and credit Dr. Sears' testimony. Both Foss and Bradford describe an enrollment process in which a customer's existing database record is established as a location for storing additional information, e.g., a player's data and information entered by an authorized person into the player ID database at Bradford's step 602, a player's first authenticator data that is read and thereafter kept in the database in Bradford, and a customer's stored value card account/primary account in Foss.

Although Patent Owner contends that, contrary to Foss, there is no existing customer in Bradford and "there would be *no existing account to reference* when enrolling an individual" in Bradford (*see* PO Resp. 10-11 (emphasis added)), Bradford actually discloses and teaches that *some of the customer's information*—such as "the initial data from the player [entered by an authorized person] into the database"—occurs before "the attendant asks the player if they need training" and enters fingerprint data. Ex. 1004, 14:21-31, 15:29-31.

As explained in detail by Petitioner's declarant, Dr. Sears,

> *Bradford* teaches that during enrollment a player's entry is created and stored with first authenticator data, the player is provided a player ID card with the first authenticator data, the casino attendant and player move to a game device for training and entry of the player's fingerprint information.

Ex. 1003 ¶ 90 (citing Ex. 1004, 15:42-16:20). We find Dr. Sears' testimony credible and supported by the disclosure of Bradford, and we are persuaded that a customer's initial information (i.e., the information saved in Bradford's player ID database during enrollment before recording the biometrics) represents account information that is available for subsequent retrieval (e.g., retrieval during Bradford's recording of the biometrics). Pet. 19-20, 26, 29-30 (citing Ex. 1003 ¶¶ 83-85, 90-98).

We find little weight in Patent Owner's argument that Foss cannot be relevant to Bradford because "*Bradford* does not contemplate creating multi-user accounts [as in Foss]." PO Resp. 11. Just as Bradford's completion of enrollment, including setting up a user account, is *in progress* until the biometric signature is added to the account, Foss's family stored value card account 600 is an in-progress enrollment process being completed when a secondary stored value card account (e.g., 604) is added thereto. *See* Ex. 1005 ¶¶ 85-86, 88, Figs. 6, 8; Pet. Reply 24 ("In the combined, modified system, an account exists prior (per *Bradford*) to receiving the card information (per *Foss*), whether or not the biometric signature has yet been stored for that account.").

Overall, we are persuaded that Petitioner and Dr. Sears have shown a preponderance of evidence that a person of ordinary skill in the art, who was aware of all the prior art in the relevant field, would have recognized that Bradford does not expressly disclose *how* a user's ID information entry would have been retrieved from a database. Petitioner and Dr. Sears have further shown

that, in turn, the person of ordinary skill in the art would have looked to Foss, which more specifically teaches that information on a user's ID card was a known way to define, that is to "establish" or "set" a memory location, for example with the user's player ID record entry, where a user's input of a second authenticator, e.g., a fingerprint, would be stored.

We acknowledge Patent Owner's extensive arguments regarding Bradford's failure to teach (alone, or in combination with Foss) "first receiving card information and then defining a memory location based on that received card information." *See* PO Resp. 9-17; PO Sur-Reply 3-4, 7-10. For example, Patent Owner argues that Petitioner's expert, Dr. Sears, "testif[ied] that *Bradford* teaches a process in which the steps are reversed—a memory location is defined before any card information is received." PO Sur-Reply 3 (citing Ex. 2004, 31:12-18). We do not agree that Dr. Sears' testimony conflicts with claim 1. When claim 1 is properly interpreted, as we have addressed herein, the creation of a player account in Bradford, or Foss, prior to receiving the card information does not preclude subsequently identifying a memory location (among preexisting memory locations/addresses within the preexisting player ID database) and establishing that memory location as the location where new biometric data, e.g., a player's fingerprint, is going to be stored. *See* Pet. Reply 23-24; Pet. 26-28. That is, creating a player account in Bradford does not preclude subsequently "defining, dependent upon the received card information, a memory location," as recited in claim 1. Pet. Reply 23-24; Pet. 26-28.

In other words, we do not agree that claim 1 excludes the existence or creation of a player account record in "a memory location" prior to receiving card information. Claim 1 precludes the establishment or setting of a memory location for the "biometric signature" prior to receiving card information, but "defining" does not mean that the memory location is created or somehow brought into existence only after "receiving card information."

Considering our claim interpretation and the parties' interpretations and constructions of limitation [1c], we have explained why Patent Owner's arguments do not undermine Petitioner's contentions and supporting evidence, and why we agree with Petitioner that a person of ordinary skill in the art would have understood that the Bradford-Foss combination teaches all the elements in limitation [1c]. Specifically, we are persuaded on the complete record now before us that where Bradford discloses an enrollment process including receiving card information and biometric information, but does not describe specifically *how* to store the biometric information, Foss teaches how, i.e., using card data to define, that is—to establish or set a memory location, e.g., the player's user account, for storage of the biometric information in a local memory.

(e) Whether Bradford and Foss are properly combined.

Patent Owner contends that a person of ordinary skill in the art would not have combined Bradford and Foss. PO Resp. 2-3, 17-19. In particular, Patent Owner argues an

ordinarily skilled artisan would not have looked to *Foss* because "*Bradford* teaches the attendant's card being placed in the machine in order to access the privileged screen in which the player's entry is retrieved to complete registration" such that the player's first authenticator card "could not, then, be 'read by a card reader to retrieve the stored first authenticator data.'" *Id.* at 18.

We do not agree with Patent Owner. Rather, we find Petitioner's position persuasive that "*Bradford* expressly envisions embodiments not 'requiring' the attendant's card staying in the machine during enrollment." Pet. Reply 19-20, 22-24 (citing Ex. 1004, 14:31-41, 14:28-37). Bradford, for instance, teaches a casino attendant accessing privilege screens using an RFID tag which does not require the casino attendant's card remaining in the machine. *See* Ex. 1004 14:28-37 (Bradford describing that "[i]n order to open the privileged screens allowing data entry, the authorized casino personnel will be required to use their own employee identification cards (badges, **RFID** tag, . . . ")). Importantly, we credit the testimony of Petitioner's expert, Dr. Sears, who testifies that to a person of ordinary skill in the art, "swiping the player ID card would have been a logical, fast, and simple method of retrieving the player ID entry." Ex. 1003 ¶ 96. Dr. Sears relies on express teachings in Foss, testifying that "*Foss* also teaches that the 'existing customer 610 swipes the existing stored value card 508 to further continue the enrollment process,' and the 'stored value card account may be identified based on the data read from the magnetic stripe 710 via card reader 706.'" *Id.* ¶ 94 (quoting Ex. 1005 ¶ 88).

Dr. Sears testifies further that "modifying *Bradford* according to the teachings of *Foss* would have had a reasonable expectation of success" because "*Bradford* teaches both hardware and software used for reading player account information from a card's magnetic strip" as well as "programmed functionality for matching a unique data sequence stored on a card as first authenticator data to the first authenticator data in the player entry and thus retrieving a corresponding player entry." *Id.* ¶ 98. Dr. Sears testifies that

> modifying *Bradford* to swipe the player ID card having the first authenticator data to retrieve a partially-completed player entry would have been applying the known technique of swiping a card that has a magnetic stripe with account information (taught by both *Bradford* and *Foss*) to a known card reader device (taught by *Bradford*).

Id. ¶ 97. Thus, Dr. Sears concludes that "[s]uch a modification would have yielded the predictable result of retrieving the player entry that matches the first authenticator data read from the player ID card." *Id.*

We further credit Dr. Sears' testimony that a person of ordinary skill in the art: (i) would have had a reason to combine the teachings of Bradford with Foss, which both relate to setup as well as augmentation of users' accounts; and (ii) would have known how to employ a customer's authenticating card to identify the customer using a card reader during an enrollment process, so that the teachings

of Foss would have been applicable to Bradford's two-factor enrollment process. Ex. 1003 ¶¶ 62, 90, 92-102. Patent Owner's observation that "*Bradford* . . . requires biometrics for at least the second authenticator," while "none of [Petitioner's] cited portions [of Foss] contains a reference to biometrics" (PO Resp. 19), does not explain why a person of ordinary skill in the art would not have recognized, as suggested by Foss, that the authenticating card could still be used to retrieve a partially-completed player entry in Bradford, before the processing of biometrics. *See* Ex. 1003 ¶ 98 (Dr. Sears testifying that swiping a user ID card to retrieve a user entry "according to *Foss's* teachings encompasses performing a known look-up process for the player entry during the enrollment for the two-level authorization process, as taught by *Bradford*"). The test for obviousness is what the combined teachings of those references would have suggested to those of ordinary skill in the art. *See In re Mouttet*, 686 F.3d 1322, 1331 (Fed. Cir. 2012) ("A reference may be read for all that it teaches, including uses beyond its primary purpose.").

(f) Whether the combination of Bradford, Foss, and Yamane teaches limitation 1(d)"determining if the defined memory location is unoccupied"

According to Patent Owner, Yamane's "protect area 1002-1 of a rewritable area 1002 is a *pre-defined* memory location, not a memory location which is defined by, contingent on, or determined by, any other information, much less received card information as the claim requires."

PO Resp. 20 (emphasis added). Patent Owner argues that "the inclusion of *Yamane* would seek to determine if a specific, pre-defined memory location was unoccupied," which is distinct from the claimed memory location "defined dependent upon received card information." *Id.* at 20-21 (emphases added) (citing Ex. 2001 ¶ 57); *see also* PO Sur-Reply 12-13 ("*Yamane* teaches checking whether a specific, pre-defined memory location is occupied via a flag, whereas the claim describes "determining if *the defined memory location* is unoccupied").

In response, Petitioner points out that "the Petition . . . relies on *Yamane* only for a method of checking a fingerprint presence flag." Pet. Reply 26 (citing Pet. 33-37). This argument, Petitioner asserts, "is improperly engaging in bodily incorporation of features from a secondary reference into a primary reference." *Id.*

We find Petitioner's arguments and evidence persuasive because Petitioner relies upon Bradford and Foss for the claimed *function*of "defining . . . a memory location," into which the biometric signature is eventually stored. *See* Pet. 17 ("*Bradford* in combination with *Foss* teaches Claim 1(c)."); *see also id.* at 19 (quoting Ex. 1004, 40:46-48) ("*Bradford* teaches an enrollment process "for the creation of an entry having biometric data in a player ID database."). And, besides bodily incorporating features, i.e., a memory location of Yamane, that Petitioner does not assert with respect to the "defining" limitations in [1c], Patent Owner's argument conflates the "defining" step in limitation [1c] with [1d]. Limitation [1d] follows [1c], and simply "determin[es] if the memory location is unoccupied." Ex. 1001, 12:35.

Secondly, and with respect to Yamane itself, claim 1 is a method claim, whereas Patent Owner's argument is based upon a specific type of "protect area" memory, e.g., a structural aspect of memory. PO Resp. 20. Apart from the assertion that a "protect area" is "pre-defined," Patent Owner's argument does not explain *how* the memory is defined, or pre-defined for that matter, except from the functional vantage point of the "received card information." In other words, the claim does not limit what type or structure of external local memory can be set or established as a memory location for the biometric signature, and Patent Owner does not explain sufficiently why "received card information" could not functionally establish a "protect area" of an external memory structure, as a memory location to store data, such as the biometric signature.

Specifically considering limitation [1d], the Petition explains that

> User information 60 and fingerprint information 70 are stored in a protect area 1002-1 of a rewritable area 1002 of the CD-RW. *Yamane*, [0039], FIG. 1. During a "registration process" (i.e., enrollment), fingerprint information 70 comprising user ID 70-1 and fingerprint data 70-2 are obtained.
>
> . . .
>
> *Yamane* discloses a "process of registering the fingerprint information of a proper user on the

> CD-RW 1000." *Yamane*, [0049], FIG. 2. *Yamane* expressly discloses determining whether a fingerprint has been registered by reference to a flag . . .

Pet. 34-37. Regardless of whether "protect area 1002-1" is "pre-defined" and whether the claim language means something different, Petitioner relies on Yamane mainly for "determining" whether the memory location is occupied or not, based on the presence or absence of a flag. *See* Ex. 1003 ¶ 104 (Dr. Sears explaining that "*Yamane* teaches that during an enrollment process, storage of a fingerprint at a memory location is determined based on the presence or the absence of a flag").

To the extent necessary, we also do not find that Petitioner's Bradford-Foss-Yamane combination relies on a memory area that is "a pre-defined" memory location as Patent Owner asserts. *See* PO Resp. 20. Patent Owner appears to contrast "pre-defined" with "card-defined." *Id.* at 21. Yamane describes "protect area 1002-1" as a "rewritable area 1002" that is "a data storage region [of CD-RW 1000] . . . in which data can be rewritten," protect area 1002-1 being an area "in which written data is protected by encryption performed by a software." Ex. 1006 ¶¶ 29, 31. Thus, the term "protect" in Yamane (i.e., in "protect area 1002-1") refers to a data storage region/memory portion for which data written therein is "protected by encryption performed by a software," not to a memory portion that is somehow functionally "pre-defined" so as to exclude the storage of information based on separate card data. *See* Ex. 1006 ¶ 31(Yamane

explaining that "[t]he rewritable area 1002 is constituted by a protect area 1002-1 in which written data is protected by encryption performed by a software").

Patent Owner next contends that an arrangement produced by the Bradford-Foss-Yamane combination "would be immaterial to *enrollment*, as the *pre-defined memory location, prior to such enrollment, would necessarily be unoccupied*." PO Resp. 21 (citing Ex. 2001 ¶ 58). Besides the fact that Petitioner is not relying on Yamane's alleged "pre-defined" memory location but on the local memory "player ID database" disclosed by Bradford, claim 1 does not condition the "defining" step [1c] on prior knowledge or information as to whether the "defined" memory location is occupied or not. Pet. 20. Limitation [1d] recites "determining if the defined memory location is unoccupied"—irrespective of any specified knowledge regarding occupancy of the local memory's memory locations. *See* Ex. 1001, 12:29-38.

Patent Owner further argues that Petitioner's reliance on "system-wide audits for records missing biometric signatures" is unsupported by Bradford, Foss, or Yamane, and "[e]ven if a POSITA would have had it in mind to run system-wide audits, these audits would be worthless when enrolling individual players, as in *Bradford*." PO Resp. 21 (citing Ex. 2001 ¶¶ 57-59).

Even if Patent Owner's position here is correct, the Petition's discussion of the Bradford-Foss-Yamane combination is not limited to a rationale based on system-wide audits. *See* Pet. Reply 26. Rather, the Petition (and supporting evidence) include "lengthy discussion

regarding obviousness of modifying *Bradford* to include *Yamane's* flag to indicate the memory is unoccupied," for example referencing "the benefit to *Bradford's* system to determine if an entry in the player ID database is 'complete, valid, or enabled' and that setting flags was well-known." *Id.* at 26-27 (citing Ex. 1003 ¶¶ 103-112; Pet. 39 (citing Ex. 1001, 17:14-26)). As discussed *infra*, we find that Petitioner provides persuasive rationale for combining the teachings of Yamane with those of Bradford and Foss. Pet. 37-39; Ex. 1003 ¶¶ 108-112.

Considering all the evidence and the parties' arguments before us, we are persuaded that Petitioner has shown a preponderance of evidence that Yamane, in combination with Bradford and Foss, teaches limitation [1d].

(g) Whether the combination of Bradford, Foss, and Yamane teaches limitation [1e]"storing, if the memory location is unoccupied, the biometric signature at the defined memory location"

According to Patent Owner, similar to the arguments for limitation [1d], "*Bradford* in view of *Yamane* does not teach the 'storing' limitation because *Yamane* relies on a pre-determined memory location whereas the location of *Bradford's* putative 'defined memory location' is, in actuality, undefined." PO Reply 21 (citing Ex. 2001 ¶ 57); *see also* PO Sur-Reply 13. We find this argument unpersuasive because, as discussed *supra*, Petitioner relies on Bradford, not Yamane, for "defining . . . a memory location."

Patent Owner next argues that "even when considering *Bradford* in combination with *Foss*, the location at which the biometric signature is stored *remains unclear*" such that "[i]t cannot be, then, that [Petitioner's] variety of references renders obvious the claimed 'storing.'" PO Resp. 21-22 (emphasis added) (citing Ex. 1001, 12:37-38, 16:10-11).

This is unpersuasive because Petitioner relies upon Bradford's "player ID database" as the memory location. Pet. 20. Interestingly, one could just as easily make this argument about claim 1, which also does not describe any specific memory location, requiring only that the memory location is "defin[ed], dependent upon the received card information." In any event, in response, Petitioner points out persuasively that the Petition "provided lengthy discussion regarding obviousness of modifying *Bradford* to include *Yamane's* flag to indicate the memory is unoccupied." Pet. Reply 26 (citing Ex. 1003, ¶¶ 103-112).

Yamane describes that "[u]ser information 60, fingerprint information 70, log information 80, authentication key information 90, and the like are stored in the protect area 1002-1 of the rewritable area 1002." Ex. 1006 ¶ 39. Yamane then explains that "[t]he user information 60 is constituted by pieces of information such as a user ID 60-1 and a fingerprint registration presence/absence flag 60-2 which are uniquely given to respective users." *Id.* ¶ 40. We credit the testimony of Dr. Sears, who testifies that Bradford teaches a "player ID entry in a player ID database" in which the claimed biometric signature is stored and that "Yamane teaches using a presence/absence flag 60-2 to determine if a fingerprint has been registered." Ex. 1003 ¶¶ 61, 63 (citing Ex. 1006

¶¶ 49, 52-54, 58-59, Fig. 2). Based on Bradford's "player ID database," the express disclosures of Yamane, and Dr. Sears' testimony, we are persuaded that Petitioner has shown a preponderance of evidence that Yamane in view of Bradford and Foss teaches limitation [1e].

(h) Motivation to combine Bradford and Yamane

Patent Owner also contends that Bradford and Yamane have "vast differences between [them]" and are improperly combined by Petitioner. PO Resp. 3-4, 23. Patent Owner submits that the "Petition ignores drastic differences between *Bradford* and *Yamane* that prove the only reason [Petitioner] has put these two references together is hindsight. *Id.* at 3-4. In particular, Patent Owner contends one of ordinary skill in the art "would not look to *Yamane* when seeking to modify the teaching of *Bradford*" because "*Yamane* teaches a 'rewritable area 1002' in which to store biometric information" which "is in direct contrast with the teachings of *Bradford*, which describe storing biometric information permanently." *Id.* at 23 (citing Ex. 1004, 23:36-40; Ex. 1006 ¶¶ 29, 31, 39, 41, Fig. 1; Ex. 2001 ¶ 60). Patent Owner also argues one of ordinary skill in the art would not seek to combine *Bradford* and *Yamane* because "*Bradford* is directed towards, in part, a casino machine, which is a stationary, single-purpose machine typically designed to prevent any external interference" while "*Yamane* is directed towards a portable recording medium, namely a Compact Disc-Rewritable, a portable storage medium designed to be transported and read by different general-purpose computer machines." *Id.* (citing Ex. 1004, 32:66-33:14; Ex. 1006 ¶¶ 1, 10-12).

Petitioner's rationale underlying the obviousness of the combination of Bradford (with Foss) and Yamane does not rest on the permanency (or impermanency) of data storage, or on the mobility (or lack thereof) of a casino machine or compact disc-rewritable storage medium. Rather, Petitioner contends an ordinarily skilled artisan would have been motivated to combine the teachings of Bradford and Yamane because (i) "[t]here would have been a reasonable expectation of success in the proposed modification" that employs "[s]etting a flag . . . [which] is a well-known method of indicating a binary state," (ii) "[i]t would have required only routine programming to determine if the memory location comprising the second authenticator data field is occupied by setting the flag," and because (iii) "checking the value of a flag to determine if a biometric signature had been previously stored as taught by *Yamane*" would "provid[e] a fast and efficient method of completing the enrollment process taught by *Bradford*." Pet. 38-40; Pet. Reply 26-27.

Moreover, Patent Owner's distinction between Yamane's "*rewritable* area 1002" and Bradford's "data . . . read at the biometric reader . . . [being] permanently recorded into the field in the player ID datable" (*see* PO Resp. 23) is not persuasive because Yamane's area 1002-1 (where fingerprint registration presence/absence flags are recorded within rewritable area 1002) is "a protect area [of a data storage region]" in which "written data is protected by encryption performed by a software." *See* Ex. 1006 ¶¶ 29, 31, 52, Fig. 1.

Patent Owner also contends "*Yamane* also teaches a CD-RW that is intended to transport multiple softwares to a wide variety of a terminals" which "cuts against

any purported rationale to combine this reference with *Bradford*, which per the Petition teaches runs at most two software programs: a 'special, privileged screen used for demonstration purposes' and a 'standard, ready mode,' on a single type of machine (a gaming machine)." PO Resp. 24; *see also* PO Sur-Reply 12. Patent Owner further submits one of ordinary skill in the art would not seek to combine Bradford and Yamane because Bradford's storage mediums are either shared by connected casino machines or located on single casino machines, none therefore corresponding to "the portable storage medium taught by *Yamane*." PO Resp. 24.

Again, these arguments are unpersuasive because Petitioner's rationale underlying the obviousness of the combination of Bradford and Yamane is not based on the transportation (or lack thereof) of software to terminals, or on databases or storage mediums being highly portable. Rather, Petitioner contends an ordinarily skilled artisan would have been motivated to combine the teachings of Bradford and Yamane because

> [s]etting a flag in computer code is a well-known method of indicating a binary state. *Dec.*, 112. *Bradford* already teaches the hardware and software for storing the second authenticator data in the second authenticator data field. *Bradford*, 3:28-36. It would have required only routine programming to determine if the memory location comprising the second authenticator data field is occupied by setting the flag.

Pet. 38. Dr. Sears testifies that setting flags as taught by Yamane, and the reason for doing so, wereF [sic]

well-known to those of ordinary skill in the art, and that "[c]ombining *Yamane's* teachings with *Bradford*(as modified by *Foss*), would have required only routine programming to determine if the memory location that comprises the second authenticator data field is occupied (or not) by setting a flag." Ex. 1003 ¶ 112. Dr. Sears explains persuasively that setting a flag "would have reduced the required computing resources compared to having to actually read data stored in a referenced memory location and would have provided a fast and efficient method of completing *Bradford's* enrollment process." *Id.* Dr. Easttom does not agree that a person of ordinary skill in the art would have looked to Yamane, yet does not contradict Dr. Sears' description that using flags and the implementation of flags to indicate occupancy of a memory location were well-known to those of ordinary skill in the art for determining whether a memory location was unoccupied. *See* Ex. 2001 ¶¶ 57-62.

In the Sur-Reply, Patent Owner argues "*Bradford teaches away* from Yamane because [Bradford] describes the CD embodiment as '[c]learly not the optimal choice.'" PO Sur-Reply 12 (emphasis added) (citing Paper 13, 25). However, Bradford recognizes that CDs are a viable storage medium, and states that "each game device could be essentially a standalone machine if configured as shown in FIG. 3, with database updates being carried out by the use of CD-ROMs." Ex. 1004, 9:11-14. A reference does not teach away if it merely expresses a general preference for an alternative invention from amongst options available to the ordinarily skilled artisan, and the reference does not discredit or discourage investigation into the invention claimed. *In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004); *see also In re Kahn*, 441 F.3d 977, 990 (Fed. Cir. 2006)

("A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant." (citations and internal quotation marks omitted)).

On the complete record now before us, we find that Petitioner and Dr. Sears have provided articulated reasoning with evidentiary underpinning as to why an ordinarily skilled artisan would have been motivated to combine the teachings of Bradford and Yamane. Pet. 37-40; Ex. 1003 ¶¶ 108-114.

(i) Conclusion as to claim 1

Based on the complete record before us and for the reasons expressed above, we are persuaded that Petitioner has shown a preponderance of evidence that claim 1 would have been obvious over Bradford, Foss, and Yamane.

5. Dependent Claim 2

Claim 2 depends from claim 1 and specifically recites "storing a biometric signature according to the enrolment method of claim 1." Ex. 1001, 12:41-42. Claim 2 specifically recites "[a] method of securing a process at a verification station." *Id.* at 12:39. Thus, different from the enrollment process of claim 1, claim 2 is directed to a verification process that follows the enrollment process.

Patent Owner does not provide substantive arguments with respect to claim 2, mainly arguing that claim 2 contains the same method steps of claim 1 and "[a]s

the prior art cited by [Petitioner] does not teach these limitations, the cited prior art does not render these dependent claims obvious as a result thereof." PO Resp. 25.

Petitioner argues that Bradford's system "is used for securing and obtaining verified access to a game device or authenticating a user." Pet. 41 (citing Ex. 1002 ¶¶ 115-116). And, as described above, Petitioner also argues that "*Bradford* teaches storing a biometric signature (*Bradford*, 15:60-63, FIG. 6), and the *Bradford-Foss-Yamane* combination teaches the enrollment method of Claim 1." *Id.*

Claim 2 recites in pertinent part the additional step of:

Claims	35 U.S.C. §	Reference(s) Basis	Claims Shown Unpatentable	Claims not shown Unpatentable
1, 2, 19, 20	103	Bradford, Foss, Yamane	1, 2, 19, 20	
Overall Outcome			1, 2, 19. 20	

> verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

Ex. 1001, 12:45-50. Petitioner argues that Bradford describes a verification process that verifies the card information of a player when "[t]he player then goes and uses a game device . . . [t]he player presents their first authenticator to the game device. Pet. 42 (quoting Ex. 1004, 13:23-33). Petitioner next contends that, as described for limitations [1c]-[1e], and as for a second authenticator, "the *Bradford-Foss-Yamane* system teaches storing a biometric signature at a location in local memory defined by card information." *Id.* at 43. Petitioner argues that

> *Bradford* teaches that, subsequent to verification of the presented card information required to perform a transaction (such as transfer funds, authorize a form, or play a game), "the second authenticator is checked, and **if the fingerprint data just read matches the fingerprint data in the second authenticator**, the action is **authorized** and carried out."

Id. at 43-44 (quoting Ex. 1004, 3:66-4:2). Dr. Sears testifies that in Bradford's gaming device 300 "if the first authenticator is verified (i.e., determined to be valid), then the steps for verifying the second authenticator data (for example, a fingerprint) occur." Ex. 1003 ¶ 118 (citing Ex. 1004, 3:50-62, 13:23-33, 17:14-27, 17:47-51, 18:27-39, 24:52-25:25).

Petitioner's arguments and Dr. Sears' testimony are consistent with Bradford's disclosure. For example, Bradford expressly describes a verification procedure

using a first and second authenticator, where the second authenticator is a biometric signature, i.e., a fingerprint:

> The player presents their first authenticator to the game device, which is used to get the associated second authenticator . . . [r]emembering that the second authenticator is always biometric data, all the player has to do is use the biometric reader. In the case of fingerprints, a quick touch of a fingerprint reader does the job. The second authenticator is checked, and if the fingerprint data just read matches the fingerprint data in the second authenticator, the action is authorized and carried out.

Ex. 1004, 3:50-4:2

For dependent claim 2 we have considered and on the complete record before us, accept as our own, Petitioner's arguments and evidence set forth at pages 41-42 of the Petition. Accordingly, we determine that Petitioner has shown by a preponderance of the evidence that claim 2 would have been obvious over Bradford, Foss, and Yamane.

6. Claims 19 and 20

Independent claim 19 and dependent claim 20 include essentially the same limitations as claims 1 and 2, except, that the preamble to claim 19 recites:

> A non-transitory computer readable medium having recorded thereon a computer program

> for directing a processor to execute a method of enrolling in a biometric card pointer system, the program comprising:

Ex. 1001, 15:25-16:2. And, for example, the limitation of "receiving card information," in independent claim 1, is recited in independent claim 19 as "code for receiving card information."

Petitioner argues that a person of ordinary skill in the art "would have understood *Bradford* teaches the game device 300 of FIG. 3 includes at least one processor, memory, and software for performing the disclosed functions for game device 300." Pet. 44 (citing Ex. 1003 ¶¶ 122-124). Dr. Sears testifies that "a POSITA would have understood that *Bradford* teaches that the game device 300 (depicted in Fig. 3) includes a central processor, associated memory, firmware, software, and the other 'normal and well known internals' as taught by *Bradford*." Ex. 1003 ¶ 123. Dr. Sears explains that a person of ordinary skill in the art "would have understood and found obvious that processors execute programming instructions (e.g., software) to perform various functions." *Id.* ¶ 124. In addition, Dr. Sears explains that a skilled artisan "would have understood that *Bradford's* software would have been stored in non-transitory memory for several reasons, including so that the game device would still be functional even if powered off and on again (i.e., power cycled)." *Id.* ¶ 126. Dr. Sears' testimony as to what a person of ordinary skill in the art would understand in regards to the known internals, programming instructions, and memory structure for a game device as shown in Bradford's Figure 3 is unrebutted on this record.

Petitioner's arguments and evidence are in all other respects the same as the arguments and evidence presented with respect to claims 1 and 2. We have considered, and on the complete record before us, accept as our own, Petitioner's arguments and evidence set forth at pages 44-48 of the Petition as to claims 19 and 20. Accordingly, we determine that Petitioner has shown by a preponderance of the evidence that claims 19 and 20 would have been obvious over Bradford, Foss, and Yamane for the same reasons as claims 1 and 2.

III. CONCLUSION[12]

For the reasons discussed above, we determine Petitioner has met its burden of establishing by a preponderance of the evidence that the challenged claims are unpatentable as summarized in the following table:

12. 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).

Appendix B

Claims	35 U.S.C. §	Reference(s) Basis	Claims Shown Unpatentable	Claims not shown Unpatentable
1, 2, 19, 20	103	Bradford, Foss, Yamane	1, 2, 19, 20	
Overall Outcome			1, 2, 19. 20	

IV. ORDER

For the reasons given, it is

ORDERED that, based on a preponderance of the evidence, claims 1, 2, 19, and 20 of the '039 patent have been shown to be unpatentable; and

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

For PETITIONER: Jennifer C. Bailey and Adam P. Seitz, ERISE IP, P.A.

For PATENT OWNER: Darlene F. Ghavimi-Alagha and Brian P. Bozzo, K&L Gates LLP

APPENDIX C — OPINION OF THE UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT, NOS. 24-1492, 24-1493, FILED NOVEMBER 10, 2025

UNITED STATES COURT OF APPEALS
FEDERAL CIRCUIT

2024-1492, 2024-1493

CPC PATENT TECHNOLOGIES PTY LTD.,

Appellant,

v.

ASSA ABLOY AB, ASSA ABLOY INC., HID GLOBAL CORP., ASSA ABLOY GLOBAL SOLUTIONS, INC., MASTER LOCK COMPANY, LLC,

Appellees.

Decided November 10, 2025

Appeals from the United States Patent and Trademark Office, Patent Trial and Appeal Board in Nos. IPR2022-01093, IPR2022-01094.

Before PROST, WALLACH, and CHEN, Circuit Judges.

Dissenting opinion filed by Circuit Judge WALLACH.

Appendix C

OPINION

CHEN, *Circuit Judge.*

CPC Patent Technologies Pty Ltd. (CPC) appeals from two final written decisions by the Patent Trial and Appeal Board (Board), both of which held the challenged claims in U.S. Patent No. 8,620,039 ('039 patent) unpatentable under 35 U.S.C. § 103. *Assa Abloy AB v. CPC Patent Techs. PTY, Ltd.*, No. IPR2022-01093, 2024 Pat. App. LEXIS 463, 2024 WL 378066, at *1 (P.T.A.B. Jan. 31, 2024) (*Final Decision I*); *Assa Abloy AB v. CPC Patent Techs. PTY, Ltd.*, No. IPR2022-01094, 2024 Pat. App. LEXIS 464, 2024 WL 378074, at *1 (P.T.A.B. Jan. 31, 2024) (*Final Decision II*). For the following reasons, we *reverse and remand* both decisions.

BACKGROUND

I

CPC owns the '039 patent, which relates to credit card security, and in particular, biometric verification of the user. '039 patent col. 1 ll. 13-15, col. 2 ll. 10-22, col. 2, ll. 51-61. Biometric verification ensures that the identity of the customer using a credit card matches the identity of the registered card owner, thereby assuring that only the authorized owner of the card can initiate transactions. This requires storing not only the user's credit card number, but also his or her biometric signature, such as a fingerprint. *Id.* col 2. ll. 23-26.

Appendix C

During a transaction, a biometric reader collects the biometric data of the customer. The biometric reader then sends that biometric information, along with the credit card information retrieved from the card reader, to a back-end system. The back-end system in turn checks for a match, and if a match exists, the transaction proceeds.

The '039 patent recognizes that biometric verification mechanisms existed within the prior art. *See, e.g.*, *id.* FIG. 2 (depicting prior art biometric verification mechanisms). The '039 patent, however, purports to introduce a particular way of storing the biometric data during enrollment of any given user: "[t]he biometric signature is stored at a memory address defined by the ('unique') card information on the user's card as read by the card reader of the verification station." *Id.* col. 2 ll. 64-67.

Claim 1, representative[1] for both appeals, recites:

> A method of enrolling in a biometric card pointer system, the method comprising the steps of:
>
> receiving card information;

1. Both parties focused on a particular limitation in this claim and treated it as representative for the appeal as to all challenged claims. We do so too. But as we note below, we summarily affirm the cancellation of claim 1 in a different IPR (which relied on different prior art). *See infra* Discussion Section I. Therefore, our discussion about errors the Board made in this appeal only extends to claims 3-18, which were not at issue in the other appeal.

> receiving the biometric signature;
>
> defining, dependent upon the received card information, a memory location in a local memory external to the card;
>
> determining if the defined memory location is unoccupied; and storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

Id. at claim 1.

CPC, on appeal, focuses on the third limitation, "defining, dependent upon the received card information, a memory location in a local memory external to the card." *Id.*; *see generally* Appellant's Br.

II

Only one prior art reference, Hsu,[2] is relevant to this appeal. Hsu, much like the '039 patent, describes a biometric verification mechanism. *See* Hsu ¶ 6. During enrollment, Hsu requires each user to present (1) a fingerprint and (2) his/her personal identification, such as an employee number, account number, card number, etc.— the system assigns an identifying number if the user does not yet have one. *Id.* ¶ 26. Hsu then teaches storing the personal identification number "in association with" the user's fingerprint image data. *See id.* ("The account

2. European Pat. Publ'n No. EP 0924655; J.A. 943-50.

number is stored in the database . . . in association with the user's fingerprint image data.").

III

ASSA Abloy AB (ASSA) petitioned for two *inter partes* reviews of the '039 patent. In its first petition, ASSA challenged claims 1-2, 13-14, and 19-20 as unpatentable over two prior art combinations, both of which relied on Hsu. *See Final Decision I*, 2024 Pat. App. LEXIS 463, 2024 WL 378066, at *3. And its second petition challenged claims 3-12 and 15-18 as un-patentable over several prior art combinations, all of which again relied on Hsu. *See Final Decision II*, 2024 Pat. App. LEXIS 464, 2024 WL 378074, at *4. The Board instituted review on both petitions.

Of relevance in the first proceeding, the Board issued a claim construction for "defining." *See Final Decision I*, 2024 Pat. App. LEXIS 463, 2024 WL 378066, at *6-7. It agreed with CPC that "defining" "mean[s] 'setting' or 'establishing,'" explaining that "[o]nce the card information and fingerprint are received during enrollment, the card information provides data that establishes *where*, i.e., at what memory location or address, the system will *store* the fingerprint data." 2024 Pat. App. LEXIS 463, [WL] at *7. The Board adopted an identical construction in the second proceeding. *See Final Decision II*, 2024 Pat. App. LEXIS 464, 2024 WL 378074, at *6-8.

After setting forth its construction, the Board turned to Hsu. It reiterated how Hsu's "fingerprint data [is] associated with corresponding user numbers." *Final*

Decision I, 2024 Pat. App. LEXIS 463, 2024 WL 378066, at *14 (quoting Hsu ¶ 26). That, in the Board's view, sufficed for having the card data "define" the memory location of biometric data because "the 'association' is the *where*," i.e., "where the fingerprint data is stored." 2024 Pat. App. LEXIS 463, [WL] at *15. The Board ultimately held that ASSA's first ground rendered the challenged claims unpatentable, and didn't reach ASSA's second ground. The second proceeding followed a similar analysis. *See Final Decision II*, 2024 Pat. App. LEXIS 464, 2024 WL 378074, at *13-16.

CPC appeals both decisions, contending the Board misapplied its construction of "defining" to Hsu.[3] We consolidated both appeals. We have jurisdiction under 28 U.S.C. § 1295(a)(4).

STANDARD OF REVIEW

Obviousness is a question of law based on underlying factual findings, and what a reference teaches is a question of fact. *In re Baxter Int'l, Inc.*, 678 F.3d 1357, 1361 (Fed. Cir. 2012). We review the Board's factual findings for substantial evidence, but the Board's legal conclusions de novo. *Id.*

3. Both CPC and ASSA treat the two appeals identically, focusing their arguments on the first proceeding. *See generally* Appellant's Br.; Appellees' Br. We therefore cite only to the first proceeding. *See Final Decision I*, 2024 Pat. App. LEXIS 463, 2024 WL 378066.

Appendix C

DISCUSSION

I

We begin with housekeeping. Today, in a separate appeal, we affirmed the unpatentability of claims 1-2 and 19-20 of the '039 patent in view of a different prior art combination. *See CPC Pat. Techs. Pty Ltd. v. Apple Inc.*, No. 24-1365, 2025 U.S. App. LEXIS 29450. Given that affirmance, our scope of review here extends only to claims 3-18 (though we subsequently refer to claim 1 for convenience, given that both parties treated it as representative and focus on the Board's analysis for claim 1). *See, e.g.*, *XY, LLC v. Trans Ova Genetics*, 890 F.3d 1282, 1294 (Fed. Cir. 2018) (declining to review patentability arguments because a separate appeal affirmed the unpatentability of the same claims).

II

CPC raises a simple and straightforward argument: "to associate with"—what the Board found Hsu teaches—does not mean "to set" or "to establish"—what the claims, as construed by the Board, require. And because of that mismatch, there is no substantial evidence for the Board's finding that Hsu uses card information to define the biometric signature's memory location. We agree.

The Board acknowledged that "associated with" differs in meaning from "set" or "establish." *Final Decision I*, 2024 Pat. App. LEXIS 463, 2024 WL 378066, at *14 (citing MERRIAM-WEBSTER ONLINE DICTIONARY). But

in its view, because Hsu teaches associating a personal identifier (e.g., employee account number) with biometric data, Hsu "concomitantly discloses 'defining,' 'setting,' or 'establishing' a memory location for the fingerprint data in relation to the employee account number." *Id.*

That inference has a problem: to associate two pieces of data with one another does not necessarily mean that one piece of data sets, or otherwise establishes, the location of the other piece of data. Of course, Hsu must necessarily set aside *a* memory location for storing a user's biometric data. *See* Hsu ¶ 26. But the Board did not meaningfully grapple with the '039 patent's additional constraint that the *card information* determines (i.e., establishes) *the* memory location of the biometric data. *See* '039 patent at claim 1. And without any explanation or evidence underpinning the Board's assumption—that associating the card information with the biometric data means the former controls the decision of where to store the latter—its decisions lack substantial evidence. *See Regents of the Univ. of Minnesota v. Gilead Scis., Inc.*, 61 F.4th 1350, 1355 (Fed. Cir. 2023) ("A finding is supported by substantial evidence if a reasonable mind might accept the evidence as adequate to support the finding.").

III

ASSA argues that, while the Board used the term "associate" in lieu of "set" or "establish" in its analysis of Hsu, it did not err. Appellees' Br. 22. Instead of equating the meaning of "associate" with "set," ASSA contends the Board found that the "*effect* of Hsu's association"

ultimately disclosed the claim limitation. *Id.* at 22-23. Yet as we just explained, the effect of Hsu's association is to do exactly that: "associate" two pieces of data together—nothing more. Contrary to the dissent's view, Hsu's disclosure offers nothing to suggest that its card information "tells you" where to store the fingerprint data. *See* Hsu ¶ 26; Dissent at 4.

Nor can the Board's cited testimony bridge this gap. Mr. Stuart Lipoff, ASSA's expert, opined that Hsu's fingerprint image "is stored at a memory location associated with the specific user/employee number received from a card." *Final Decision I*, 2024 Pat. App. LEXIS 463, 2024 WL 378066, at *14 (quoting J.A. 1025 ¶ 93). But at most, that statement merely confirms the associative link between the card information and the biometric data. Still missing is any non-conclusory testimony that Hsu's card information determines the memory location of the biometric data.

Mr. Lipoff further opined that, even if Hsu does not explain the mechanics of where to store the biometric information, a skilled artisan would resort to a few "simple known options" for storing that data. 2024 Pat. App. LEXIS 463, [WL] at *15 (citing J.A. 3160-61 ¶ 33). In one such option, "[u]pon a user enrolling by providing a user number, the system looks up the user number and determines the corresponding memory location for storing the user's fingerprint." J.A. 3160-61¶ 33. While this statement engages with the correct understanding of "set" or "establish," it suffers from a different issue: it simply parrots the elements of the claim, and deems it

a "known option," without any non-conclusory reasoning for why. *See TQ Delta, LLC v. CISCO Sys., Inc.*, 942 F.3d 1352, 1358 (Fed. Cir. 2019) ("Conclusory expert testimony does not qualify as substantial evidence.").

The Board also reasoned that, from a temporal standpoint, Hsu's system must first receive card information before then storing any biometric data, since the biometric data "cannot be stored until directed to, i.e. 'associated with,'" the card information. *Final Decision I*, 2024 Pat. App. LEXIS 463, 2024 WL 378066, at *15. Perhaps. But requiring card information to *exist* before storing any biometric data does not mean that the card information itself *sets* the *location* of the biometric data. The Board offered no explanation to bridge this lacuna.[4]

CONCLUSION

We have considered the remaining arguments, but find them unpersuasive. Both parties agree that, if we find the Board's analysis of Hsu lacks substantial evidence, we should remand for consideration of other unpatentability grounds not reached by the Board and not otherwise foreclosed by this decision. *See* Oral Arg at 13:53-14:18, 14:39-15:29. Accordingly, we *reverse* and *remand* both of the Board's decisions as to claims 3-18. Because of our affir-mance in appeal No. 24-1365, finding claims 1-2 and 19-20 unpatentable, we dismiss the appeal to those claims as moot. *See, e.g.*, *XY*, 890 F.3d at 1298.

4. The dissent faults us for "fail[ing] to examine 'the record as a whole.'" Dissent at 6 (citation omitted). We disagree. All of the Board's relied-upon evidence has the same infirmity we identified above.

Appendix C

DISMISSED-IN-PART, REVERSED-IN-PART, AND REMANDED

COSTS

Costs to Appellant.

Appendix C

WALLACH, *Circuit Judge*, dissenting.

I would affirm the Board. The Board's conclusion that Hsu discloses the Defining Limitation is supported by substantial evidence. The majority's holding to the contrary substitutes its own analysis of the facts for that of the Board. Accordingly, I respectfully dissent.[5]

I.

A claim is invalid for obviousness if, to a person having ordinary skill in the art, "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made." 35 U.S.C. § 103(a) (2006).[6] *Graham v. John Deere Co.*

---

5. While I dissent in this case, I join the majority today in a separate appeal affirming the unpatentability of claims 1-2 and 19-20 of the '039 patent in view of a different prior art combination and agree with the majority's articulation of the claims within the scope of this case's review as a result. Maj. Op. at 6. *See CPC Pat. Techs. Pty Ltd. v. Apple Inc.*, No. 24-1365, 2025 U.S. App. LEXIS 29450.

Except where indicated, I rely on the majority's factual background; legal standards; and shorthand nomenclature for the underlying proceeding, parties, and prior art. Unlike the majority, Maj. Op. at 3-4, 3 n.1, 6, 7, I refer to the relevant claim limitation in this appeal as "the Defining Limitation" consistent with the parties' briefing. Blue Br. 1-2 & n.2; Red Br. 7-8.

6. Section 103 has since been amended. *See* Leahy Smith America Invents Act, Pub. L. No. 112-29, § 3(c), 125 Stat. 284, 287-88 (2011) ("AIA"). However, because the application that led to the '039 patent was filed before March 16, 2013, the pre-AIA § 103(a)

sets forth underlying factual inquiries, two of which are relevant here: (1) "the scope and content of the prior art"; (2) "differences between the prior art and the claims at issue." 383 U.S. 1, 17, 86 S. Ct. 684, 15 L. Ed. 2d 545 (1966).

"The scope of our review in an appeal from a Board decision is limited." *In re Baxter Int'l, Inc.*, 678 F.3d 1357, 1361 (Fed. Cir. 2012). We review the Board's decisions in accordance with the Administrative Procedure Act, 5 U.S.C. § 706. The differences between the claimed invention and the prior art and the determination of what a reference teaches are underlying factual findings that we review for substantial evidence. *In re Baxter*, 678 F.3d at 1361 (citations omitted). The substantial evidence standard "involves examination of the record as a whole, taking into account evidence that both justifies and detracts from an agency's decision." *TQ Delta, LLC v. CISCO Sys., Inc.*, 942 F.3d 1352, 1358 (Fed. Cir. 2019) (citation omitted). "Substantial evidence is something less than the weight of the evidence but more than a mere scintilla of evidence." *In re Nuvasive, Inc.*, 842 F.3d 1376, 1379-80 (Fed. Cir. 2016) (citation omitted). "[T]he possibility of drawing two inconsistent conclusions from the evidence does not prevent an administrative agency's finding from being supported by substantial evidence." *In re Gartside*, 203 F.3d 1305, 1312 (Fed. Cir. 2000) (citation omitted).

---

applies. *See id.*, § 3(n)(1), 125 Stat. at 293. References to "35 U.S.C. § 103" are to pre-AIA 35 U.S.C. § 103.

II.

The Board sufficiently "show[ed] the evidence on which [its] findings are based, accompanied by the agency's reasoning in reaching its conclusions." *TQ Delta*, 942 F.3d at 1358 (citation omitted). The Board construed the Defining Limitation. Appx0013-16. It summarized CPC's and ASSA's arguments on the Defining Limitation. Appx0024-26; Appx0032. It provided its corresponding analysis. Appx0032-39. In the Board's analytical portion alone, it cited as evidence: Hsu ¶¶ 11, 20, 26, Fig. 4; Lipoff Declaration ¶ 93; Lipoff Deposition at 33:16-34:9, 34:19-35:9; Second Lipoff Declaration ¶¶ 33-34; Merriam-Webster Online Dictionary; and CPC's expert, Dr. Russ's, Declaration ¶¶ 49, 53-54.[7] Volume is not a measure of compliance with the Administrative Procedure Act, but in this case, an examination of the record as a whole evinces that the Board's factfinding is supported by "substantial evidence." *In re Gartside*, 203 F.3d at 1312.

The crux of Hsu's disclosure was put by ASSA's counsel during oral argument, consistently with the briefing and Board decision, as: "you cannot put the fingerprint information into Hsu unless you have the user information that tells you . . . where in the table in the database to put the fingerprint information." Oral Arg. at 16:48-17:32; *see also* Red Br. 13, 21-22, 28; Appx0033.

The first part, that putting fingerprint information into Hsu requires user information, is not disputed. In Hsu:

7. In the Board's claim construction portion, it cited an additional source: Microsoft Computer Dictionary, 5th Ed. (2002). Appx0015 n.8.

"[t]he enrollment procedure requires that each user enroll by presenting a finger to the fingerprint sensor . . . . [T]he user also presents an account number [or] one is assigned at this stage." Hsu ¶ 26 at column 7, lines 1-12; Appx3160-61 ¶¶ 33-34.

The second part was disclosed by Hsu according to the Board relying on substantial evidence that the user information "tells you" (as in "sets" or "establishes") where in the table in the database to put the fingerprint. To summarize: the Board relied on Hsu's Figure 4 and description in ¶ 26, for disclosing a fingerprint database in which the fingerprint is to be stored during enrollment and that includes reference prints and related account number for each user. Appx0033 (quoting Hsu ¶ 26 ("fingerprint data are associated with corresponding user numbers . . . ."). The Board further understood that the user number "defines, sets, or establishes *where* the fingerprint is stored" because: "the user's identity has to be independently verified" by the user number; Hsu stores the user's fingerprint data "associated with" a user's employee number; and "associated" means "related, connected, or combined together." Appx0033-34 (first citing Hsu ¶¶ 11, 26, Fig. 4 at block 66; then citing Merriam-Webster Online Dictionary). The Board was persuaded by Mr. Lipoff's testimony that "[t]he 'fingerprint image . . .' [is] not stored at *any* memory location in the database—rather, it is stored at a memory location associated with the specific user/employee number received from a card." Appx0034-35 (quoting Appx1024-25 ¶ 93). Mr. Lipoff was an undisputed POSITA and expert in the subject matter whose education, historical knowledge, and background in databases was provided to the Board.

Appx0984-88. In this summary, I have omitted the Board's engagement with CPC's counterarguments; recitation of Lipoff in deposition testifying "consistently with his declaration"; and credit of the Lipoff Second Declaration as "[c]ommensurate with [the Board's] understanding of Hsu's disclosure." Appx0035-38.

The majority substitutes its own analysis for that of the Board on "underlying factual findings" that this Court is supposed to review "for substantial evidence." *In re Baxter*, 678 F.3d at 1361. This occurs twice.

First, the majority substitutes its own judgment of the differences between the claimed invention and the prior art. *Id.* The majority agrees that Lipoff analyzing Hsu "confirms the associative link between the card information and the biometric data." Maj. Op. at 8 (quoting Appx1025 ¶ 93). However, the majority holds that Hsu's effect is to "'associate' two pieces of data together—*nothing more*." Maj. Op. at 7 (emphasis added). This improperly supplants the Board's factfinding. The majority's reversal of the Board only to circumscribe Hsu's disclosure as literally just the words of Hsu is contrary to the statutory standard "to a person having ordinary skill in the art," 35 U.S.C. § 103(a), and to our standard to review for what "*a* reasonable fact finder could have arrived at," *TQ Delta*, 942 F.3d at 1358 (emphasis added).

The majority's rigid interpretation of the prior art stands in contrast to the majority's paraphrasing of the Defining Limitation. The majority faults the Board for allegedly lacking support to conclude (in the majority's

words): "that associating the card information with the biometric data means the former controls the decision of where to store the latter." Maj. Op. at 7. "Control[ling]" a "decision" is not in the words of the Defining Limitation or the Board's analysis. Similarly, the majority says an "additional constraint" of the Defining Limitation is "that the *card information* determines (i.e., establishes) *the* memory location of the biometric data." Maj. Op. at 7 (citing "'039 patent at claim 1"). The majority also implies that the patent requires that "the card information itself *sets* the *location* of the biometric data." Maj. Op. at 8-9. The majority elides that under the Board's undisputed construction, the card information itself does not establish the location, but "the card information provides data that establishes *where*, i.e., at what memory location or address, the system will *store* the fingerprint data." Appx0015-16. The majority's analysis does not cite to the Board's claim construction at all. The majority's substitution of its own judgment is inconsistent with our standard of review.

Second, the majority fails to examine "the record as a whole." *TQ Delta*, 942 F.3d at 1358; *see also* 5 U.S.C. § 706. The Board found that Hsu's "associated" teaching discloses the Defining Limitation based on Merriam-Webster's Dictionary, the Board's reading of Hsu, the Lipoff Deposition, and "common database structures and functions"—as well as the Lipoff Declaration and Lipoff Second Declaration. Appx0032-39. From those Declarations, the majority selectively quotes excerpts of some, but not all, of the material on which the Board relied, and deems it conclusory. Maj. Op. at 8. In so doing, the majority fails to acknowledge Lipoff's reasoning

and evidentiary basis in the prior art. Without further explanation, the majority rejects the Board's findings for lack of substantial evidence. I disagree that Lipoff's testimony was conclusory. Sentences may, of course, be reduced to fractions that sound conclusory in isolation, but such reduction is contrary to our substantial evidence review. Indeed, even if Lipoff's testimony in both his reports was conclusory, the majority does not meaningfully examine the Board's other evidentiary bases for its finding. The majority merely asserts that "[a]ll of the Board's relied-upon evidence has the same infirmity [the majority] identified" as to Lipoff's Declarations. Maj. Op. at 9 n.4. Because this characterization of all the remaining evidence is at once sweeping and also vague, it is inconsistent with our standard of review. 5 U.S.C. § 706.

III.

For these reasons, I respectfully dissent.

APPENDIX D — JUDGMENT OF THE PATENT TRIAL AND APPEAL BOARD, NO. IPR2022-01093, DATED JANUARY 31, 2024

PATENT TRIAL AND APPEAL BOARD

IPR2022-01093
Patent No. 8,620,039 B2

ASSA ABLOY AB, ASSA ABLOY INC., ASSA ABLOY RESIDENTIAL GROUP, INC., AUGUST HOME, INC., HID GLOBAL CORPORATION, AND ASSA ABLOY GLOBAL SOLUTIONS, INC.,

Petitioner,

v.

CPC PATENT TECHNOLOGIES PTY, LTD,

Patent Owner.

Dated January 31, 2024

Before SCOTT A. DANIELS, AMBER L. HAGY and FREDERICK C. LANEY, Administrative Patent Judges.

JUDGMENT

Final Written Decision Determining All Challenged Claims Unpatentable

35 U.S.C. § 318(a)

DANIELS, Administrative Patent Judge.

Appendix D

I. INTRODUCTION

ASSA ABLOY AB, ASSA ABLOY Inc., ASSA ABLOY Residential Group, Inc., August Home, Inc., HID Global Corporation, and ASSA ABLOY Global Solutions, Inc., ("ASSA" or "Petitioner") filed a Petition requesting *inter partes* review ("IPR") of claims 1, 2, 13, 14, 19, and 20 of U.S. Patent No. 8,620,039 B2 (Ex. 1001, "the '039 patent"). Paper 2 ("Pet"). CPC Patent Technologies PTY, Ltd, ("CPC" or "Patent Owner") filed a Preliminary Response to the Petition. Paper 12 ("Prelim. Resp."). With our email authorization, Petitioner filed a Reply to Patent Owner's Preliminary Response. Paper 16 ("Prelim. Reply"). Also with our authorization, Patent Owner filed a Sur-Reply to Petitioner's Reply. Paper 19 ("Prelim. Sur-Reply").

Following our Institution Decision (Paper 20, "Inst. Dec."), in which we determined that Petitioner was *not* time-barred from filing its Petition, Patent Owner filed a Response. Paper 24 ("PO Resp."). *See* Inst. Dec. 9-34. Petitioner filed a Reply. Paper 26 ("Pet. Reply"). Patent Owner filed a Sur-Reply. Paper 30 ("PO Sur-Reply"). An oral hearing was held on November 9, 2023. A transcript of the hearing has been entered as Paper 37. ("Tr.").

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision is entered pursuant to 35 U.S.C. § 318(a). For the reasons explained below, we determine that Petitioner has met its burden of showing by a preponderance of the evidence that claims 1, 2, 13, 14, 19, and 20 are unpatentable.

Appendix D

A. Real Parties in Interest

Petitioner states that ASSA ABLOY AB, ASSA ABLOY Inc., ASSA ABLOY Residential Group, Inc., August Home, Inc., HID Global Corporation, and ASSA ABLOY Global Solutions, Inc., are the real parties in interest.[1] Pet. 1. Patent Owner states that CPC Patent Technologies PTY, LTD is the real party in interest. Paper 4, 2.

B. Related Matters

Petitioner indicates that it filed a declaratory judgment against Patent Owner with respect to the '039 patent in *ABLOY AB, et al. v. CPC Patent Technologies Pty Ltd., et al.*, No. 3-22-cv-00694, in the United States District Court for the District of Connecticut. Pet. 1-2. And Petitioner points out that the '039 Patent is asserted against Apple, Inc., in *CPC Patent Technologies Pty Ltd v. Apple Inc.*, No. 3:22-cv-02553, in the United States District Court for the Northern District of California, San Jose Division. *Id.* Petitioner points out that Apple challenged the '039 patent in IPR2022-00600. *Id.* at 2. On October 13, 2023, we entered a Final Written Decision (Paper 22) in IPR2022-00600 finding claims 1, 2, 19, and 20 of the '039 patent invalid for obviousness.

---

1. In its Declaratory Judgment Complaint against Patent Owner, Petitioner also refers to ASSA ABLOY Global Solutions, Inc., as "ASSA ABLOY Global Solutions, Inc. ('Hospitality')." Ex. 2007, 2.

Appendix D

In addition to the proceedings noted by Petitioner, Patent Owner indicates that "the following judicial and/or administrative matters [] may affect, or be affected by, a decision in this proceeding:" *CPC Patent Technologies PTY Ltd. v. HMD Global Oy*, Case No. 6:21-cv-00166 in the United States District Court for the Western District of Texas; IPR2022-00601; IPR2022-00602; IPR2022-01006; IPR2022-01045; IPR2022-01089; and IPR2022-01094. Paper 4, 2-3.

C. The '039 Patent (Ex. 1001)

The '039 patent, titled "Card Device Security Using Biometrics," relates to a biometric card pointer (BCP) system intended to more efficiently and securely permit a user to store biometric information during a user enrollment phase, and in future verification processes permits the user access their account using an identification (ID) card and biometric information such as a fingerprint. Ex. 1001, code (54), 2:51-3:11.

The '039 patent explains that in the enrollment phase "[t]he card user's biometric signature is automatically stored the first time the card user uses the verification station in question (this being referred to as the enrolment phase)." *Id.* at 2:62-64. The '039 patent explains further that "[t]he biometric signature is stored at a memory address defined by the ('unique') card information on the user's card as read by the card reader of the verification station." *Id.* at 2:64-67. Following the enrollment phase, the '039 patent describes that

> [a]ll future uses (referred to as uses in the verification phase) of the particular verification station by someone submitting the aforementioned card requires the card user to submit both the card to the card reader and a biometric signature to the biometric reader, which is verified against the signature stored at the memory address defined by the card information thereby determining if the person submitting the card is authorised to do so.

Id. at 3:4-11.[2] For both enrollment and future uses, the use of the ID card at a verification station "is identical from the card user's perspective, requiring merely input of the card to the card reader, and provision of the biometric signature ([e.g.] thumb print or retinal scan etc.) to the biometric reader." *Id.* at 3:12-15.

2. The words "enrolment," "authorise," and "authorisation" are the British spellings of "enrollment," "authorize," and "authorization." *See*, *e.g.*, https://www.merriam-webster.com/dictionary/authorisation, last visited Jan. 5, 2023. We will use the American English spelling of these words except where quoted from the '039 patent.

Appendix D

Figure 4 of the '039 patent is reproduced below.

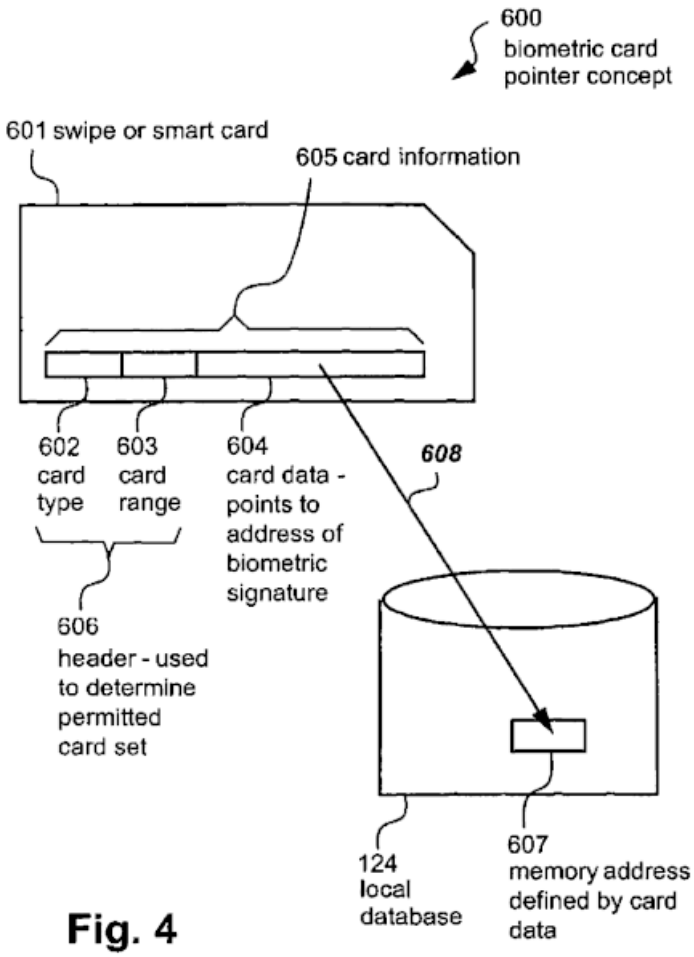


Fig. 4

Figure 4, of the '039 patent, above, illustrates swipe or smart card 601 including card information 605 encompassing fields for card type 602, card range 603, and card data 604. The '039 patent describes that "the card

data 604 acts as the memory reference which points, as depicted by an arrow 608, to a particular memory location at an address 607 in the local database 124." *Id.* at 7:31-35. Information 605 can be encoded on a magnetic strip on the card, for example. *Id.* at 7:28-29. The '039 patent explains that for a specific user "[i]n an initial enrolment phase, . . . [t]he card data 604 defines the location 607 in the memory 124 where their unique biometric signature is stored." *Id.* at 7:43-49. And, the '039 patent explains further that "in later verification phases, . . . [t]his signature is compared to the signature stored at the memory location 607 in the memory 124, the memory location 607 being defined by the card data 604 read from their card 601 by the card reader 112." *Id.* at 7:50-56.

Figures 6 and 7, reproduced below, depict the differences between verification process 205 shown in Figure 6, and enrollment process 207 shown in Figure 7.

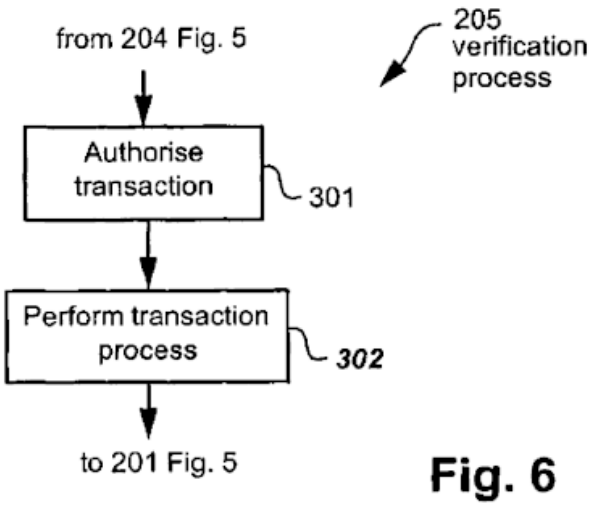


Fig. 6

Appendix D

Figure 6 illustrates verification process 205, which occurs after the enrollment process, illustrated below in Figure 7.

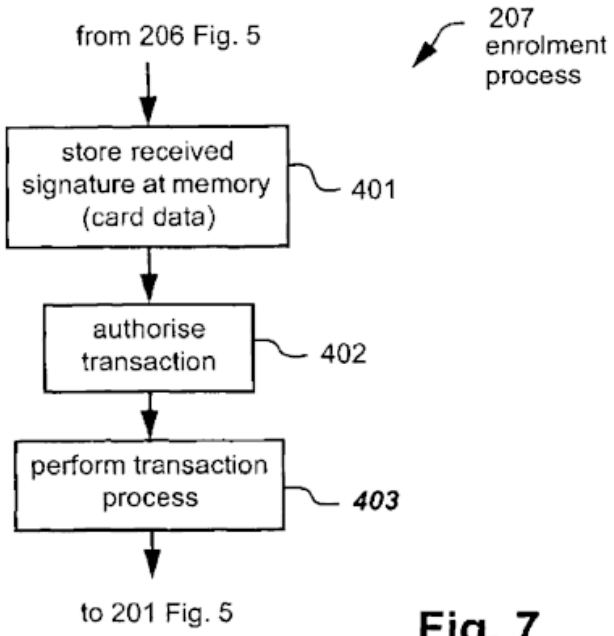


Fig. 7

Figure 7 of the '039 patent illustrates enrollment process 207 where the system at "step 401 stores the biometric signature received by the step 203 in the memory 124 at a memory address defined by the card data 604." *Id.* at 9:64-66 (referring to elements 203 and 124 described in Figure 5). Figure 6 illustrates that verification process 205

> is entered from the step 204 in FIG. 5, after which a step 301 authorises the transaction. This authorisation step 301 indicates that the biometric signal received by the biometric reader 102 in the step 203 matches the biometric signature previously stored in the local database 124 by a previous enrolment process 207.

Id. at 9:43-48. Then, "step 204 reads the contents stored at a single memory address defined by the card data 604 and checks these contents against the biometric signature received in the step 203." *Id.* at 8:34-37.

A difference between verification process 205 and enrollment process 207 is that the enrollment process includes step 401, which *stores* the biometric signature "at a memory address defined by the card data 604," whereas in verification process 205 "step 204 *reads* the contents stored at a single memory address defined by the card data 604" and compares the stored biometric signature with the input biometric signature. *Id.* at 9:65-66, 8:24-26.

D. Illustrative Claim

Claims 1 and 19 are independent. Each of claims 2 and 20 depends, respectively, from independent claims 1 and 19. Claim 1, a method claim, including disputed limitations highlighted in italics, illustrates the claimed subject matter and is reproduced below:

Appendix D

1. 1[P] A method of enrolling in a biometric card pointer system, the method comprising the steps of:

1[A] receiving card information;

1[B] receiving the biometric signature;

1[C] *defining, dependent upon the received card information, a memory location in a local memory external to the card;*

1[D] determining if the defined memory location is unoccupied; and

1[E] storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

Ex. 1001, 12:29-38.[3]Limitations 1[A]-1[E] are similarly recited in independent claim 13 as an apparatus claim for "[a] biometric card pointer enrolment system," and also in independent claim 19 in the context of "a processor to execute a method of enrolling in a biometric card pointer system." *Id.* at 13:67-14:9, 15:25-16:11.

3. We adopt and have applied Petitioner's alphanumeric designations for the elements of the challenged claims. *See, e.g.*, Pet. 17-37.

Appendix D

E. Prior Art and Asserted Grounds

Petitioner asserts that claims 1, 2, 13, 14, 19, and 20 would have been unpatentable based on the following grounds:

Ground	Claim(s) Challenged	35 U.S.C. § [4]	Reference(s) Basis
1	1, 2, 13, 14, 19, 20	103(a)	Hsu,[5] Sandford,[6]
2	1, 2, 13, 14, 19, 20	103(a)	Hsu, Sanford, Tsukamura[7]

Petitioner relies on the testimony of Stuart Lipoff. Ex 1006 ¶¶ 1-138. Patent Owner presents the testimony of Samuel Russ, Ph.D. Ex. 2039 ¶¶ 1-72.

---

4. The Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112-29, 125 Stat. 284, 296-07 (2011), took effect on September 16, 2011. The changes to 35 U.S.C. §§ 102 and 103 in the AIA do not apply to any patent application filed before March 16, 2013. Because the application for the patent at issue in this proceeding has an effective filing date before March 16, 2013, we refer to the pre-AIA version of the statute.

5. Ex. 1003, European Patent Appl'n No. EP 0924655 A2 (pub. June 23, 1999).

6. Ex. 1003, European Patent Appl'n No. EP 0924655 A2 (pub. June 23, 1999).

7. Ex. 1004, PCT Appl'n No. PCT/US03/07238 (pub. Sept. 18, 2003).

II. ANALYSIS

A. Legal Standards

A patent claim is unpatentable under 35 U.S.C. § 103 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. 35 U.S.C. § 103; *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). "[W]hen a patent claims a structure already known in the prior art that is altered by the mere substitution of one element for another known in the field, the combination must do more than yield a predictable result." *KSR*, 550 U.S. at 416 (citing *United States v. Adams*, 383 U.S. 39, 50-51 (1966)). The question of obviousness is resolved based on 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 ordinary skill in the art; and (4) when in evidence, objective evidence of non-obviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966).

B. Level of Ordinary Skill in the Art

Factors pertinent to a determination of the level of ordinary skill in the art include (1) the educational level of the inventor; (2) the type of problems encountered in the art: (3) prior art solutions to those problems; (4) rapidity with which innovations are made; (5) sophistication of the technology, and (6) educational level of workers active in

the field. *Envt'l. Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 696-697 (Fed. Cir. 1983) (citing *Orthopedic Equip. Co. v. All Orthopedic Appliances, Inc.*, 707 F.2d 1376, 1381-82 (Fed. Cir. 1983)). Not all such factors may be present in every case, and one or more of these or other actors may predominate in a particular case. *Id.* Moreover, these factors are not exhaustive but are merely a guide to determining the level of ordinary skill in the art. *Daiichi Sankyo Co. Ltd, Inc. v. Apotex, Inc.*, 501 F.3d 1254, 1256 (Fed. Cir. 2007).

In determining a level of ordinary skill, we also may look to the prior art, which may reflect an appropriate skill level. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). Additionally, the Supreme Court informs us that "[a] person of ordinary skill is also a person of ordinary creativity, not an automaton." *KSR*, 550 U.S. at 421.

Petitioner proposes that a person of ordinary skill in the art at the time of the '039 patent "would have had at least an undergraduate degree in electrical engineering, or equivalent education, and at least two years of work experience in the field of security and access-control." Pet. 10-11 (citing Ex. 1006 ¶ 26).

Patent Owner offers the level of ordinary skill we adopted in IPR2022-00600 which is that a person of ordinary skill in the art at the time of the '039 Patent

> would have had at least a bachelor's degree in computer engineering, computer science, electrical engineering, or a related field, with

> at least one year of experience in the field of human-machine interfaces and device access security. Additional education or experience might substitute for the above requirements.

See IPR2022-00600, Paper 22 at 12 (PTAB October 13, 2023) (Final Written Decision).

In this proceeding, Patent Owner's and Petitioner's levels of ordinary skill in the art, in particular education, are not substantively different. Petitioner's proposal requires at least two years of experience in the field of security and access control, compared to one year in Patent Owner's case. We maintain our determination of the level of ordinary skill in the art from IPR2022-00600 including at least one year of experience as Patent Owner urges. On this record, Patent Owner's proposed level of ordinary skill in the art is consistent with our review and understanding of the technology and descriptions in the '039 patent and the asserted prior art references. *Okajima*, 261 F.3d at 1355. Indeed, the difference between one and two years of experience in the field is fairly minimal considering that neither party asserts that it is necessary to have a significant amount of experience, e.g., 5-10 years in the field. For consistency we rely on the same level of ordinary skill in the art that we determined in IPR2022-00600.

C. Claim Construction

We interpret 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)." 37 C.F.R. § 42.100(b) (2020). Under this standard, we construe 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." *Id.* Furthermore, we expressly construe the claims only to the extent necessary. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) ("[W]e 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))).

1. "A method of enrolling"

Patent Owner argues that the independent claims are specifically directed to an enrollment process, e.g., "[a] method of enrolling," recited in the preamble of claim 1, and that the preamble should be considered limiting. PO Resp. 6. Patent Owner argues that "the 'method of enrolling' in the preamble of Claim 1 provides antecedent basis for 'the enrolment method' in the body of dependent Claim 2." *Id.* (citing Ex. 1001, 12:29-42). Petitioner disagrees, arguing that "a 'method of enrolling' is nothing more than a nonlimiting intended use." Pet. Reply 13. Petitioner also asserts that this term is "not critical to the issues in dispute" and "[e]ven if the phrase is limiting, Hsu, Sanford, and Tsukamura each disclose an enrollment process." *Id.* at 14 (citing Pet. 20, 36-37, 78).

Because Petitioner contends that Hsu, Sanford, and Tsukamura each disclose an enrollment process and

Patent Owner does not expressly dispute that they do, in this case we need not explicitly determine whether the term is limiting. We can agree that "[a] method of enrollment" provides antecedent basis for at least dependent claim 2 and that the preamble provides context to the recited method step limitations in the body of independent claim 1. *See* Ex. 1001 12: 41-42 (dependent claim 2 referring "to the enrollment method of claim 1"). Apart from considering the limitations of claim 1 within the context of an enrollment process, because the term does not create any particular dispute between the parties that we need to resolve, we need not determine whether it is limiting.

2. "dependent upon"

Petitioner indicates that the parties agreed in the district court litigation that "dependent upon," recited in claim 1 and 19, should be given its plain and ordinary meaning, "defined as 'contingent on or determined by.'" Pet. 16 (citing Ex. 1013, 2). Patent Owner agrees, adding that "a memory location in a local memory which merely corresponds to, *but is not contingent upon or determined by*, the received card information is not 'dependent upon' the received card information." PO Resp. 10 (citing Ex. 2039 ¶ 33). Patent Owner points out that Petitioner asserts the meaning of "dependent upon" is not material to patentability. *Id.* Patent Owner contends, however, that "because 'dependent upon' is integral to the 'defining, *dependent upon* the received card information, a memory location in a local memory external to the card', its

meaning must be considered when analyzing the entire claim term." *Id.*

We agree that for purposes of understanding claim 1, we should consider the plain and ordinary meaning of "dependent upon," so that limitation 1[c] is understood as follows:

> [1c] *defining, [contingent upon or determined by] the received card information, a memory location in a local memory external to the card;*

Accordingly, in this proceeding, we will consistently apply the plain and ordinary meaning of "dependent upon" which is "contingent upon or determined by."

3. "defining, dependent upon the received card information, a memory location in a local memory external to the card"

Patent Owner argues that "the proper construction of this entire clause is: 'the system sets or establishes a memory location in a local memory external to the card, said location being contingent upon or determined by the received card information.'" PO Resp. 11. Patent Owner asserts that a person of ordinary skill in the art "would interpret the word 'defining,' especially in the context of enrollment, to mean 'setting' or 'establishing.'" *Id.* at 12.

Petitioner proposes alternative constructions, first that "defining" means that "a memory location is somehow

determined from (or is dependent on) the card information." Pet. 11. Second, that "defining" means "a memory location is specified by the card information itself." Petitioner contends that the second construction is most consistent with the specification of the '039 patent specification. *Id.* at 12. According to Petitioner, and considering that the '039 describes "a biometric card pointer system," a person of ordinary skill in the art "would have understood that the user's card information itself specifies the physical memory address (such as by acting as a pointer) for the user's biometric signature." *Id.* at 13 (citing Ex. 1006 ¶ 47).

Consistent with our prior decision in IPR2022-00600, we determine, also in this proceeding, that Patent Owner's construction is sufficiently accurate. *See Apple, Inc. v. CPC Patent Technologies, Ltd.*, IPR2022-00600, Paper 22, 29-39 (Final Written Decision); *see also NTP Inc., v. Research in Motion, Ltd.*, 418 F.3d 1282, 1293 (Fed. Cir. 2005) (noting that, when construing claims in patents that derive from the same parent application and share common terms, "we must interpret the claims consistently across all asserted patents"). In IPR2033-00600, we explained that

> [c]onsidering the abstract and the specification of the '039 patent, what "defining, dependent upon . . . " means as a whole, in the context of claim 1 and "a method of enrolling," is that during an *enrollment* process, the claimed "biometric signature," e.g., a fingerprint, is not yet stored in the memory and no memory location or address has been "set" or

> "established" for the fingerprint. When the fingerprint, and then the card, is provided to the system during enrollment, the card information provides data that establishes *where, e.g.*, at what memory location or address, the system will *store* the fingerprint data. [8]

IPR2022-00600, Paper 22, 30. We also explained that "[i]mportantly . . . we do not understand that 'defining . . . a memory location,' or Patent Owner's alternative wording, 'establishing' or 'setting,' means '[*creating*] . . . a memory location in a local memory.'" *Id.* at 32. We explained further that "[w]hile we might agree that 'the memory location cannot [already be defined],' . . . we do not agree that it 'cannot already exist.'" *Id.* at 33.

During the oral hearing in this proceeding, Patent Owner's counsel argued that "Patent Owner in this case has not argued that defining means creating." Tr. 31:3-4. Patent Owner's counsel argued further, "[a]ll we're saying that Claim 1 requires is that when a user swipes their card, that is the information that is on the card, not – in that moment in time, not something else in the system, but the information on the card that directs the system where to store that particular user's fingerprint or other biometric data." *Id.* at 31:7-11.

---

8. We use the terms "memory location" and "memory address" interchangeably because, in terms of computer memory, an "address" is well-understood as "[a] number specifying a location in memory where data is stored." Microsoft Computer Dictionary, 5th Ed. (2002) Microsoft Press.

Considering Patent Owner's arguments and asserted claim construction with respect to the phrase "defining, dependent upon" and limitation 1[C] as a whole, we maintain the claim construction given in IPR2022-00600 for the reasons given in the Final Written Decision. IPR2022-00600, Paper 22, 30. We understand that during an enrollment process the claimed "biometric signature," e.g., a fingerprint, is not yet stored in the memory, and no memory location or address has been "defined," as in "set" or "established," in the memory for storing the fingerprint, until card information is received. Once the card information and fingerprint are received during enrollment, the card information provides data that establishes *where*, i.e., at what memory location or address, the system will *store* the fingerprint data.

4. "unoccupied"

In our Institution Decision, as argued by Petitioner and based on the express written description of the '039 patent, we determined that "unoccupied" means "a memory location that has not been used in the enrollment process for a user, or the information stored at the memory location has been deleted." Inst. Dec. 38-39; *see also* Ex. 1001, 9:29-33 ("The term 'occupied' in this context means that the memory location in question has been used in the enrolment process for a user, and that the information stored at the memory location in question has not been deleted by a BCP system administrator."). Patent Owner does not dispute this construction. PO Resp. 14.

Although patentability on the claims at issue in this case does not turn on the construction of this term, we nevertheless maintain our construction from our Institution Decision that "unoccupied" means "a memory location that has not been used in the enrollment process for a user, or the information stored at the memory location has been deleted." Inst. Dec. 38-39.

5. Other claim terms agreed upon and construed by the District Court

The parties indicate that the following terms have been construed by the District Court:

> "*biometric card pointer system*" – Nonlimiting preamble term with no patentable weight;
>
> "*biometric card pointer enrollment system*"- Nonlimiting preamble term with no patentable weight;
>
> "*biometric signature*" – Plain and ordinary meaning.

Pet. 16 (citing Ex. 1012, 1); PO Resp. 15 (citing Ex. 1012, 2).

Considering these constructions and that our analysis does not turn on any particular claim construction for these terms, and because these constructions are not in dispute, we need not determine any specific claim construction for these terms in this proceeding.

6. Means-plus-function terms

In our Institution Decision we accepted Petitioner's proposed constructions for the several "means for" and "code for" limitations recited in claims 13, 14, 19, and 20. *See* Inst. Dec. 43 (The Board explaining that "we find Petitioner's proposed constructions of these term under 35 U.S.C. § 112(6) consistent with the record in this case."). These constructions are also consistent with the District Court proceeding. Inst. Dec. 39-43; *see also* Ex. 1012, 1-4. For its part, Patent Owner states that it "takes no position on these proposed constructions as they are not material to the alleged grounds for unpatentability asserted in the Petition." PO Resp. 15.

Based on our review of the complete trial record and because patentability on the claims at issue in this case does not turn on construction of the relative structures and functions of these means-plus-function terms, and because they are not in dispute, we maintain the constructions from our Institution Decision including that "code for" is an equivalent recitation for "means for." Inst. Dec. 39-43.

D. Ground 1: Claims 1, 2, 13, 14, 19 and 20 – Obviousness over Hsu (Ex. 1003) and Sanford (Ex. 1004)

For the reasons below, and on the complete record before us, Petitioner has shown by a preponderance of the evidence that claims 1, 2, 13, 14, 19, and 20 would have been obvious over Hsu and Sanford.

Appendix D

1. Hsu (Ex. 1003)

Titled "Controlled Access to Doors and Machines Using Fingerprint Matching," Hsu describes "[a] system and related method for controlling access to building doors or to machines, such as automatic teller machines (ATMs)." Ex. 1003, Abstract, codes (54), (57). Hsu describes using "an account number or employee number, to access a fingerprint database (44) and retrieve reference fingerprint data previously stored there during an enrollment procedure." *Id.*, Abstract. Figure 3 from Hsu, as annotated by Petitioner (Pet. 8), is reproduced below.

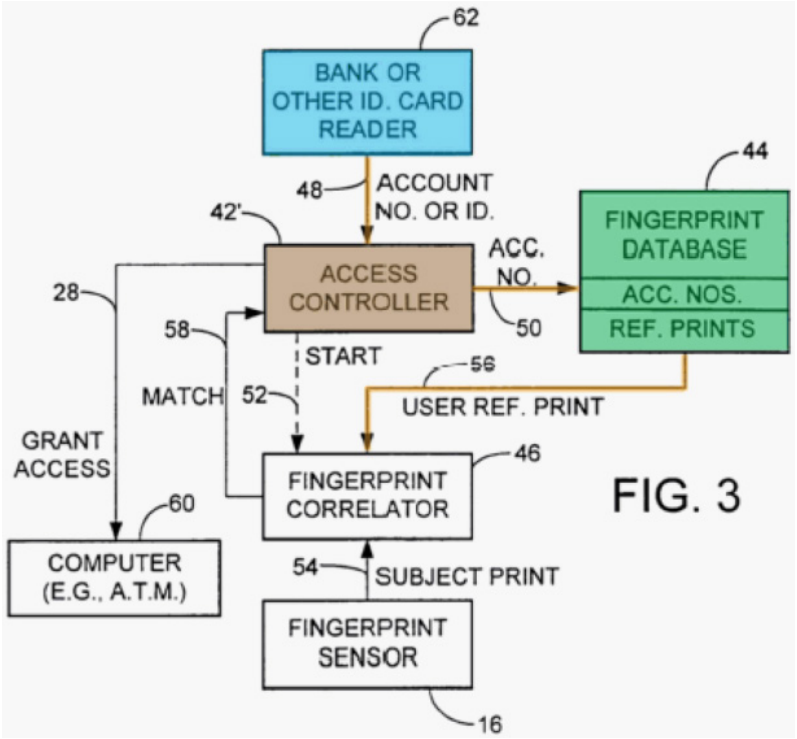


FIG. 3

Appendix D

Hsu's Figure 3 is a block diagram illustrating card reader 62 (blue) reading "an account number or other type of identification unique to the user, and passes this data to the access controller 42' [(brown)] over line 48." Ex. 1003, 6:10-12. Based on the user's unique identification, access controller 42' communicates with finger print database 44 (green) "to access the fingerprint database 44 and obtain a user reference fingerprint on line 56 from the database." *Id.* at 6:14-16. Hsu explains that

> [t]he controller 42' also sends a "start" signal on line 58 to the fingerprint correlator 46, which compares the reference fingerprint with a subject fingerprint image supplied from the sensor 16 over line 54. If the correlator 46 finds a match, the correlator sends a signal over line 58 to the access controller 42', which transmits an appropriate signal to the computer 60 on line 28, indicating that access has been granted.

Id. at 6:16-24.

Appendix D

Hsu also describes an enrollment process shown in Figure 4 and reproduced below.

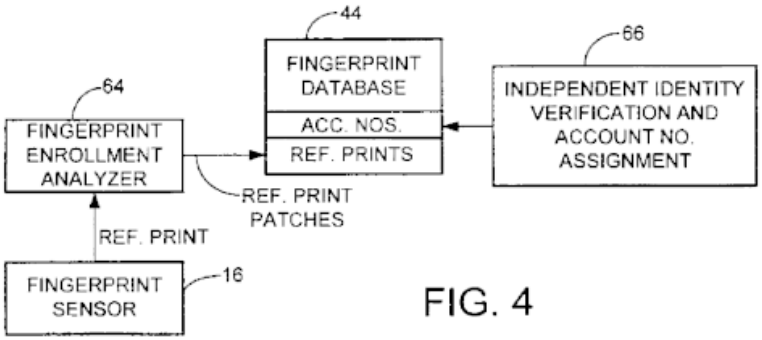


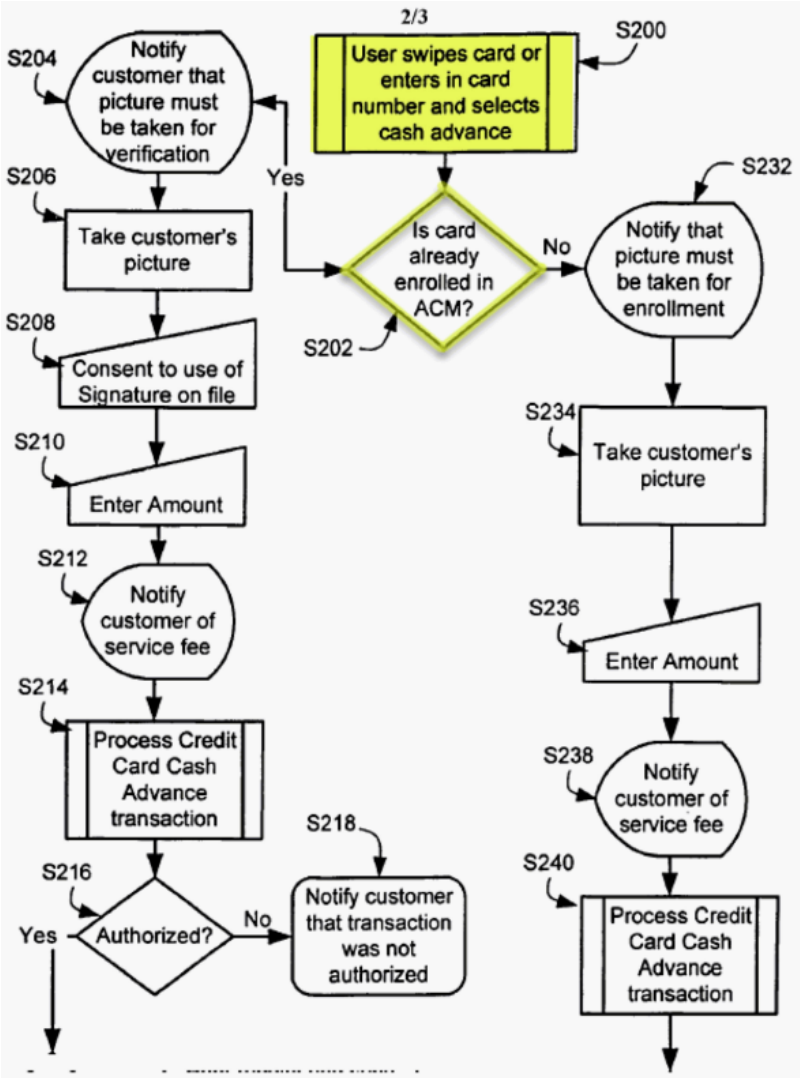
FIG. 4

Hsu's Figure 4 illustrates a block diagram showing that a user's fingerprint is obtained by fingerprint sensor 16 and passes through fingerprint enrollment analyzer 64 before being stored in fingerprint database 44. *Id.* at 7:51-8:23. Hsu explains that, along with providing a fingerprint during enrollment, "[a]t the same time, the user's identity has to be independently verified, by some means other than fingerprint matching, as indicated in block 66, and the user also presents an account number, employee number or similar identity number." *Id.*

2. Sanford (Ex. 1004)

Sanford is titled "Credit Card Transaction without using a Pin with Automated Cashier Machine" and describes "[a]n automated cashier machine (ACM) is provided that offers a secure and convenient way for users to access cash from their card without using a PIN." Ex. 1004, Abstract, codes (54), (57). Sanford describes that "[b]y verifying a user's image using facial biometrics, transactions may be conducted without using a pin." *Id.* ¶ 7. Sanford explains further that "[o]ther methods of verification known in the art may

also be used, such as iris, voice signature, and fingerprint technology." *Id.* ¶ 20. The relevant part of Sanford's Figure 2, as annotated by the Board, is reproduced below.



Sanford's figure 2 is a block diagram illustrating a method for performing a PIN-less credit card transaction using an ACM (automated cashier machine). *Id.* ¶ 24. After swiping a user's card at step 200, the system determines whether the user's card information is already stored, i.e., enrolled, and "the ACM 12 determines if the credit card account number of the user is enrolled to use the PIN-less credit card system." *Id.* In determining if the user is enrolled, "ACM 12 may communicate with ACM computer system 18 to look up the user's credit card number." *Id.* ¶ 25. At step 202, highlighted yellow above, ACM 12 determines an enrollment course of action; if the card is not enrolled, moving to step 232, or, if the card is already enrolled, conducting a verification course of action via step 204. *Id.*

3. Independent Claim 1

We consider initially the elements of claim 1.

a) Petitioner's Arguments

(1) Preamble – 1[P] "A method of enrolling in a biometric card pointer system"

To the extent the preamble could be considered limiting, Petitioner argues that Hsu teaches "a biometric card pointer system" where "access control unit 14 includes an access controller (42 or 42') that "uses the account number [or user number] . . . to access the fingerprint database 44 [green] and obtain a user

reference fingerprint." Pet. 19 (citing Ex. 1006 ¶¶ 20, 24). With respect to "enrolling," Petitioner contends that Hsu's Figure 4 "discloses 'a method of enrolling' in its biometric card pointer system. Specifically, 'FIG. 4 is a block diagram showing a fingerprint enrollment process as used in FIG[]. 3.'" *Id.* at 20 (quoting Ex. 1003 ¶ 14). Hsu's Figure 4, as annotated by Petitioner (*id.* at 20), is reproduced below.

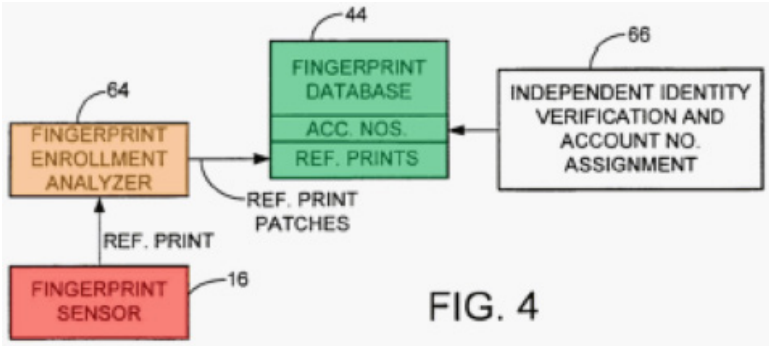


Figure 4 is a block diagram illustrating "a fingerprint enrollment process as used in either of the systems of FIGS. 2 and 3." Ex. 1003 ¶ 14. Mr. Lipoff testifies that considering Hsu's Figure 4 "[a]s shown, '[t]he account number is stored in the database 44 [green] in association with the user's fingerprint image data.' Once a user is enrolled, he or she may use his or her card to access his or her reference fingerprint for verification purposes." Ex. 1006 ¶ 73 (quoting Ex. 1003 ¶ 24).

(2) Limitation 1[A] – "receiving card information"

Petitioner points to Hsu's Figure 3 and argues that a person of ordinary skill in the art "would have understood that Hsu's received 'account number' is the claimed 'card information.'" Pet. 23 (citing Ex. 1006 ¶ 78). Petitioner argues that "Hsu's enrollment process also includes 'receiving card information.' Hsu includes various disclosures of 'reading data from a card reader,' which confirm that the card reader (or its equivalent, a polling transceiver) in the access controller is receiving card information." *Id.* (citing Ex. 1003 ¶ 9). Mr. Lipoff testifies that based on Hsu's "various disclosures of 'reading data from a card reader,'" . . . a person of ordinary skill in the art "would have understood that regardless of the type of card used, Hsu's enrollment process includes receiving card information (*e.g.*, account number or employee number)." Ex. 1006 ¶¶ 79-80 (citing Ex 1009 ¶¶ 9, 26).

(3) Limitation 1[B] – "receiving the biometric signature"

Petitioner argues that as shown in Hsu's Figure 1, "the access control unit includes a 'fingerprint sensor 16' (red) for 'scan[ning] the user's fingerprint.'" Pet. 26 (citing Ex. 1003 ¶¶ 20-21, 24). Hsu's Figure 1 as annotated by Petitioner (*id.* at 27) is reproduced below.

Appendix D

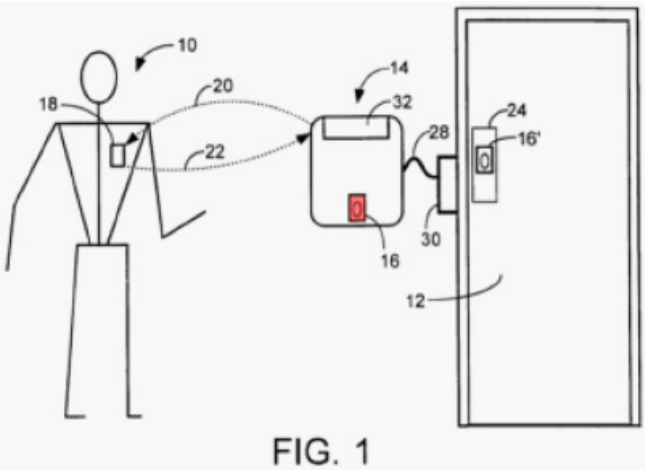


FIG. 1

Hsu's Figure 1 depicts access controller 14 having fingerprint sensor 16 (highlighted red) for receiving a fingerprint from user 10. *See* Ex. 1003 ¶ 17 ("When the user 10 reaches the door, he or she places a finger on the fingerprint sensor 16.").

(4) Limitation 1[C] – "defining, dependent upon the received card information, a memory location in a local memory external to the card"

Petitioner argues specifically that Hsu's Figure 1 "discloses 'a local memory external to the card.' As shown in Figure 1, the 'access control unit 14' (yellow) is external to the 'identification badge 18 [card]' (pink)." Pet. 28. Hsu's Figure 1 as annotated by Petitioner (*id.* at 28) is reproduced below.

Appendix D

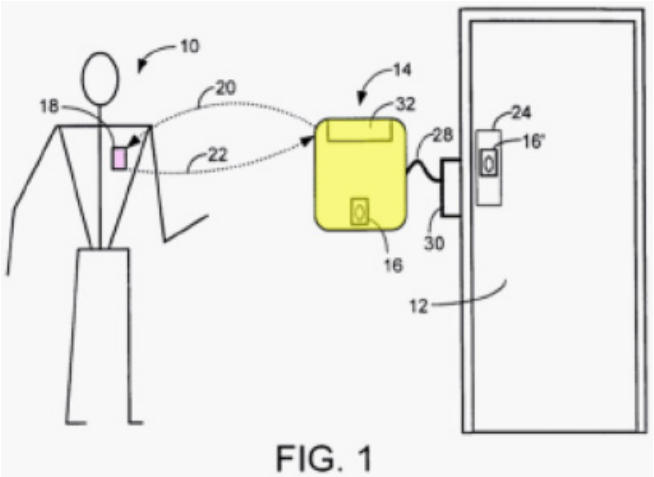
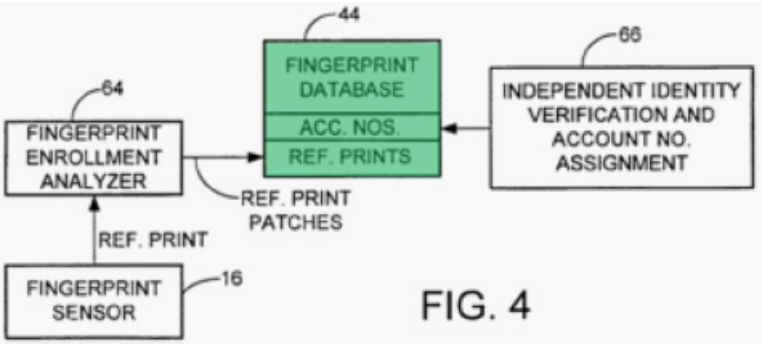


FIG. 1

Hsu's Figure 1 depicts access controller 14 (highlighted yellow) which is separate, i.e., external to the card or ID badge 18 (highlighted pink) worn by user 10. *See* Ex. 1003 ¶ 20 (access controller 14 includes "fingerprint database 44, and a fingerprint correlator 46"). Mr. Lipoff testifies that a person of ordinary skill in the art "would also have understood that a database is stored in a memory. Thus, in my opinion, the 'fingerprint database (44)' in Figure 2 of Hsu discloses 'a local memory external to the card.'" Ex. 1006 ¶ 90.

Petitioner argues with respect to the phrase "defining dependent upon the received card information, a memory location . . . " that Hsu specifically discloses "'[t]he database is basically a table that associates each user number with a stored fingerprint image, or with selected distinctive attributes or features of the user's fingerprint

image.'" Pet. 31 (quoting Ex. 1003 ¶ 20). Hsu's Figure 4, as annotated by Petitioner (*id.* at 20), is reproduced below.

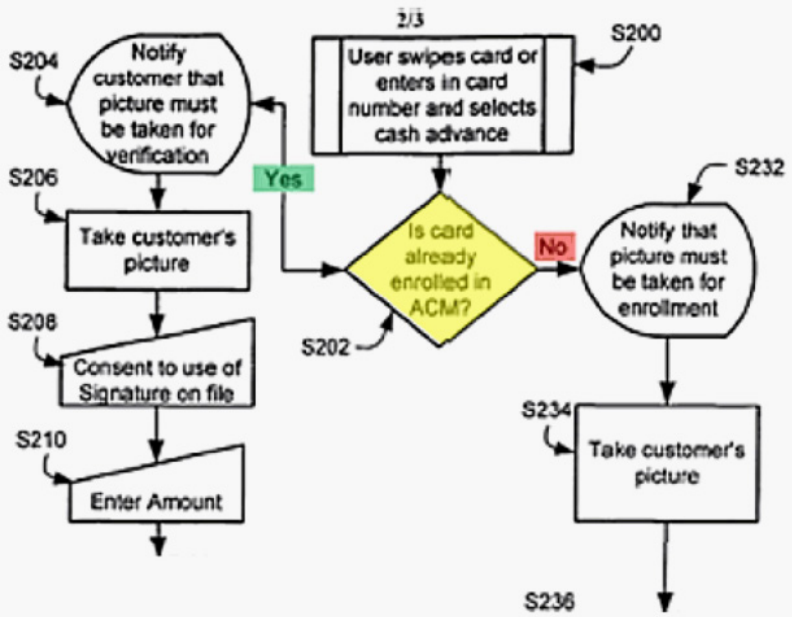


Hsu's Figure 4 is a block diagram of an enrollment process illustrating fingerprint database 44 (highlighted green) including reference prints and related account number for each user or employee. Ex. 1003 ¶ 26. Mr. Lipoff testifies that a person of ordinary skill in the art "would have understood that, given a user [account] number, Hsu's system easily determines from fingerprint database 44 the specific memory location for storing the associated fingerprint." Ex. 1006 ¶ 93.

(5) Limitation 1[D] – "determining if the defined memory location is unoccupied"

Petitioner argues that Hsu in combination with Sanford renders claim limitation 1[D] obvious. Pet. 32. Petitioner asserts that Hsu discloses the "defined memory location," but does not explicitly discuss determining whether a memory location is occupied or not. *Id.* Petitioner turns

to Sanford, arguing that "Sanford discloses in step S202 (yellow) 'determin[ing] if the credit card account number of the user is enrolled to use the PIN-less credit card system.'" *Id.* at 33. Sanford's Figure 2, in relevant part, and as annotated by Petitioner (*id.* at 34), is reproduced below.



Sanford's Figure 2, reproduced in part above, as annotated by Petitioner, is a block diagram illustrating a decision making process at step 202 (highlighted yellow) based on whether a user's card is enrolled (yes, highlighted in green) or not (no, highlighted in red) in the ACM. *See* Ex. 1004, Fig. 2.

With respect to a motivation to combine Hsu and Sanford, which we address in further detail below, Mr. Lipoff testifies that a person of ordinary skill in the art, understanding that Hsu has a database that may include a fingerprint associated with a user or employee number, "would not want to enroll a user who already enrolled." Ex. 1006 ¶ 112 (citing Ex. 1004 ¶ 38). Mr. Lipoff explains that "[r]e-enrollment is usually unnecessary because fingerprints do not change. Re-enrollment also consumes unnecessary system resources, takes time, and is generally undesirable. Therefore, before enrolling a user, it is my opinion that a POSITA would have been motivated to first check whether the user is already enrolled, as disclosed by Sanford." *Id.* Mr. Lipoff testifies further that "checking whether a user is enrolled also makes the system more user-friendly. If the user is enrolled, the user can seamlessly proceed with biometric verification." *Id.* ¶ 114.

(6) Limitation 1[E] – "storing, if the memory location is unoccupied, the biometric signature at the defined memory location"

Following from limitations 1[C]-[D], Petitioner argues that Hsu in combination with Sanford renders claim limitation 1[E] obvious, because "Sanford discloses that if a user is not enrolled (*i.e.*, if Hsu's memory location is unoccupied), the user is directed to complete enrollment, which involves storing the user's biometric information (*e.g.*, picture or fingerprint) in the database." Pet. 36 (citing Ex. 1004 ¶ 37). Mr. Lipoff testifies that because both Hsu

and Sanford disclose an enrollment process for a user, where Sanford teaches checking if a storage location is unoccupied, a person of ordinary skill in the art, would have known to, "*e.g.*, check[] Hsu's database to see if a user is not yet enrolled per Sanford, and if so, storing], the biometric signature [*e.g.*, user's fingerprint] at the defined memory location [*e.g.*, at the memory address in Hsu's database assigned to the user]." Ex. 1006 ¶ 107.

(7) Analogous Art and Motivation to Combine Hsu and Sanford

Petitioner's assertion that Hsu and Sanford are analogous art to the '039 Patent, and Petitioner's evidence and arguments as to motivation to combine, are undisputed by Patent Owner. *See* generally Prelim. Resp. For completeness, we address Petitioner's foundational arguments and evidence as to analogous art and motivation to combine to ensure that Petitioner has met its burden under 35 U.S.C. §§ 312 (a)(3), 316(e).

(a) Analogous Art

Petitioner argues that Hsu and Sanford are analogous prior art with respect to the '039 patent. Pet. 37. Petitioner contends that "[b]oth references (and the '039 Patent) are directed to ways of performing efficient biometric authentication, including using fingerprints." *Id.* Petitioner argues that "[b]oth references (and the '039 Patent) teach authenticating a user by comparing a fingerprint captured by a sensor to a stored fingerprint." *Id.* (citing Ex. 1003, Abstract; Ex. 1004, Abstract).

As to analogous art, we consider two criteria when evaluating whether prior art is analogous: (1) whether the art is from the same field of endeavor, regardless of the problem addressed, and (2) if the reference is not within the field of the inventor's endeavor, whether the reference still is reasonably pertinent to the particular problem with which the inventor is involved. *In re Clay*, 966 F.2d 656, 658-59 (Fed. Cir. 1992).

The '039 patent is directed broadly to "security issues associated with use of card devices such as credit cards, smart cards, and wireless card-equivalents such as wireless transmitting fobs." Ex. 1001, 1:14-16. More specifically, the '039 patent explains that its disclosure addresses "problems relating to secure access and/or secure processes, by automatically storing a card user's biometric signature in a local memory in a verification station comprising a card reader, [and] a biometric signature reader." *Id.* at 2:53-57. Based on this, a reasonable field of endeavor involves enrollment and user verification systems including card devices and biometric signatures.

As Petitioner points out, both Hsu and Sanford expressly disclose enrollment and biometric user verification systems that compare a user fingerprint to a stored fingerprint for identity verification purposes. *See*, *e.g.*, Ex. 1003 ¶¶ 4, 13, 20, 24, Fig. 3, *see also* Ex. 1004 ¶¶ 4, 8-9, 16, 36. For example, Hsu explains that "FIG. 2 shows the principal components of the access control unit 14 in block diagram form, including an identification polling transceiver 40, a door controller 42, a fingerprint database

44, and a fingerprint correlator 46." *Id.* at ¶ 20. Similarly, Sanford describes that in "a secure and convenient way for users to access cash from their card without using a PIN . . . [a]n identifying image of a user is taken and an amount for withdraw is received. If the amount for withdrawal is approved, the ACM verifies the identifying image of the user to an image of the user in a profile." Ex. 1004 ¶ 6. Also, Sanford states that "[o]ther methods of verification known in the art may also be used, such as iris, voice signature, and fingerprint technology." *Id.* ¶ 20.

On the complete record now before us, we are persuaded that Hsu and Sanford are analogous art to the '039 patent as they are directed to the same field of endeavor, which is enrollment and user verification systems including card devices and biometric signatures.

(b) Motivation to Combine

With respect to a motivation to combine, Petitioner argues that although Hsu does not expressly disclose checking if the memory location in Hsu's database assigned to the user is unoccupied "this would be obvious to a POSITA." Pet. 32. To this end, Petitioner argues that Sanford describes an algorithm including a "check of whether a user is enrolled into Hsu's system." *Id.* at 37 (citing Ex. 1006 ¶ 108)." Petitioner points out that Hsu describes an embodiment "where the user already has an account/user/ employee number but has not yet enrolled their fingerprint." *Id.* at 26 (citing Ex. 1006 ¶ 110). Petitioner argues that "[i]n this context, a POSITA would have been motivated to implement Sanford's check

to determine whether a user (*e.g.*, with a user/account number) is enrolled in Hsu's system." *Id.* (citing Ex. 1006 ¶ 111).

In support, Petitioner's declarant, Mr. Lipoff, testifies that a person of ordinary skill in the art would have implemented Sanford's check to determine whether a user is enrolled in Hsu's system, for several reasons. Ex. 1006 ¶¶ 111-114. First, Mr. Lipoff explains, "in most instances, a POSITA would not want to enroll a user who already enrolled" because "[r]e-enrollment also consumes unnecessary system resources, takes time, and is generally undesirable." *Id.* ¶ 112. Second, Mr. Lipoff explains that "checking whether a user is enrolled helps prevent fraud whereby an unauthorized user is able to overwrite the fingerprint of an authorized user by using the authorized user's user number or account number." *Id.* ¶ 113. Also, Mr. Lipoff testifies that "checking whether a user is enrolled also makes the system more user-friendly. If the user is enrolled, the user can seamlessly proceed with biometric verification." *Id.* ¶ 114.

On the complete record now before us, we find persuasive Petitioner's explanations for a motivation to combine Hsu and Sanford. Sanford, as Mr. Lipoff testifies persuasively, describes *how* a person of ordinary skill in the art would construct a system to check to see if a user is enrolled in a biometric identity verification system before determining a further course of action. *Id.* ¶¶ 98-100. In addition, Mr. Lipoff provides several reasons *why* a person of ordinary skill in the art would have looked to Sanford for "the simple and straightforward way to determine

whether such user has been enrolled [and] to check if the user's data is already stored in Hsu's database." *Id.* ¶ 115; *see also KSR*, 550 U.S. at 420 (explaining that "any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed").

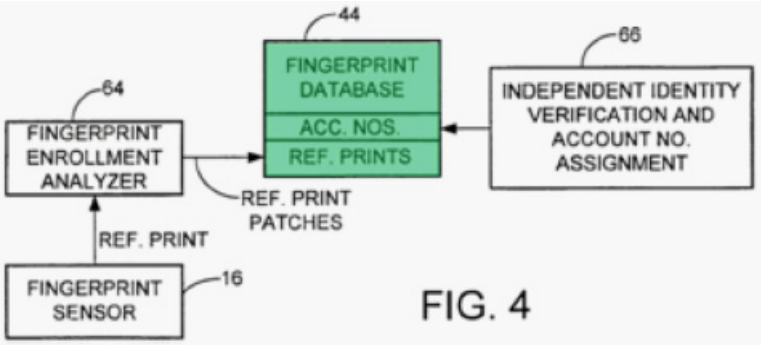
b) Patent Owner's Arguments

Patent Owner focuses its arguments on limitation 1[C], arguing that "Hsu is devoid of any teaching or suggestion that the user's card information sets or establishes (*i.e.*, defines) the memory location for the user's fingerprint data during enrollment." PO Resp. 16 (citing Ex. 2039 ¶ 46). According to Patent Owner, Hsu does not "set" or "establish" a memory location for the fingerprint data because Hsu mainly describes that "[t]he account number is stored in the database 44 in association with the user's fingerprint image data." *Id.* at 17 (quoting Ex. 1003, 7:1-12). Patent Owner's position is that Hsu doesn't define any memory location in particular, but "that the user's fingerprint data and account number are presented *at the same time* and are then stored in the database *in association with* each other." *Id.* at 18 (citing Ex. 2039 ¶ 49). In other words, Patent Owner's argument is that, unlike the claimed method, Hsu's card information does not provide data that sets or establishes *where*, i.e., at what memory location or address, the system will *store* the fingerprint data.

Appendix D

c) Analysis

Hsu expressly describes an enrollment process for a user including fingerprint database 44 and describes that "the fingerprint database 44 contains reference fingerprint image data for each user, employee, or customer using the system, and that the reference fingerprint data are associated with corresponding user numbers, or employee or customer account numbers." Ex. 1003 ¶ 26. Hsu's Figure 4, illustrating the enrollment process, as annotated by Petitioner (Pet. 20), is reproduced below.



Hsu's Figure 4 is a block diagram showing an enrollment process illustrating fingerprint database 44 (highlighted green) including reference prints and related account number for each user or employee. Ex. 1003 ¶ 26.

Based on the description and Figure 4, Hsu tells us a location, that is *where*, i.e., in fingerprint database 44, the fingerprint is to be stored during enrollment. Hsu explains that in fingerprint database 44, "fingerprint data are associated with corresponding user numbers, or

employee or customer account numbers." *Id.* Accordingly, we understand from this description that the user's fingerprint is stored in relation to, i.e., "associated with," the user's employee account number, for example. Still, a key question is *how* is the fingerprint data stored during enrollment, because, consistent with our claim construction, the card information must "set" or "establish" where the fingerprint data is to be stored. This question is also answered by Hsu. Hsu explains that when a user presents a fingerprint during enrollment, "[a]t the same time, the user's identity has to be independently verified, by some means other than fingerprint matching, as indicated in block 66, and the user also presents an account number, employee number or similar identity number." *Id.* In this way, Hsu describes presenting identification data apart from biometric data, and includes presenting, for example, an employee identification card or badge, including the user's employee number. *See* Ex. 1003 ¶ 11 (Hsu describing that "the identification medium carried by each user includes a machine-readable card, and the step of reading data from an identification medium includes reading data from a card reader in which the machine-readable card is placed by the user"). Understanding that during enrollment Hsu stores the user's fingerprint data "associated with" a user's employee number on the card, we further understand that the identification information, e.g., employee number, on the identification card defines, sets, or establishes *where* the fingerprint is stored; that is, the user's fingerprint data is stored with the database record corresponding to the relevant employee number.

Given this, we conclude that Patent Owner's position that Hsu does not disclose a memory location "defined by," "set," or "established" by card information is not accurate. Patent Owner's argument mainly contrasts the terms "associated with," as described in Hsu, with our claim construction that "defined by," means "set" or "established." We agree that these are different words, but an ordinary meaning of "associated" is "related, connected, or combined together." MERRIAM WEBSTER ONLINE DICTIONARY, https://www.merriam-webster.com/dictionary/associated (last visited Jan. 9, 2024) (Ex. 3001). Considering common database structures and functions, we are persuaded that Hsu, by "associating" a user's fingerprint data with a database record corresponding to a particular employee, concomitantly discloses "defining," "setting," or "establishing" a memory location for the fingerprint data in relation to the employee account number. Consistent with our understanding of Hsu's disclosure, Mr. Lipoff testifies persuasively that in Hsu "[t]he 'fingerprint image, or [] selected distinctive attributes or features of the user's fingerprint image' are not stored at *any* memory location in the database – rather, it is stored at a memory location associated with the specific user/employee number received from a card." Ex. 1006 ¶ 93 (citing Ex. 1003 ¶ 26).

Patent Owner's counsel made clear, during oral argument, its position that "there's no discussion at all in Hsu that the ID number/card information in enrollment for purposes of storing the signature, stores [fingerprint data] at a specified location – by location specifically specified by the card data." Ex. 3001 42:21-23. But we

do not agree with this position. As discussed above, Hsu describes that fingerprint data is stored associated with the card data, e.g., an account or employee number. Ex. 1003 ¶ 26 (Hsu describing that "the reference fingerprint data are associated with corresponding user numbers, or employee or customer account numbers."). Consistent with our claim construction, the "association" is the *where.* In other words, we understand that Hsu's associating the fingerprint data with the personal data record in fingerprint database 44 defines, sets, or establishes where the fingerprint data is stored. This occurs, as Hsu explains, because during enrollment the user data such as account or employee number is supplied by the user's card. *Id.* ¶ 11. We do not see it as a significant leap to understand that in Hsu the user's personal data record is the location with which the fingerprint data is associated and stored in fingerprint database 44.

Patent Owner also argues that "[i]n contrast to the claimed method, Hsu teaches that the user's fingerprint data and account number are presented *at the same time* and are then stored in the database *in association with* each other." PO Resp. 18 (citing Ex. 2039 ¶ 49). Patent Owner's declarant, Dr. Russ, similarly testifies that "in Hsu, the fingerprint data and the account number are presented together and are then stored together . . . [t]here is no step in Hsu wherein the account number (or the 'card information') first sets or establishes the memory location." Ex. 2039 ¶ 49. This argument takes advantage of the fact that Hsu does explicitly state a temporal order for "storing . . . the biometric signature" as recited in claim 1. However, as we explained in our claim construction,

> during an enrollment process the claimed "biometric signature," e.g., a fingerprint, is not yet stored in the memory, and no memory location or address has been "defined," as in "set" or "established," in the memory for storing the fingerprint, until card information is received. Once the card information and fingerprint is received during enrollment, the card information provides data that establishes *where*, i.e., at what memory location or address, the system will *store* the fingerprint data.

Section II.C.3. Similarly, in Hsu, the fingerprint data can only be stored once the system has received data indicative of, for instance, an employee number from a user's identification badge, which thus defines a database record with which the fingerprint data can be "associated."

This all makes sense, logically, because Hsu's fingerprint data are not randomly stored, as Mr. Lipoff explains, "in *any* memory location." Ex. 1006 ¶ 93. Hsu's fingerprint data cannot be stored until directed to, i.e. "associated with," a certain database address or record, and in Hsu that is a database record containing the user's identification information.*See* Ex. 1003, 7:7-12. (Hsu describing that during enrollment "the user also presents an account number, employee number or similar identity number . . . [t]he account number is stored in the database 44 in association with the user's fingerprint image data"). Accordingly, from a temporal standpoint during enrollment, Hsu must also use card information, e.g., an employee number stored on the card, to define, set, or

establish a memory location before storing the fingerprint data, wherein the employee number is associated with the fingerprint data. Commensurate with our understanding of Hsu's disclosure, we credit Mr. Lipoff's testimony that even though Hsu does not explain exactly "how a new user record is created" during enrollment, a person of ordinary skill in the art would "try using simple known options for creating database records." Ex. 1032 ¶ 33. Mr. Lipoff explains persuasively that "upon a user enrolling, they provide a previously unseen card/user number, [and] the system then creates a new record for the user, including setting/establishing for the first time the memory location for storing the user's fingerprint." *Id.* ¶ 34.

When asked during his deposition to describe Hsu's database structure and functions, Mr. Lipoff testified consistently with his declaration, explaining essentially that it is the user's employee or account number that defines where the fingerprint data is stored:

> Q. So the account number indicates where the fingerprint is stored because they are stored in association with each other; is that correct?
>
> . . .
>
> A. THE WITNESS:· Well, I think it's – it's more than that. The structure that the database, as Hsu describes it, I believe – let me see. I think it's in paragraph 20. Let me see if I can find it. Yeah, so in paragraph 20, column 4, the database is basically a table that associates each

> user number with a stored fingerprint image or selected attributes.
>
> So what this is telling me is the user number, which you – you said we should call the account number, I believe it's the same thing here, is – is a database, and so the user number is defining the memory location in which the stored fingerprint image will be stored because the structure of the database is one, as indicated here in column 4, that starts with the user number telling you where to find the memory location that has the stored fingerprint image.

Ex. 1041, 33:16-34:9. When Patent Owner's counsel pointed out that Hsu's paragraph 20 did not pertain specifically to enrollment, Mr. Lipoff explained that the database structure and function in paragraph 20 also applies to the enrollment process shown in Figure 4:

> A. Paragraph 20 describes the principle [sic] components of the access control unit, which includes the fingerprint database which is the same fingerprint database that's in – that's in – I'm sorry. Same fingerprint database that's in Figure 4. Figure 4 is the previous paragraph of Hsu we were discussing. Paragraph 26 is the enrollment procedure, but by the time you get to the enrollment procedure, Hsu, earlier in paragraph 20, defined the structure of that same database – database item 44 in Figure 4.

Id. at 34:19-35:9.

Summarizing its position, Patent Owner argues that "Hsu merely discloses that the user's account number and fingerprint data are stored in association with each other. Hsu offers no other teachings as to how the account number and fingerprint data are stored in the database." PO Resp. 15XX (citing Ex. 2039 ¶¶ 53-54). Considering our analysis and the evidence discussed above, we disagree. We are persuaded that Hsu does, in fact, explain *how* the account number and fingerprint data are stored in the fingerprint database. Hsu establishes a memory location for storing the fingerprint data in "association" with an employee or account number, and the "association" is contingent on receiving the employee or account number from Hsu's card or badge during enrollment. *See* Ex 1003, 7:10-12, Fig. 4. (Hsu explaining that "[t]he account number is stored in the database 44 in association with the user's fingerprint image data.").

Overall, we are persuaded, based on Petitioner's arguments and evidence, including the testimony of Mr. Lipoff, that Hsu's association of a fingerprint with a user's underlying account or employee number in a database record during enrollment discloses limitation 1[C], namely "defining, dependent upon the received card information, a memory location in a local memory external to the card."

Patent Owner does not present substantive arguments with respect to the remaining limitations 1[P]-[B] and 1[D]-[E] nor with respect to the combination of Hsu and Sanford. Having reviewed the entirety of the record now before us, specifically the disclosures in Hsu and Sanford,

we accept Petitioner's arguments and evidence with respect to the remaining limitations as our own. Pet. 17-40. We also find that Petitioner and Mr. Lipoff have provided articulated reasoning with evidentiary underpinning as to why an ordinarily skilled artisan would have been motivated to combine the teachings of Hsu and Sanford. Pet. 37-40; Ex. 1003 ¶¶ 108-115.

d) Conclusion as to claim 1

Based on the complete record before us and for the reasons expressed above, we are persuaded that Petitioner has shown by a preponderance of evidence that claim 1 would have been obvious over Hsu and Sanford.

4. Dependent claim 2

Claim 2 depends from claim 1 as it recites "storing a biometric signature according to the enrolment method of claim 1." Ex. 1001, 12:41-42. Claim 2 specifically recites "[a] method of securing a process at a verification station." *Id.* at 12:39. Thus, different from the enrollment process of claim 1, claim 2 is directed to a verification process that follows the enrollment process.

Patent Owner does not provide separate substantive arguments with respect to claim 2, mainly arguing that claim 2 contains the same method steps, specifically limitation 1[C], of claim 1 and "[a]s the prior art cited by [Petitioner] does not teach this limitation, the cited prior art does not render these dependent claims obvious as a result thereof." PO Resp. 30.

Appendix D

Petitioner argues that Hsu discloses using its system for ATM machines to "conduct banking transactions, such as cash withdrawal or deposit transactions." Pet. 41 (quoting Ex. 1003 ¶ 24). Petitioner argues specifically, that "[b]ecause a user of Hsu's system may conduct banking transactions only after her fingerprint is verified, access to the banking transaction process is a verified access." *Id.*

Claim 2 recites in pertinent part the additional step of:

> verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

Ex. 1001, 12:45-50.

Appendix D

Petitioner argues that Hsu discloses "fingerprint correlator 46" in Figure 2 as annotated by Petitioner (Pet. 47) and reproduced below.

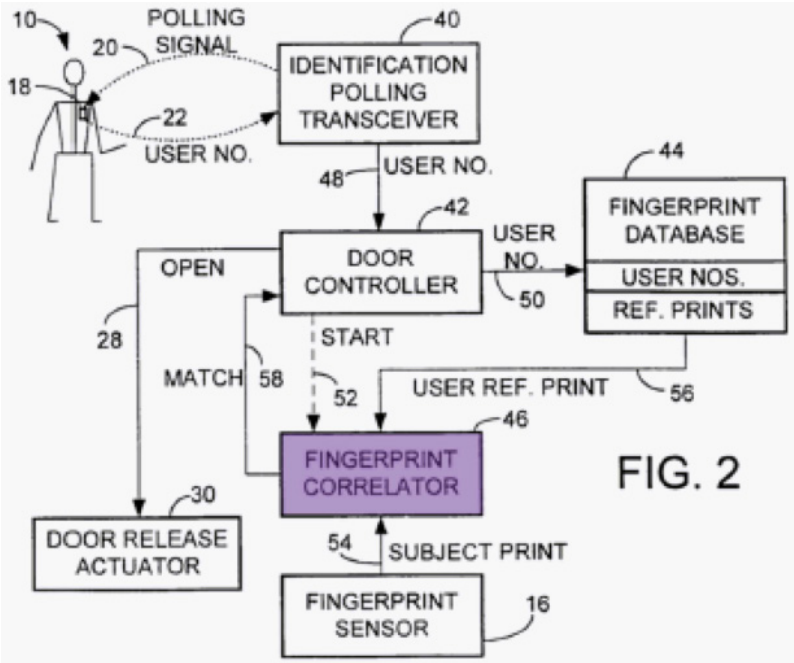


FIG. 2

Hsu's Figure 2 illustrates diagrammatically the use of fingerprint correlator 46 in conjunction with fingerprint sensor 16 and fingerprint database 44. Ex. 1003, Fig. 2. Petitioner argues that "fingerprint correlator 46 (purple) 'compares the subject fingerprint from the sensor 16, received over line 54, with the reference fingerprint features received from the database 44 over line 56' to 'determine[] . . . [if] there is a match.'" Pet. 48 (quoting Ex. 1003 ¶¶ 21, 24). Petitioner argues

further that because "Hsu's card information (*e.g.*, user number or account number) is used to retrieve the stored biometric signature (*e.g.*, fingerprint) . . . Hsu discloses 'verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the [stored] biometric signature.'" *Id.* at 48-49 (citing Ex. 1006 ¶ 131).

Mr. Lipoff testifies that after enrollment, and because the fingerprint is stored associated with, i.e., "set" or "established" by the employee number or account number in a database record, "Hsu discloses 'verifying the subsequently presented presentation of the card information [*e.g.*, Hsu's account or user number] and the biometric signature [*e.g.*, Hsu's fingerprint] if the subsequently presented biometric signature [*e.g.*, Hsu's fingerprint] matches the biometric signature at the memory location.'" Ex. 1006 ¶ 133.

Petitioner's arguments and Mr. Lipoff's testimony are consistent with Hsu's disclosure. For example, Hsu expressly describes a verification procedure using a stored fingerprint:

> The correlator 46 then rapidly compares the subject fingerprint from the sensor 16, received over line 54, with the reference fingerprint features received from the database 44 over line 56. If the correlator 46 determines that there is a match, a match signal is transmitted to the door controller 42 over line 58, and the

> controller generates an "open" signal on line 28 to the door release actuator 30.

Ex. 1003, 5:22-29. For dependent claim 2, we have considered and, on the complete record before us, in addition to our analysis above, accept as our own, Petitioner's arguments and evidence set forth at pages 40-49 of the Petition. Accordingly, we determine that Petitioner has shown by a preponderance of the evidence that claim 2 would have been obvious over Hsu and Sanford.

5. Independent claim 13 and dependent claim 14

Independent claim 13 is an apparatus claim reciting "[a] biometric card pointer enrolment system," and includes similar limitations as independent claim 1. Ex. 1001, 13:67. Different from claim 1, claim 13 also recites "a card device reader," "a biometric reader," and for the remaining limitations recites "means for" along with the same functional language as in limitations 1[C]-[E].

Petitioner argues that besides disclosing the biometric pointer system, "Hsu's biometric card pointer system is also an enrollment system that allows users to be enrolled." Pet. 49-50 (citing Ex. 1006 ¶¶ 68-74, 136). Petitioner points to Hsu's "bank card reader 62," and "fingerprint sensor 16 to account for the recited card and biometric readers in claim 13. *Id.* at 50-51. Considering the "means for" limitations in the remainder of the claim, Petitioner points to the requisite function and structure, for example, for limitation 13[C] Petitioner explains that

> [t]he function of this limitation is "defining, dependent upon the received card information, a memory location in a local memory external to the card."

Id. And for the structure:

> Structure corresponding to the claimed means is a computer system with a processor executing an application that uses any segment of card information 605 from a card 601 (1) as a memory reference as shown in Fig. 4 or (2) to determine a group of associated memory references or 3) all equivalents of (1) and (2). Structure is found in '039 Patent, col. 6, line 66 – col. 7, line 23; col. 7, lines 31-35, 39-42, 47-48; col. 8, lines 44-46; col. 11, lines 29-37; col. 12, lines 1-9; Fig. 4.

Id. at 51-52. Petitioner argues that "as explained for Limitation 1[C], Hsu discloses the recited function" which is "defining, dependent upon the received card information, a memory location in a local memory external to the card." *Id.* at 52. For the structure, Petitioner asserts that "Hsu discloses or renders obvious that fingerprint matching is performed by computer processors executing software/application . . . [f]or example, Hsu discloses using ASIC capable of 'parallel processing' for fingerprint verification." *Id.* at 53 (citing Ex. 1006 ¶ 23). And, Petitioner argues "Hsu discloses using card information to determine a group of memory references, which are associated because they correspond to the same user." *Id.* (citing Ex. 1006 ¶ 149).

Apart from its arguments with respect to independent claim 1[C], Patent Owner does not dispute Petitioner's evidence that Hsu, and Hsu in view of Sanford, disclose and teach the limitations of independent claim 13. *See generally* PO Resp. And, in addition to being persuaded that Hsu discloses the necessary structure and function intimated by "means for," we find that Hsu renders obvious limitation 13[C] for the same reasons as limitation 1[C]. Based on our review, we find that the complete record fully supports Petitioner's showing that Hsu and Sanford disclose all the limitations of claim 13. Pet. 49-56.

Dependent claim 14, similar to claim 2, relates to a "verified access system" including "means for verifying (i) a subsequent presentation of card information to the card device reader . . . and (ii) a subsequent presentation of a biometric signature to the biometric reader." Ex. 1001, 14:10-21. Mr. Lipoff testifies that with respect to "means for verifying," "Hsu discloses the recited function, for the same reasons I explained for Limitation 2[C]." Ex. 1006 ¶ 174. And for structure, Mr. Lipoff testifies that a person of ordinary skill in the art "would have understood that the verification process in Hsu (*i.e.*, comparing an inputted fingerprint to a stored fingerprint) would or could obviously be accomplished by at least one processor executing an application." *Id.* ¶ 175.

For dependent claim 14, we have considered and on the complete record before us, accept as our own, Petitioner's arguments and evidence set forth at pages 57-60 of the Petition. After weighing all relevant factual findings, including the level of ordinary skill in the art, the scope

and content of Hsu and Sanford, and any differences between Hsu, Sanford and the claimed invention, we conclude that Petitioner demonstrates by a preponderance of the evidence that claims 13 and 14 of the '039 patent are unpatentable as obvious over Hsu and Sanford under 35 U.S.C. § 103(a).

6. Claims 19 and 20

Independent claim 19 and dependent claim 20 include essentially the same limitations as claims 1 and 2, except, that the preamble to claim 19 recites:

> A non-transitory computer readable medium having recorded thereon a computer program for directing a processor to execute a method of enrolling in a biometric card pointer system, the program comprising:

Ex. 1001, 15:25-16:2. And, for example, the limitation of "receiving card information," in independent claim 1, is recited in independent claim 19 as "code for receiving card information."

Petitioner argues that Hsu "discloses various components of its biometric card pointer system (*e.g.*, access control unit) in Figs. 2, 3, and 4, such as a card reader, a fingerprint sensor, a door/access controller, a fingerprint correlator, and a fingerprint database." Pet. 60. Petitioner argues further that Sanford specifically describes a system that "includes a processor. The processor may be, for example, a computer, workstation, mainframe, pocket PC, personal digital assistant, etc. The

processor also preferably includes or is in communication with a verification process 22 and database 24. Verification process 22 may be a software-implemented process that communicates with database 24." *Id.* at 61 (quoting Ex. 1004 ¶ 18). Based on such disclosures, Mr. Lipoff testifies that a person of ordinary skill in the art "would have understood that the Hsu-Sanford system includes a processor running computer programs stored on a non-transitory computer readable medium." Ex. 1006 ¶ 179.

Mr. Lipoff's testimony as to what a person of ordinary skill in the art would understand in regards to the known internals, programming instructions, and memory structure for a biometric card enrollment and verification system is unrebutted on this record.

Petitioner's arguments and evidence are in all other respects the same as the arguments and evidence presented with respect to claims 1 and 2. We have considered, and on the complete record before us, accept as our own, Petitioner's arguments and evidence set forth at pages 60-73 of the Petition as to claims 19 and 20. Accordingly, we determine that Petitioner has shown by a preponderance of the evidence that claims 19 and 20 would have been obvious over Hsu and Sanford for the same reasons as claims 1 and 2.

E. Ground 2: Claims 1, 2, 13, 14, 19 and 20 in view of Hsu, Sanford, and Tsukamura

Because we determine that claims 1, 2, 13, 14, 19, and 20 would have been obvious over Hsu and Sanford, we

need not address these same claims 1, 2, 13, 14, 19, 20 as obvious over Hsu, Sanford, and Tsukamura.

F. Patent Owner's continued 315(b) arguments

In their Response, Patent Owner reiterates their 315(b) argument that we previously addressed in our Institution Decision. PO Resp. 30-47; Inst. Dec. 9-34. Now, Patent Owner argues that in our prior decision we placed too much weight on a lack of control of the proceedings by Apple, and that "[r]ather, a key to the RPI analysis is whether Apple and Petitioners have a structured, preexisting business relationship and whether Apple would receive more than a merely generalized benefit if trial is instituted." PO Resp. 34 (citing *Applications in Internet Time, LLC v. RPX Corp.*, 897 F.3d 1336, 1351 (Fed. Cir. 2018)).

As an initial matter, we think that Patent Owner's argument mischaracterizes, or at least oversimplifies the holding in *AIT.* In *AIT*, the Federal Circuit admonished the Board for (1), making "certain factual findings that are not supported by substantial evidence," and (2) "fail[ing] to adhere to the expansive formulation of 'real party in interest' that is dictated by the language, structure, purpose, and legislative history of § 315(b)." *AIT*, 897 F.3d at 1351. The Federal Circuit explained in *AIT* that the Board failed to appreciate, among other things, the specific nature of the relationship between RPX and Salesforce, "that RPX, . . . is a for-profit company whose clients pay for its portfolio of 'patent risk solutions.'" *Id.* The Court stated that "the Board did not consider these

facts, which, taken together, imply that RPX can and does file IPRs to serve its clients' financial interests, and that a key reason clients pay RPX is to benefit from this practice in the event they are sued by an NPE." *Id.* at 1352. As discussed below, we have not overlooked the facts and evidence surrounding the parties' relationship nor failed to consider the parties' litigation efforts in the district courts. To the extent Patent Owner has raised valid arguments that may have not been clearly addressed by the Board, we provide the following additional analysis.

With respect to point (1), it is important, factually, that the developer-distributor business relationship between Petitioner and Apple contrasts sharply with the specific intent of the NPE patent portfolio litigation relationship between RPX and Salesforce. As we described in our Institution Decision, Petitioner's product "Yale Smart Locks", including "the Yale Assure Lock uses a software application ('App') on one's mobile phone, here on an iPhone sold by Apple, to lock and unlock doors. The App is developed by Petitioner, or one of its business partners, and distributed to iPhone users through the Apple App store." Inst. Dec. 16. The Developer Agreement (the "Agreement") between Petitioner and Apple mainly provides "a limited license" to use Apple software "to develop and test" the developer's software applications for integration on Apple's iOS platforms. Ex. 2009. Importantly, different from *AIT*, in this case we have before us no facts or evidence showing that the intent, express or otherwise, of the Agreement between Petitioner and Apple is *fundamentally* based on

protecting one party or the other from patent litigation.[9] To the extent Patent Owner now argues that we did not appreciate all of its arguments and evidence as to the parties underlying actions in related district court proceedings, we address that matter in due course below. Before doing so, we turn to point (2), and whether, in this case, our Institution Decision appropriately considered the "expansive formulation of 'real party in interest.'" *AIT*, 897 F.3d at 1351.

In *AIT*, the Federal Circuit explained that the "Board's determination that Salesforce was not a real party in interest under § 315(b) relied on an impermissibly narrow understanding of the common-law meaning of the term." *Id.* at 1357. For one thing, the Court pointed out that "an agent with an ownership interest in the subject matter of the suit, or one who is the trustee of an express trust or a party in whose name a contract has been made for the benefit of another, may qualify as a real party in interest." *Id.* In this proceeding, Patent Owner has failed to point to any persuasive evidence, apart from software compatibility with Apple's iOS platforms as discussed in the Agreement, that Apple has any overt interest, influence, development or design influence over Petitioner's "Yale Smart Locks" products or App. In

9. We acknowledge that the Agreement contains representations and warranties of noninfringement, as well as indemnification clauses. Ex. 2009, 16, 41-43. We consider that these clauses are perhaps best understood, at least from Apple's perspective as a distributor, as mechanisms to avoid liability should the need arise, rather than tools exerting control or perpetuating an agency relationship with Petitioner.

addition, Patent Owner has produced no evidence that Apple holds any ownership interest, assets, or expressly administers any property rights as a trustee or agent for the benefit of Petitioner indicative of real party in interest relationships under common law.

Essentially the entirety of the evidence of the business relationship in this proceeding is contained within the Agreement which we already discussed in detail in our Institution Decision. Inst. Dec, 9-34. For example, there is an indemnification clause that requires Petitioner to

> [u]pon Apple's request, defend, Apple, its directors, officers, employees, independent contractors and agents (each an "Apple Indemnified Party") from any and all claims, losses, liabilities, damages, taxes, expenses and costs, including without limitation, attorneys' fees and court costs (collectively, "Losses"), incurred by an Apple Indemnified Party and arising from or related to . . . any claims that Your Covered Product or the distribution, sale, offer for sale, use or importation of Your Covered Product (whether alone or as an essential part of a combination), Licensed Application Information, metadata, or Pass Information violate or infringe any third party intellectual property or proprietary rights;

Id. at 43. There is no evidence in this case that Apple has invoked their rights under this clause, nor has Patent Owner argued or explained how this clause or the

parties' actions before the Board and in the underlying district court litigation implicate a common law agency relationship between the parties. An agency relationship could potentially occur if Apple were to request Petitioner to step in and defend it. Yet Patent Owner has provided no argument or persuasive evidence that such is the case here. Apple has, in fact, committed to its own defense by filing its own IPR, e.g., IPR2022-00600, against Patent Owner. Moreover, compelling evidence provided by Petitioner in this case is exactly the opposite, and avers under penalty of perjury that "[t]here have been no communications between Petitioners and Apple, directly or through counsel, relating to indemnification or obligation to indemnify based on assertion of . . . U.S. Patent No. 8,620,039) (*id.* at 11-12)." Ex. 1023, 8-9, 14.

We recognize that Apple may derive some benefit if additional claims of the '039 patent are determined to be unpatentable in this proceeding. This derived benefit does not, however, make Apple an RPI to this proceeding. *See WesternGeco LLC v. ION Geophysical Corp.*, 889 F.3d 1308, 1321 (Fed. Cir. 2018) (stating in the context of the broader concept of privity that "[a]s a general proposition, we agree with the Board that a common desire among multiple parties to see a patent invalidated, without more, does not establish privity").

On the facts and evidence before us in this proceeding it is the Agreement, analyzed here and in our Institution Decision, that best explains the business relationship between the parties. The Agreement sets forth with reasonable clarity the specific expectations of the parties,

mainly that (a) Petitioner is allowed "a limited license to use the Apple Software and Services provided to You under this Program to develop and test Your Applications on the terms and conditions set forth in this Agreement;" and (b) "Applications that meet Apple's Documentation and Program Requirements may be submitted for consideration by Apple for distribution via the App Store, Custom App Distribution, or for beta testing through TestFlight." Ex. 2009, 1. Accordingly, the evidence leads us to conclude that Apple is a distributor of Petitioner's App for use with Petitioner's "Yale Smart Lock" products, and without more, that is about all that can be said about the relationship.

We turn, below, to particular facts in this case that Patent Owner argues the Board overlooked in our Institution Decision.

During oral argument Patent Owner's counsel raised an issue concerning our earlier conclusion in our Institution Decision that Apple is *not* a real party in interest to this proceeding or a privy with Petitioner. Inst. Dec. 28; Tr. 45-46. Counsel contends "there is an inconsistency between [Petitioner's], you know, assertions regarding Apple in the [Declaratory Judgment] complaint. And then in defending the RPI position." Tr. 45:20-23. Specifically, counsel explained that they "didn't see that the Board specifically considered our argument that it's relevant that ASSA ABLOY filed the DJ complaint with respect to the '039 patent, even though the '039 patent had never been raised by Patent Owner to ASSA ABLOY." *Id.* at 46:3-6. Counsel further argued that the present

"situation mirror[s] the situation in the *Worlds v. Bungie* case, where a very similar fact pattern was considered relevant by the [F]ederal [C]ircuit." *Id.* at 46:7-9; *see also Worlds Inc. v. Bungie, Inc.*, 903 F.3d 1237, 1239 (Fed. Cir. 2018) ("*Bungie*") (determining that because "the Board erred in its real-party-in-interest analysis, we vacate its decisions and remand for proceedings consistent with this opinion").

As an initial matter, our analysis of Petitioner's section 315(b) time-bar arguments in our Institution Decision covers 20 pages and considers in detail evidence submitted by both parties regarding business relationships and the Apple Developer License Agreement, i.e., the "Agreement," (Ex. 2009) including warranties, indemnification, product inspection and insurance, between Petitioner and Apple. Inst. Dec. 9-29. For example, as it relates to Patent Owner's issue raised here, we noted that "[i]n the Declaratory Judgment complaint, Petitioner states, '[CPC] is also engaged in an aggressive litigation campaign that includes Apple Inc. ('Apple'), *a business partner* of [Petitioner]." *Id.* at 14. We explained that

> [t]he business relationship between Apple and Petitioner is that Petitioner, or one of the named entities collectively referred to as Petitioner, makes products that interface with Apple products and may be sold on Apple's website. For example, ASSA ABLOY Residential Group, Inc., a named entity included as a Petitioner in this proceeding, makes and sells security locks under the brand name "Yale" . . . the

> Yale Assure Lock uses a software application ("App") on one's mobile phone, here on an iPhone sold by Apple, to lock and unlock doors. The App is developed by Petitioner, or one of its business partners, and distributed to iPhone users through the Apple App store.

Id. at 14-15. Thus, in our Institution Decision, we did consider the fact that Petitioner, in its Declaratory Judgment Complaint, admitted to being a business partner with Apple. We also considered the fact that as part of the business relationship Petitioner entered into the Agreement. *Id.* at 18. We considered critical clauses in the Agreement such as the representations and warranties clause explaining that "[w]e do *not* consider Section 3.2(d) to be a 'warranty.' It is not a guarantee that products will not infringe. It is a representation of the developer's current 'knowledge and belief.' It is far different from the obligations created by the App developer's agreement in *Bungie*." *Id.* at 19.

With respect to indemnification, we determined that the Agreement did in fact contain an indemnification clause, which *could* be implemented "upon Apple's request." *Id.* at 22. However, also different from the facts in *Bungie*, in this case we have sworn interrogatories provided by Petitioner presenting strong evidence that "[t]here have been no communications between Petitioners and Apple, directly or through counsel, relating to indemnification or obligation to indemnify based on assertion of . . . U.S. Patent No. 8,620,039." *Id.* at 23 (quoting Ex. 1023, 11-12).

Patent Owner now urges us to also consider the fact that its cease-and-desist letters to Petitioner, i.e., the "Yale Letters" (Exs. 2005, 2006), never threatened Petitioner with infringement of the '039 patent, only U.S. Patent Nos. 9,665,705 and 9,269,208. *See* Prelim. Resp. 7 (Patent Owner arguing that it "never raised or otherwise mentioned the '039 Patent to Yale or any of the Petitioners at any time") (citing Ex. 2008). This is a concern, Patent Owner contends, because Petitioner filed its Declaratory Judgment Complaint admitting to a business relationship with Apple as well as this IPR, and both proceedings challenge the '039 patent. *See* Ex. 2007 ¶ 2 (Petitioner stating in its Declaratory Judgment Complaint that "[t]he ASSA ABLOY Entities seek a declaration of non-infringement of U.S. Patent Nos. 9,269,208 ("the '208 Patent"), 9,665,705 ("the '705 Patent"), and 8,620,039 ("the '039 Patent") (collectively, the "Patents-in-Suit")").

This argument is frankly somewhat undeveloped in Patent Owner's explanations of the facts and background in its Preliminary Response. Prelim. Resp. 5-10. We acknowledge that Petitioner was apparently never overtly threatened with infringement of the '039 patent. Ex 2005; Ex. 2006. Yet Patent Owner fails to persuasively explain *why* Petitioner's challenges to the '039 patent in the Declaratory Judgment Complaint weigh in favor of finding a privy or a real party-in-interest relationship between Petitioner and Apple. *See* Prelim. Resp. 7 (Patent Owner arguing largely that "Patent Owner never raised or otherwise mentioned the '039 Patent to Yale or any of the Petitioners at anytime"). As we understand the argument,

Patent Owner alleges that because it never threatened Petitioner with the '039 patent, Petitioner is now, without provocation, doing Apple's bidding and working at Apple's behest by challenging the '039 patent in the Declaratory Judgment Complaint and in these *inter partes* review proceedings. It is also not clearly explained why the inclusion of Petitioner's related entities of ASSA ABLOY Global Solutions, Inc. ('Hospitality'), and HID Global Corporation, in these IPR proceedings as real parties-in-interest and also in the Declaratory Judgment Complaint, matters as to the relationship between Petitioner and Apple. *See* Prelim. Resp. 8 (Patent Owner's arguing that "Petitioners also filed the Declaratory Judgment Complaint as to HID and Hospitality, whom Patent Owner had never contacted regarding the patents or technology at issue") (citing Ex. 2005; Ex. 2006; Ex. 2008).

Two things can be true. Petitioner can have a business relationship with Apple and both parties can have a legitimate interest in defending themselves separately in litigation. We do not find anything in Petitioner's Declaratory Judgment Complaint that alters our prior decision in this regard. The fact that Petitioner and each of its entities were not explicitly threatened with infringement allegations in the Yale Letters as to the '039 patent does not mean that Patent Owner would never assert infringement against Petitioner based on the '039 patent claims. Ex. 2005; Ex. 2006. This is especially true in light of the fact that Patent Owner asserted the '039 patent against Apple in *CPC Patent Technologies Pty Ltd v. Apple Inc.*, No. 3:22-cv-02553, apparently due to or resulting from the products that Petitioner makes, uses,

and sells through Apple's electronic device platforms. Ex. 2007 ¶ 44 ("On February 23, 2021, [Patent Owner] asserted all three of the Patents-in-Suit against Apple.").

On the facts here, we conclude that filing a declaratory judgment action or an *inter partes* review to challenge the claims of a patent, i.e., the '039 patent, that was asserted against a third party, but based on Petitioner's product, is a reasonable litigation strategy for Petitioner independently. The declaratory judgment action filing itself does not demonstrate some sort of heightened collusion even where a benefit inures to a party with whom Petitioner has a business relationship. Patent Owner has not explained, for instance, that, but for Apple's technology or actions, Petitioner has no actionable reason to challenge the patentability of the '039 patent claims. *See*, *generally*, Prelim. Resp. Also, by way of example, Patent Owner argues in its Preliminary Response that in the Declaratory Judgment Complaint, "Petitioners further asserted that 'it is highly likely that Charter Pacific will sue the Assa Abloy Entities *on the same patents that have been asserted against Apple*.'" Prelim. Resp. 22 (quoting Ex. 2007 ¶ 30). In our view, this assertion is primarily offered in the Complaint to show Petitioner's apprehension of litigation because it admittedly makes, uses, and sells products potentially covered by the claims in the same three patents through Apple's platforms. Patent Owner does not explain persuasively why Petitioner would not have been concerned about infringing the '039 patent, nor why such apprehension shows any more intimate relationship than we considered in our Institution Decision. The mere fact that an accused infringer, in this case Petitioner, files a declaratory judgment action explaining its business

relationship with Apple and offering reasons supporting the declaratory judgment action with respect to the same three patents that Apple is accused of infringing, does not, without more, establish persuasive additional information or substantive facts that we failed to consider in our original analysis.

Overall, and on the complete record before us we do not find that any of Petitioner's assertions in its Declaratory Judgment Complaint change our underlying conclusion that Petitioner and Apple are not in privy or real parties in interest. *See* Inst. Dec. 34 (determining that "[t]he totality of the evidence before us does not establish anything other than a traditional business relationship between Apple and Petitioner").

III. CONCLUSION[10]

For the reasons discussed above, we determine Petitioner meets its burden of establishing, by a preponderance of the evidence, that the challenged claims are unpatentable, as summarized in the following table:

---

10. 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).

Appendix D

Claims	35 U.S.C. §	Reference(s) Basis	Claims Shown Unpatentable	Claims not shown Unpatentable
1, 2, 13, 14, 19, 20	103(a)	Hsu, Sanford	1, 2, 13, 14, 19, 20	
1, 2, 13, 14, 19, 20	103(a)	Hsu, Sanford, Tsukamura[11]		

III. ORDER

For the reasons given, it is

ORDERED that, based on a preponderance of the evidence, claims 1, 2, 13, 14, 19, and 20 of the '039 patent have been shown to be unpatentable; and

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

For PETITIONER: Dion Bregman, Andrew Devkar, and James Kritsas - MORGAN LEWIS & BOCKIUS LLP

For PATENT OWNER: Andrew Ryan - CANTOR COLBURN LLP

---

11. Because Petitioner's contentions regarding the obviousness of claims 1, 2, 13, 14, 19, and 20 in view of Hsu and Tsukamura are dispositive of these challenged claims, we do not reach asserted ground 2. *See In re Gleave*, 560 F.3d. at 1338.

APPENDIX E — JUDGMENT OF THE PATENT TRIAL AND APPEAL BOARD, NO. IPR2022-01093, DATED JANUARY 31, 2024

PATENT TRIAL AND APPEAL BOARD

IPR2022-01094
Patent No. 8,620,039 B2

ASSA ABLOY AB, ASSA ABLOY INC., ASSA ABLOY RESIDENTIAL GROUP, INC., AUGUST HOME, INC., HID GLOBAL CORPORATION, AND ASSA ABLOY GLOBAL SOLUTIONS, INC.,

Petitioner,

v.

CPC PATENT TECHNOLOGIES PTY, LTD,

Patent Owner.

Dated January 31, 2024

Before SCOTT A. DANIELS, AMBER L. HAGY and FREDERICK C. LANEY, Administrative Patent Judges.

JUDGMENT

Final Written Decision Determining All Challenged Claims Unpatentable

35 U.S.C. § 318(a)

DANIELS, Administrative Patent Judge.

Appendix E

I. INTRODUCTION

ASSA ABLOY AB, ASSA ABLOY Inc., ASSA ABLOY Residential Group, Inc., August Home, Inc., HID Global Corporation, and ASSA ABLOY Global Solutions, Inc., ("ASSA" or "Petitioner") filed a Petition requesting *inter partes* review ("IPR") of claims 3-12 and 15-18 of U.S. Patent No. 8,620,039 B2 (Ex. 1001, "the '039 patent"). Paper 2 ("Pet"). CPC Patent Technologies PTY, Ltd., ("CPC" or "Patent Owner") filed a Preliminary Response to the Petition. Paper 11 ("Prelim. Resp."). Petitioner filed a Reply to Patent Owner's Preliminary Response. Paper 15 ("Prelim. Reply"). Patent Owner filed a Sur-Reply to Petitioner's Reply. Paper 18 ("Prelim. Sur-Reply").

Following our Institution Decision (Paper 20, "Inst. Dec."), in which we determined that Petitioner was *not* time-barred from filing its Petition, Patent Owner filed a Response. Paper 23 ("PO Resp."). *See* Inst. Dec. 9-34. Petitioner filed a Reply. Paper 25 ("Pet. Reply"). Patent Owner filed a Sur-Reply. Paper 29 ("PO Sur-Reply"). An oral hearing was held on November 9, 2023. A transcript of the hearing has been entered as Paper 35. ("Tr.").

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision is entered pursuant to 35 U.S.C. § 318(a). For the reasons explained below, we determine that Petitioner has met its burden of showing by a preponderance of the evidence that claims 3-12 and 15-18 are unpatentable.

Appendix E

A. Real Parties in Interest

Petitioner states that ASSA ABLOY AB, ASSA ABLOY Inc., ASSA ABLOY Residential Group, Inc., August Home, Inc., HID Global Corporation, and ASSA ABLOY Global Solutions, Inc., are the real parties in interest.[1] Pet. 1. Patent Owner states that CPC Patent Technologies PTY, Ltd., is the real party in interest. Paper 4, 2.

B. Related Matters

Petitioner indicates that it filed a declaratory judgment against Patent Owner with respect to the '039 patent in *ASSA ABLOY AB, et al. v. CPC Patent Technologies Pty Ltd., et al.*, No. 3-22-cv-00694, in the United States District Court for the District of Connecticut. Pet. 1-2. And Petitioner points out that the '039 Patentis asserted against Apple, Inc., in *CPC Patent Technologies Pty Ltd v. Apple Inc.*, No. 3:22-cv-02553, in the United States District Court for the Northern District of California, San Jose Division. *Id.* Petitioner points out that Apple challenged the '039 patent in IPR2022-00600. *Id.* at 2. On October 13, 2023, we entered a Final Written Decision (Paper 22) in IPR2022-00600 finding claims 1, 2, 19, and 20 of the '039 patent invalid for obviousness. Concurrently with this Decision, in IPR2022-01093, we determine that

1. In its Declaratory Judgment Complaint against Patent Owner, Petitioner also refers to ASSA ABLOY Global Solutions, Inc., as "ASSA ABLOY Global Solutions, Inc. ('Hospitality')." Ex. 2007, 2.

claims 1, 2, 13, 14, 19, and 20 of the '039 patent are invalid for obviousness.

In addition to the proceedings noted by Petitioner, Patent Owner indicates that "the following judicial and/or administrative matters [] may affect, or be affected by, a decision in this proceeding:" *CPC Patent Technologies PTY Ltd. v. HMD Global Oy*, Case No. 6:21-cv-00166 in the United States District Court for the Western District of Texas; IPR2022-00600; IPR2022-00601; IPR2022-00602; IPR2022-01006; IPR2022-01045; IPR2022-01089; and IPR2022-01093. Paper 4, 2-3.

C. The '039 Patent (Ex. 1001)

The '039 patent, titled "Card Device Security Using Biometrics," relates to a biometric card pointer (BCP) system intended to more efficiently and securely permit a user to store biometric information during a user enrollment phase, and in future verification processes permits the user access their account using an identification (ID) card and biometric information such as a fingerprint. Ex. 1001, code (54), 2:51-3:11.

The '039 patent explains that in the enrollment phase "[t]he card user's biometric signature is automatically stored the first time the card user uses the verification station in question (this being referred to as the enrolment phase)." *Id.* at 2:62-64. The '039 patent explains further that "[t]he biometric signature is stored at a memory address defined by the ('unique') card information on the user's card as read by the card reader of the verification

station." *Id.* at 2:64-67. Following the enrollment phase, the '039 patent describes that

> [a]ll future uses (referred to as uses in the verification phase) of the particular verification station by someone submitting the aforementioned card requires the card user to submit both the card to the card reader and a biometric signature to the biometric reader, which is verified against the signature stored at the memory address defined by the card information thereby determining if the person submitting the card is authorised to do so.

Id. at 3:4-11.[2] For both enrollment and future uses, the use of the ID card at a verification station "is identical from the card user's perspective, requiring merely input of the card to the card reader, and provision of the biometric signature ([e.g.] thumb print or retinal scan etc.) to the biometric reader." *Id.* at 3:12-15.

2. The words "enrolment," "authorise," and "authorisation" are the British spellings of "enrollment," "authorize," and "authorization." *See*, *e.g.*, https://www.merriam-webster.com/dictionary/authorisation, last visited Jan. 5, 2023. We will use the American English spelling of these words except where quoted from the '039 patent.

Appendix E

Figure 4 of the '039 patent is reproduced below.

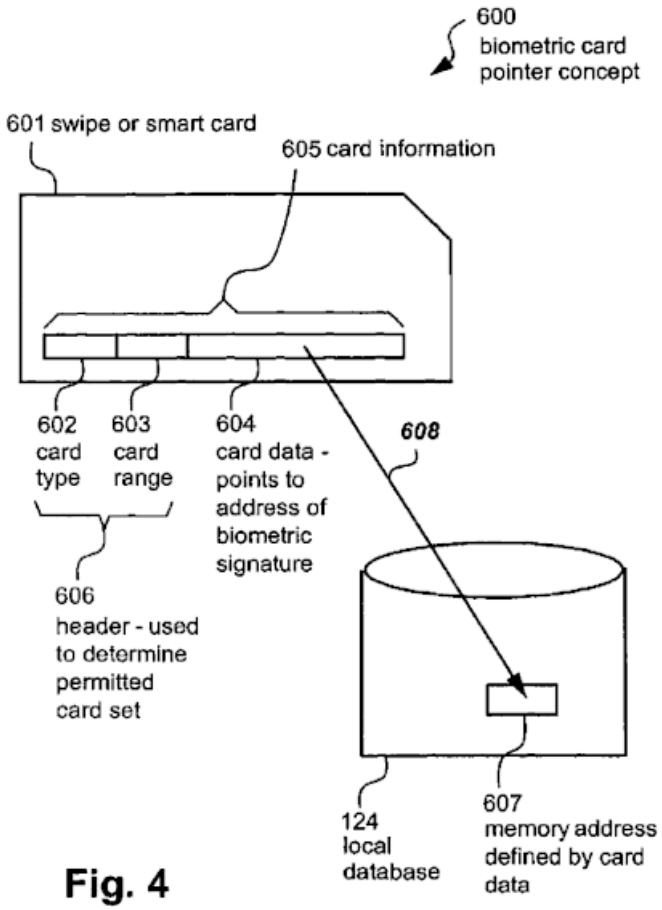


Fig. 4

Figure 4, of the '039 patent, above, illustrates swipe or smart card 601 including card information 605 encompassing fields for card type 602, card range 603, and card data 604. The '039 patent describes that "the card data 604 acts as the memory reference which points, as

depicted by an arrow 608, to a particular memory location at an address 607 in the local database 124." *Id.* at 7:31-35. Information 605 can be encoded on a magnetic strip on the card, for example. *Id.* at 7:28-29. The '039 patent explains that for a specific user "[i]n an initial enrolment phase, . . . [t]he card data 604 defines the location 607 in the memory 124 where their unique biometric signature is stored." *Id.* at 7:43-49. And, the '039 patent explains further that "in later verification phases, . . . [t]his signature is compared to the signature stored at the memory location 607 in the memory 124, the memory location 607 being defined by the card data 604 read from their card 601 by the card reader 112." *Id.* at 7:50-56.

Figures 6 and 7, reproduced below, depict the differences between verification process 205 shown in Figure 6, and enrollment process 207 shown in Figure 7.

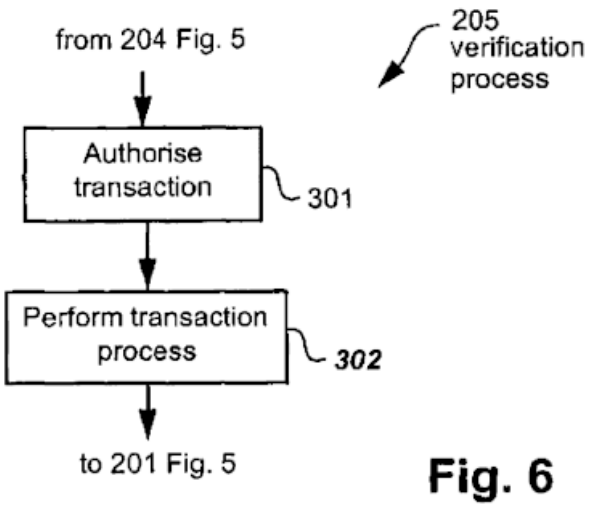


Fig. 6

Appendix E

Figure 6 illustrates verification process 205, which occurs after the enrollment process, illustrated below in Figure 7.

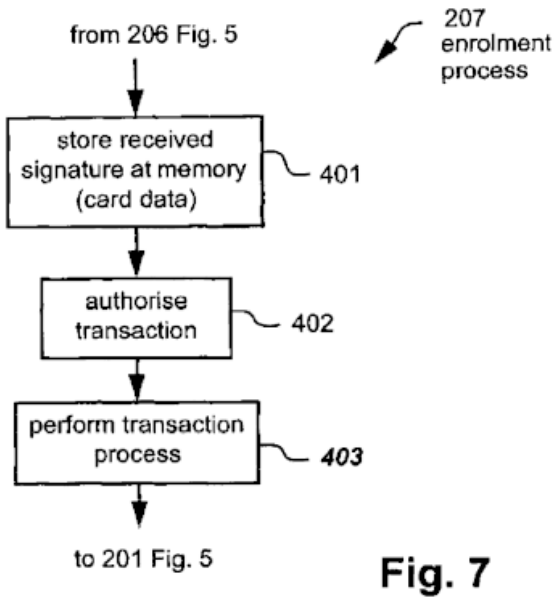


Fig. 7

Figure 7 of the '039 patent illustrates enrollment process 207 where the system at "step 401 stores the biometric signature received by the step 203 in the memory 124 at a memory address defined by the card data 604." *Id.* at 9:64-66 (referring to elements 203 and 124 described in Figure 5). Figure 6 illustrates that verification process 205

> is entered from the step 204 in FIG. 5, after which a step 301 authorises the transaction. This authorisation step 301 indicates that the

> biometric signal received by the biometric reader 102 in the step 203 matches the biometric signature previously stored in the local database 124 by a previous enrolment process 207.

Id. at 9:43-48. Then, "step 204 reads the contents stored at a single memory address defined by the card data 604 and checks these contents against the biometric signature received in the step 203." *Id.* at 8:34-37.

A difference between verification process 205 and enrollment process 207 is that the enrollment process includes step 401, which *stores* the biometric signature "at a memory address defined by the card data 604," whereas in verification process 205 "step 204 *reads* the contents stored at a single memory address defined by the card data 604" and compares the stored biometric signature with the input biometric signature. *Id.* at 9:65-66, 8:24-26 (emphasis added).

D. Illustrative Claim

Claims 3, 15, and 18 are independent. Each of claims 4-12 and 16-17 depends, respectively, from independent claims 3 and 15. Claim 3, a method claim, illustrates the claimed subject matter and is reproduced below with certain limitations of interest in italics:[3]

---

3. We adopt and have applied Petitioner's alphanumeric designations for the elements of the challenged claims. *See, e.g.*, Pet. 12-36.

Appendix E

3. 3[P] A method of securing a process at a verification station, the method comprising the steps of:

3[A] (a) providing card information from a card device to a card reader in the verification station;

3[B] (b) inputting a biometric signature of a user of the card device to a biometric reader in the verification station;

3[C] (c) determining if the provided card information has been previously provided to the verification station;

3[D(P)] (d) *if the provided card information has not been previously provided to the verification station;*

3[D(1)] *(da) storing the inputted biometric signature in a memory at a memory location defined by the provided card information;* and

3[D(2)] (db) performing the process dependent upon the received card information;

3[E(P)] (e) if the provided card information has been previously provided to the verification station;

> 3[E(1)] (ea) comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;
>
> 3[E(2)] (eb) if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and
>
> 3[E(3)] (ec) if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

Ex. 1001, 11:67-14:21. The limitations 3[A]-3[E(3)] are similarly recited in independent claim 15 as an apparatus claim for "[a] verification station for securing a process," and also in independent claim 18 in the context of "[a] non-transitory computer readable medium." *Id.* at 14:23-46, 14:64-15:24.

E. Prior Art and Asserted Grounds

Petitioner asserts that claims 1-12 and 15-18 would have been unpatentable based on the following grounds:

Appendix E

Ground	Claim(s) Challenged	35 U.S.C. §[4]	Reference(s)/ Basis
1	3, 4, 6-11, 15, 16, 18	103(a)	Sanford,[5] Hsu,[6]
2	3, 4, 6-11, 15, 16, 18	103(a)	Sanford, Hsu, Tsukamura[7]
3	5	103(a)	Sanford, Hsu, Leu[8]
4	5	103(a)	Sanford, Hsu, Leu, Tsukamura
5	12	103(a)	Sanford, Hsu, Houvener[9]

4. The Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112-29, 125 Stat. 284, 296-07 (2011), took effect on September 16, 2011. The changes to 35 U.S.C. §§ 102 and 103 in the AIA do not apply to any patent application filed before March 16, 2013. Because the application for the patent at issue in this proceeding has an effective filing date before March 16, 2013, we refer to the pre-AIA version of the statute.

5. Ex. 1004, PCT Appl'n No. PCT/US03/07238 (pub. Sept. 18, 2003).

6. Ex. 1003, European Patent Appl'n No. EP 0924655 A2 (pub. June 23, 1999).

7. Ex. 1005, US Patent No. 6,963,660 B1 (Nov. 8, 2005).

8. Ex. 1008, European Patent Appl'n No. EP O 881 608 A1 (pub. Dec. 2, 1986)

9. Ex. 1010, US Patent No. 5,790,674 (Aug. 4, 1998).

6	12	103(a)	Sanford, Hsu, Tsukamura, Houvener
7	17	103(a)	Sanford, Hsu, McCalley[10]
8	17	103(a)	Sanford, Hsu, Tsukamura, McCalley

Petitioner relies on the testimony of Stuart Lipoff. Ex 1006 ¶¶ 1-459. Patent Owner presents the testimony of Samuel Russ, Ph.D. Ex. 2039 ¶¶ 1-72.

II. ANALYSIS

A. Legal Standards

A patent claim is unpatentable under 35 U.S.C. § 103 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. 35 U.S.C. § 103; *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). "[W]hen a patent claims a structure already known in the prior art that is altered by the mere substitution of one element for another known in the field, the combination must do more than yield a predictable result." *KSR*, 550 U.S. at 416 (citing *United States v. Adams*, 383 U.S. 39, 50-51

10. Ex. 1011, US Patent No. 5,956,415 (Sep. 21, 1999).

(1966)). The question of obviousness is resolved based on 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 ordinary skill in the art; and (4) when in evidence, objective evidence of non-obviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966).

B. Level of Ordinary Skill in the Art

Factors pertinent to a determination of the level of ordinary skill in the art include (1) the educational level of the inventor; (2) the type of problems encountered in the art: (3) prior art solutions to those problems; (4) rapidity with which innovations are made; (5) sophistication of the technology, and (6) educational level of workers active in the field. *Envt'l. Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 696-697 (Fed. Cir. 1983) (citing *Orthopedic Equip. Co. v. All Orthopedic Appliances, Inc.*, 707 F.2d 1376, 1381-82 (Fed. Cir. 1983)). Not all such factors may be present in every case, and one or more of these or other actors may predominate in a particular case. *Id.* Moreover, these factors are not exhaustive but are merely a guide to determining the level of ordinary skill in the art. *Daiichi Sankyo Co. Ltd, Inc. v. Apotex, Inc.*, 501 F.3d 1254, 1256 (Fed. Cir. 2007).

In determining a level of ordinary skill, we also may look to the prior art, which may reflect an appropriate skill level. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). Additionally, the Supreme Court informs us that

"[a] person of ordinary skill is also a person of ordinary creativity, not an automaton." *KSR*, 550 U.S. at 421.

Petitioner proposes that a person of ordinary skill in the art at the time of the '039 patent "would have had at least an undergraduate degree in electrical engineering, or equivalent education, and at least two years of work experience in the field of security and access-control." Pet. 8 (citing Ex. 1006 ¶ 26).

Patent Owner offers the level of ordinary skill we adopted in IPR2022-00600, which is that a person of ordinary skill in the art at the time of the '039 Patent

> would have had at least a bachelor's degree in computer engineering, computer science, electrical engineering, or a related field, with at least one year of experience in the field of human-machine interfaces and device access security. Additional education or experience might substitute for the above requirements.

PO Resp. 6-7; *see also* IPR2022-00600, Paper 22 at 12 (PTAB October 13, 2023) (Final Written Decision).

In this proceeding, Patent Owner's and Petitioner's levels of ordinary skill in the art, in particular education, are not substantively different. Petitioner's proposal requires at least two years of experience in the field of security and access control, compared to one year as proposed by Patent Owner. We maintain our determination of the level of ordinary skill in the art from

IPR2022-00600, including at least one year of experience as Patent Owner urges. On this record, Patent Owner's proposed level of ordinary skill in the art is consistent with our review and understanding of the technology and descriptions in the '039 patent and the asserted prior art references. *See Okajima*, 261 F.3d at 1355. Indeed, the difference between one and two years of experience in the field is fairly minimal considering that neither party asserts that it is necessary to have a significant amount of experience, e.g., 5-10 years in the field. For consistency, we rely on the same level of ordinary skill in the art that we determined in IPR2022-00600.

C. Claim Construction

We interpret 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)." 37 C.F.R. § 42.100(b) (2020). Under this standard, we construe 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." *Id.* Furthermore, we expressly construe the claims only to the extent necessary to determine whether to institute *inter partes* review. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) ("[W]e 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))).

Appendix E

1. "if the provided card information has not been previously provided to the verification station . . . storing the imputed biometric signature"

Patent Owner argues that the independent claims challenged here, for example limitations 3[D](P)+[D](1)], are specifically directed to an enrollment process, although the word "enrolling" or "enrollment," is not recited expressly in the claims. PO Resp. 7 (citing Ex. 2039 ¶ 39). Patent Owner argues that a person of ordinary skill in the art "would understand this to be an enrollment process because the user's card information has not previously been entered into the system and the user's biometric data has not previously been stored in the system's memory. *Id.*

Petitioner does not address whether the claims encompass an enrollment process. *See*, *generally*, Pet.

Because at least Hsu, Sanford, and Tsukamura each discloses an enrollment process, in this case we need not explicitly determine whether the language from which Patent Owner argues infers "enrollment" in claim 3 is limiting. We can agree that from reading the '039 patent in context there is a difference between verification process 205 and enrollment process 207. As we explained in our Institution Decision

> the enrollment process includes step 401, which *stores* the biometric signature "at a memory address defined by the card data 604," whereas

> in verification process 205 "step 204 *reads* the contents stored at a single memory address defined by the card data 604" and compares the stored biometric signature with the input biometric signature.

Inst. Dec. 7 (citing Ex. 1001, 9:65-66, 8:24-26). The language of the independent claims and the requirement that where the card information has *not* been previously provided, "storing the inputted biometric signature," tracks with the specification description of an enrollment phase. *See* Ex. 1001, 9:63-65 ("The [enrollment] process 207 is entered from the step 206 in FIG. 5, after which a step 401 stores the biometric signature received by the step 203 in the memory 124."). Therefore, for purposes of this Decision, we will consider the limitations of claims 3, 15, and 18 to include, at least in part, an enrollment process. However, because the terms "enrolling" or "enrollment" do not create any particular dispute between the parties that we need to resolve, we need not determine whether they are, in fact limitations.

2. "a memory location defined by the provided card information"

Claim limitation 3[D](1) recites the step of "storing the inputted biometric signature in a memory *at a memory location defined by the provided card information*." Ex. 1001, 12:61-63 (emphasis added). Patent Owner argues that "the proper construction of [this] claim term is: 'the system sets or establishes a memory location in a memory, said location being contingent upon or determined by the

provided card information.'" PO Resp. 8. Patent Owner also argues that a person of ordinary skill in the art "would interpret the word 'defined,' especially in the context of enrollment, to mean 'setting' or 'establishing.'" *Id.*

Petitioner proposes alternative constructions. Petitioner first proposes that "defining" means that "a memory location is somehow determined from (or is dependent on) the card information." Pet. 9. Petitioner alternatively proposes that "defining" means "a memory location is specified by the card information itself." *Id.* Petitioner contends that the second construction is most consistent with the specification of the '039 patent specification. *Id.* According to Petitioner, and considering that the '039 describes "a biometric card pointer system," a person of ordinary skill in the art "would have understood that the user's card information itself specifies the physical memory address (such as by acting as a pointer) for the user's biometric signature." *Id.* at 11 (citing Ex. 1006 ¶ 47).

Consistent with our prior decision in IPR2022-00600 and our concurrent decision in IPR2022-01093, we determine also in this proceeding that Patent Owner's construction is sufficiently accurate.[11] *See Apple, Inc. v.*

---

11. Different from independent claim 1 addressed in IPR2022-01093 and IPR2022-00600, independent claim 3, and specifically limitation 3[D(1)], does not recite "defining, *dependent* upon the received card information," but "defined by the provided card information." *Compare* Ex. 1001, 12:33, *with id.* at 12:63-64. Limitation 3[E(2)] does additionally recite "performing the process *dependent upon* the received card information." For purposes of claim construction, we do not find the claim language as to these

CPC Patent Technologies, Ltd., IPR2022-00600, Paper 22, 29-39 (Final Written Decision); *see also NTP Inc., v. Research in Motion, Ltd.*, 418 F.3d 1282, 1293 (Fed. Cir. 2005) (noting that, when construing claims in patents that derive from the same parent application and share common terms, "we must interpret the claims consistently across all asserted patents"). In our Final Written Decision in IPR2033-00600, we explained that

> [c]onsidering the abstract and the specification of the '039 patent, what "defining, dependent upon . . . " means as a whole, in the context of claim 1 and "a method of enrolling," is that during an *enrollment* process, the claimed "biometric signature," e.g., a fingerprint, is not yet stored in the memory and no memory location or address has been "set" or "established" for the fingerprint. When the fingerprint, and then the card, is provided to the system during enrollment, the card information provides data that establishes *where, e.g.*, at what memory location or address, the system will *store* the fingerprint data.[12]

IPR2022-00600, Paper 22, 30. We also explained that "[i]mportantly . . . we do not understand that 'defining

---

limitations between claims 1 and 3 to be substantively different in scope or meaning nor does either party argue that they are.

12. We use the terms "memory location" and "memory address" interchangeably because, in terms of computer memory, an "address" is well-understood as "[a] number specifying a location in memory where data is stored." MICROSOFT COMPUTER DICTIONARY, 5th Ed. (2002) Microsoft Press.

. . . a memory location,' or Patent Owner's alternative wording, 'establishing' or 'setting,' means '[*creating*] . . . a memory location in a local memory.'" *Id.* at 32. We explained further that "[w]hile we might agree that 'the memory location cannot [already be defined],' . . . we do not agree that it 'cannot already exist.'" *Id.* at 33. During the oral hearing in this proceeding, Patent Owner's counsel argued that "Patent Owner in this case has not argued that defining means creating." Tr. 31:3-4. Patent Owner's counsel argued further, "[a]ll we're saying that Claim 1 requires is that when a user swipes their card, that is the information that is on the card, not – in that moment in time, not something else in the system, but the information on the card that directs the system where to store that particular user's fingerprint or other biometric data."[13] *Id.* at 31:7-11.

Considering Patent Owner's arguments and asserted claim construction with respect to the phrase "memory location defined by the provided card information" and limitation 3[D](1) as a whole, we maintain the claim construction given in IPR2022-00600 for the reasons provided here and in the Final Written Decision in that proceeding. IPR2022-00600, Paper 22, 29-36.

We understand that, during an enrollment process, the claimed "biometric signature," e.g., a fingerprint, is not yet stored in the memory, and no memory location or address has been "defined," as in "set" or "established,"

13. We understand in the context of this proceeding that Patent Owner's counsel's argument would apply to independent claims 3, 15, and 18 as well as claim 1.

in the memory for storing the fingerprint, until card information is received. Once the card information and fingerprint are received during enrollment, the card information provides data that establishes *where*, i.e., at what memory location or address, the system will *store* the fingerprint data. The memory location or address where the fingerprint data is stored is, therefore, "contingent" on the card information, as Patent Owner's construction requires.

3. Other claim terms agreed upon and construed by the District Court

Petitioner indicates that the following terms have been previously agreed to between Apple and Patent Owner:

> "*dependent upon*" – Plain and ordinary meaning, defined as "contingent on or determined by"
>
> "*biometric signature*" – Plain and ordinary meaning.

Pet. 12 (citing Ex. 1013, 2). Patent Owner does not specifically address these terms in its Patent Owner Response.

Considering these constructions and that our analysis does not turn on any particular claim construction for these terms, and because these constructions are not in dispute, we need not determine any specific claim construction for these terms in this proceeding.

4. Means-plus-function terms

In our Institution Decision we accepted Petitioner's proposed constructions for the several "means for" and "code for" limitations recited in claims 15 and 18. *See* Inst. Dec. 42 (The Board explaining that "we find Petitioner's proposed constructions of these term under 35 U.S.C. § 112(6) consistent with the record in this case."). These constructions are also consistent with the District Court proceeding. Inst. Dec. 39-43; *see also* Ex. 1012, 1-4. Patent Owner does not address the means-plus-function terms in the challenged claims.

Because patentability on the claims at issue in this case does not turn on construction of the relative structures and functions of these means-plus-function terms, and because they are not in dispute, we maintain the constructions from our Institution Decision including that "code for" is an equivalent recitation for "means for." Inst. Dec. 39-43.

D. Ground 1: Claims 3, 4, 6-11, 15, 16, and 18 – Obviousness over Sanford (Ex. 1004) and Hsu (Ex. 1003)

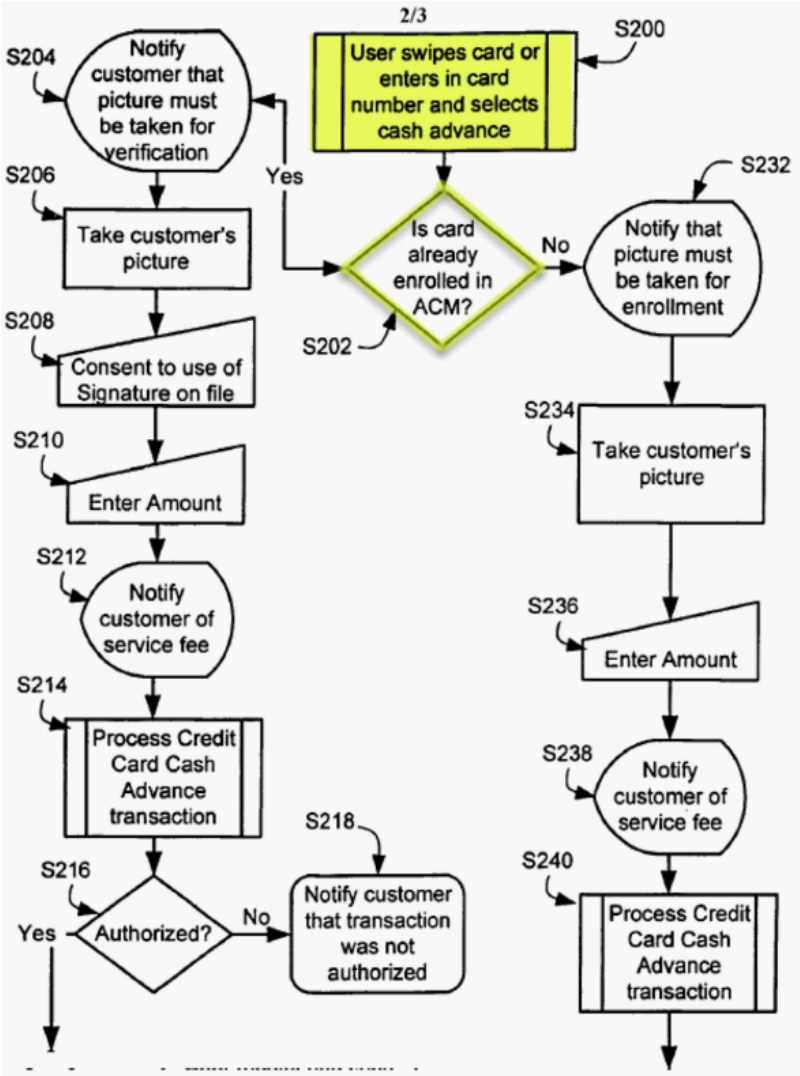
For the reasons below, and on the complete record before us, Petitioner has shown by a preponderance of the evidence that claims 3, 4, 6-11, 15, 16, and 18 would have been obvious over Sanford and Hsu.

Appendix E

1. Sanford (Ex. 1004)

Sanford is titled "Credit Card Transaction without using a Pin with Automated Cashier Machine" and describes "[a]n automated cashier machine (ACM) is provided that offers a secure and convenient way for users to access cash from their card without using a PIN." Ex. 1004, Abstract, codes (54), (57). Sanford describes that "[b]y verifying a user's image using facial biometrics, transactions may be conducted without using a pin." *Id.* ¶ 7. Sanford explains further that "[o]ther methods of verification known in the art may also be used, such as iris, voice signature, and fingerprint technology." *Id.* ¶ 20. The relevant part of Sanford's Figure 2, as annotated by the Board, is reproduced below.

Appendix E



Sanford's figure 2 is a block diagram illustrating a method for performing a PIN-less credit card transaction

using an ACM (automated cashier machine). *Id.* ¶ 24. After swiping a user's card at step 200, the system determines whether the user's card information is already stored, i.e. enrolled, and "the ACM 12 determines if the credit card account number of the user is enrolled to use the PIN-less credit card system." *Id.* In determining if the user is enrolled, "ACM 12 may communicate with ACM computer system 18 to look up the user's credit card number." *Id.* ¶ 25. At step 202, highlighted yellow above, ACM 12 determines an enrollment course of action; if the card is not enrolled, moving to step 232, or, if the card is already enrolled, conducting a verification course of action via step 204. *Id.*

2. Hsu (Ex. 1003)

Titled "Controlled Access to Doors and Machines Using Fingerprint Matching," Hsu describes "[a] system and related method for controlling access to building doors or to machines, such as automatic teller machines (ATMs)." Ex. 1003, Abstract, codes (54), (57). Hsu describes using "an account number or employee number, to access a fingerprint database (44) and retrieve reference fingerprint data previously stored there during an enrollment procedure." *Id.*, Abstract. Figure 3 from Hsu is reproduced below.

Appendix E

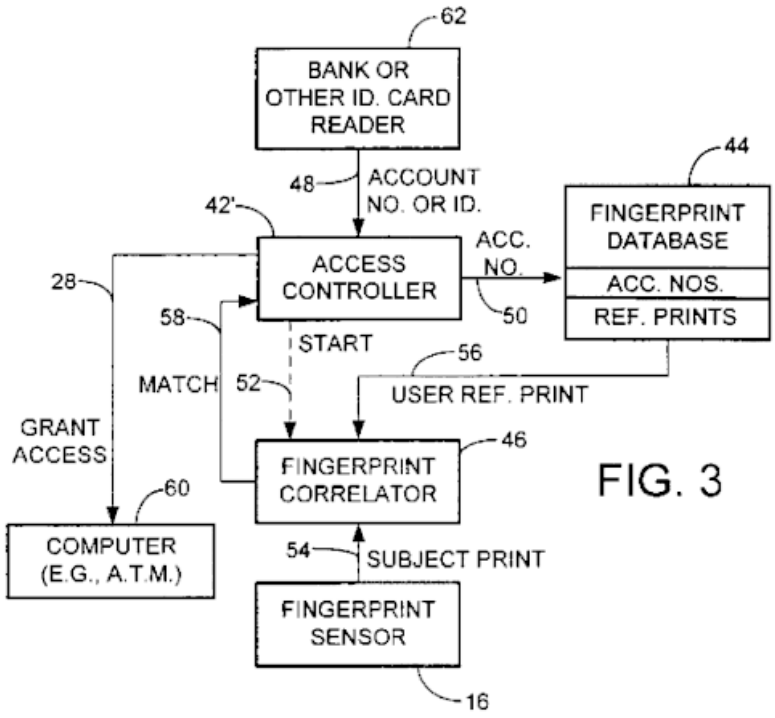


FIG. 3

Hsu's Figure 3 is a block diagram illustrating card reader 62 reading "an account number or other type of identification unique to the user, and passes this data to the access controller 42' over line 48." *Id.* at 6:10-12. Based on the user's unique identification access controller 42' communicates with finger print database 44 "to access the fingerprint database 44 and obtain a user reference fingerprint on line 56 from the database." *Id.* at 6:14-16. Hsu explains that

> [t]he controller 42' also sends a "start" signal on line 58 to the fingerprint correlator 46,

> which compares the reference fingerprint with a subject fingerprint image supplied from the sensor 16 over line 54. If the correlator 46 finds a match, the correlator sends a signal over line 58 to the access controller 42', which transmits an appropriate signal to the computer 60 on line 28, indicating that access has been granted.

Id. at 6:16-24.

Hsu also describes an enrollment process shown in Figure 4 and reproduced below.

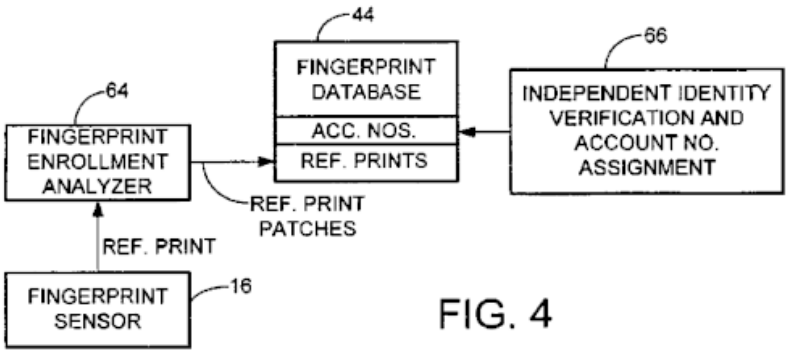


FIG. 4

Hsu's Figure 4 illustrates a block diagram showing that a user's fingerprint is obtained by fingerprint sensor 16 and passes through fingerprint enrollment analyzer 64 before being stored in fingerprint database 44. *Id.* at 7:51-8:23. Hsu explains that along with providing a fingerprint during enrollment, "[a]t the same time, the user's identity has to be independently verified, by some means other than fingerprint matching, as indicated in block 66, and the

user also presents an account number, employee number or similar identity number." *Id.*

3. Independent claim 3

We consider initially the elements of independent claim 3.

a) Petitioner's Arguments

(1) 3[P] – "A method of securing a process at a verification station"

Petitioner argues that Sanford discloses a "method of securing a process at a verification station" because Sanford teaches that a user needs to be verified at an ATM, e.g., Sanford's ACM (automated cashier machine). Pet. 13 (citing 1006 ¶¶ 268-272). Specifically, Sanford discloses a secure and easy way for a user to access cash using a picture, i.e., facial recognition, and without having to use a PIN. *Id.* (citing Ex. 1006 ¶ 269).

Sanford illustrates an exemplary verification system in Figure 1, reproduced below, as annotated by Petitioner (*id.* at 14).

Appendix E

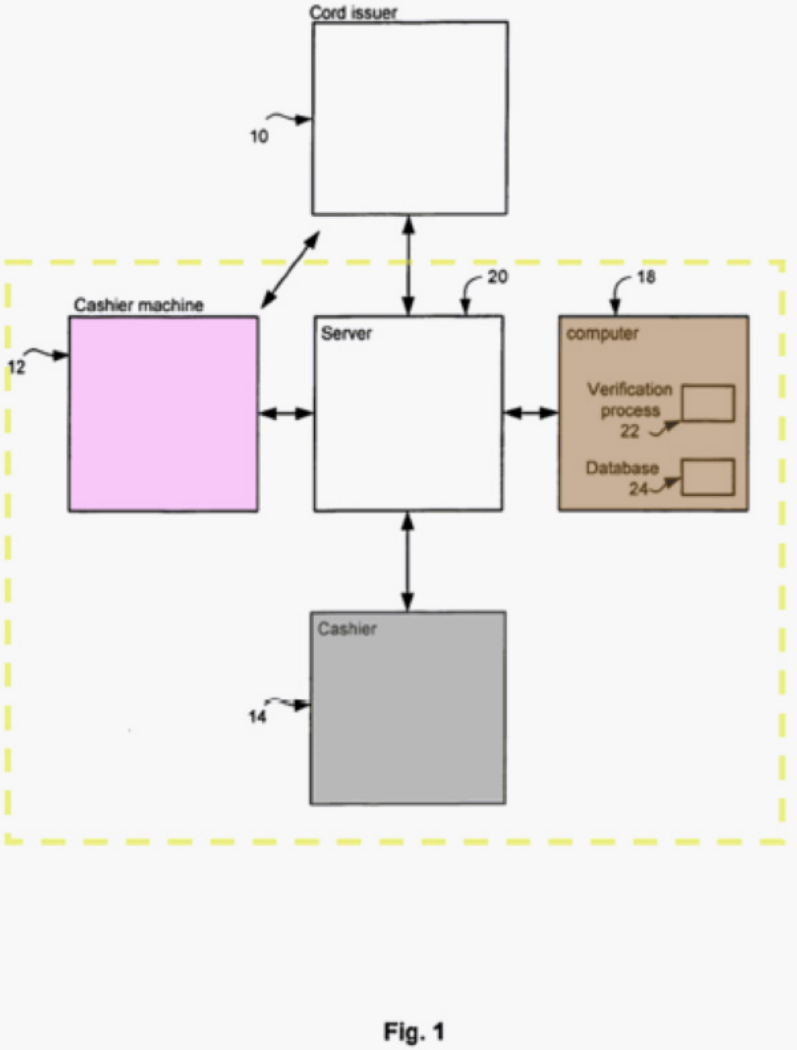


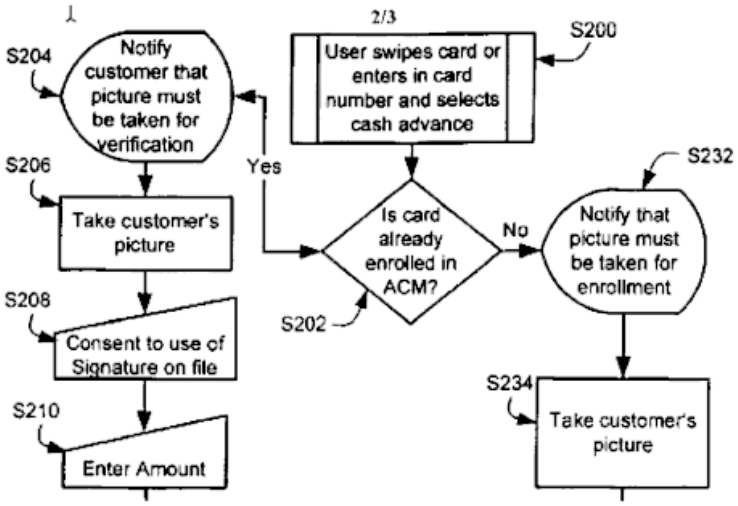
Figure 1 of Sanford illustrates verification system 10 including cashier machine 12 "capable of taking a picture of a person, and dispensing money" and server

20 "capable of receiving and forwarding communications to and from components of system 10." Ex. 1004 ¶¶ 16-17. Sanford explains that "[v]erification process 22 also may query database 24 to validate a user's credit card number associated with the picture to a card number associated with the user's picture in the database. Additionally, verification process 22 may query database 24 to verify other aspects of identifying information in the profile." *Id.* ¶ 21.

(2) 3[A] – "(a) providing card information from a card device to a card reader in the verification station;"

For limitation 3(a), Petitioner argues that Sanford's Figure 2 and step 200 disclose swiping or inserting a card in a card reader. Pet. 17-18 (citing Ex. 1004 ¶ 24, Fig. 2). According to Petitioner, Sanford teaches a process including providing *information* from a card to a card reader at a verification station, e.g., Sanford's ACM 12. *Id.* at 17. An excerpt from Sanford's Figure 2 is reproduced below.

Appendix E



Sanford's Figure 2 illustrates step 200 (S200) for swiping or entering a card number at a verification station, and step 202 (S202) determines whether the card is already enrolled.

(3) 3[B] – "(b) inputting a biometric signature of a user of the card device to a biometric reader in the verification station"

Petitioner argues that Sanford's Figure 2, step 234, which states "[t]ake customer's picture," teaches inputting a biometric signature, in the form of a user's picture, to a biometric reader in the ACM verification system. Pet. 18-19 (citing Ex. 1004 ¶ 16). Mr. Lipoff testifies that a person of ordinary skill in the art "would have understood that if a fingerprint biometric were used in Sanford's system,

then the picture taking device would be replaced with a fingerprint reader." Ex. 1006 ¶ 279.

(4) 3[C] – "(c) determining if the provided card information has been previously provided to the verification station;"

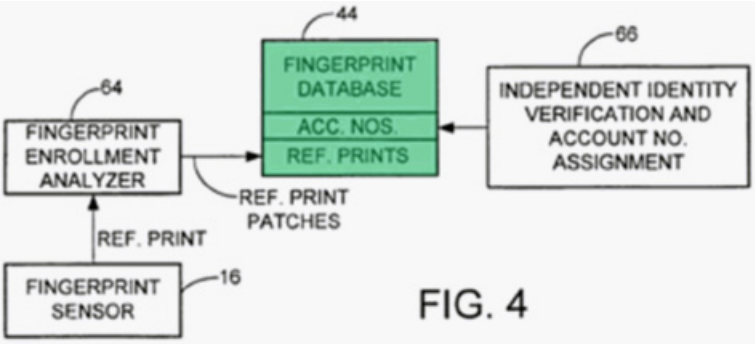
Petitioner contends that Sanford teaches this limitation because at step 202, as shown in Figure 2, Sanford determines whether the card is enrolled, i.e., stored in memory. Pet. 21 (citing Ex. 1004, Fig. 2, step 202; Ex. 1006 ¶¶ 282-285). Mr. Lipoff testifies that a person of ordinary skill in the art would have understood that this "means determining if the card has been previously enrolled, which Sanford discloses," because "after a user provides the credit card account number at step S200 (blue), 'ACM 12 determines [at step S202 (yellow)] if the credit card account number of the user is enrolled to use the PIN-less credit card system.'" Ex. 1006 ¶ 283 (quoting Ex. 1004 ¶¶ 24-25).

(5) 3[D(P)+D(1)+D(2)] – "(d) if the provided card information has not been previously provided to the verification station; (da) storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and (db) performing the process dependent upon the received card information;"

Petitioner argues that Sanford checks to see if card information has, or has *not*, been provided, i.e., enrolled, as outlined in Figure 2, step 202; if the card has *not* been enrolled, Sanford then stores the user's picture or, for example, other biometric data, such as a fingerprint. Pet. 23-24 (citing Ex. 1004 ¶ 25). Petitioner explains, however, that "Sanford does not provide specific details about how the user's picture or fingerprint is stored in the database." *Id.* at 27 (citing Ex. 1004 ¶¶ 21, 18). Petitioner argues that Hsu discloses a database that creates an association between a biometric fingerprint and a user employee number or account number. Pet. 33 (citing Ex. 1003 ¶¶ 26, 20). Mr. Lipoff testifies that a person of ordinary skill in the art "would have known that Sanford's database could be setup like that disclosed in Hsu to store Sanford's credit card numbers and associated pictures/fingerprints . . . such that given a user's credit card number, Sanford's ACM could locate the customer's picture/fingerprint data at the associated memory location." Ex. 1006 ¶ 292. Mr. Lipoff testifies further that a person of ordinary skill

in the art "would have understood that the biometric signature (*e.g.*, fingerprint) in the Sanford-Hsu system is not stored at *any* memory location in the database – rather, it is stored at *the* memory location associated with the corresponding credit card number (Hsu's user/account/employee number) received from a card." *Id.* ¶ 293 (citing Ex. 1003 ¶¶ 26, 20). Given the knowledge of a person of ordinary skill in the art regarding how a database and tables relate stored information, Petitioner argues that "the 'memory location' for storing the biometric signature (*e.g.*, fingerprint) the Sanford-Hsu system is 'defined by the provided card information.'" Pet. 28 (citing Ex. 1006 ¶ 293).

Petitioner points out that Hsu's Figure 4, as shown below and annotated by Petitioner (*id.* at 72), depicts memory and storage 44 where an account number is stored in the database associated with a fingerprint. *Id.*



Hsu's Figure 4 is a block diagram illustrating storage 44 (highlighted green) including "fingerprint database," "Acc[ount] Nos.," and "Ref. Prints." Ex. 1003, 6:51-58.

(6) 3[E(P)+E(1)] – "(e) if the provided card information has been previously provided to the verification station; (ea) comparing the inputted biometric information to the biometric signature stored in the memory at the memory location defined by the provided card information"

In line with its analysis of the above limitations, Petitioner contends that Sanford discloses checking if the card information has or has not been provided, i.e., enrolled, and if it has been, then the verification process can compare the picture or fingerprint stored in the manner of Hsu's database; for example, with a user's provided picture or fingerprint. Pet. 31 (citing Ex. 1006 ¶¶ 300-302). In this case, in which Sanford discloses that a user is enrolled, Mr. Lipoff testifies that "[t]he 'verification process 22 may employ an algorithm based on facial biometrics' and compares the inputted image to a stored picture/fingerprint." Ex. 1006 ¶ 301 (quoting Ex. 1004 ¶ 19).

(7) 3[E(2)] – "(eb) if the biometric signature matches the stored biometric signature, performing the process dependent upon the received card information"

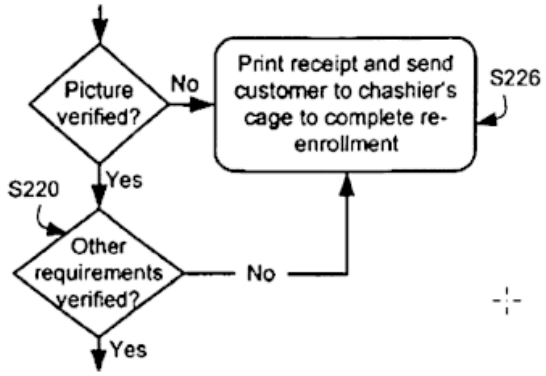
Petitioner argues that Sanford teaches this limitation because Sanford verifies the user, for example, in Fig.

2, steps 204-220, which illustrate that a user's picture or other biometric signature, such as a fingerprint, is compared and verified, in the manner taught by Hsu's database for example, with a user's stored picture or fingerprint. Pet. 33. Mr. Lipoff testifies that after verification Sanford discloses "performing the process [*e.g.*, antecedent process from the preamble, here Sanford's cash dispensing] dependent upon the received card information [*e.g.*, Sanford's credit card account number]." Ex. 1006 ¶ 305. In other words, according to Petitioner and Mr. Lipoff, Sanford's process is carried out – that is dispensing cash – after successfully comparing the biometric signatures, and a badge or card account number, for example as described by Hsu, points to the location of the stored biometric signature for verification and comparison purposes.

(8) 3[E(3)] – "(ec) if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information."

According to Petitioner, Sanford teaches that if the biometric signature does not match a stored signature, then, as shown and described in Figure 2, step 226, the user is printed a receipt and instructed to re-enroll, and the system does not dispense cash to the user. Pet. 34-35 (citing Ex. 1004 ¶ 30). An excerpt from Sanford's Figure 2 is reproduced below.

Appendix E



Sanford's Figure 2 describes at step 226 (S226) that where a user's picture cannot be verified, "[p]rint receipt and send customer to c[]ashier's cage to complete re-enrollment."

(9) Analogous Art and Motivation to Combine Sanford and Hsu

Petitioner argues that Sanford and Hsu are analogous prior art with respect to the '039 patent. Pet. 37. Petitioner contends that "[b]oth references (and the '039 Patent) are directed to ways of performing efficient biometric authentication, including using fingerprints." *Id.* Petitioner argues that "[b]oth references (and the '039 Patent) teach authenticating a user by comparing a fingerprint captured by a sensor to a stored fingerprint." *Id.* (citing Ex. 1003, Abstract; Ex. 1004, Abstract).

We consider two criteria when evaluating whether prior art is analogous: (1) whether the art is from the same field of endeavor, regardless of the problem

addressed; and (2) if the reference is not within the field of the inventor's endeavor, whether the reference still is reasonably pertinent to the particular problem with which the inventor is involved. *In re Clay*, 966 F.2d 656, 658-59 (Fed. Cir. 1992).

The '039 patent is directed broadly to "security issues associated with use of card devices such as credit cards, smart cards, and wireless card-equivalents such as wireless transmitting fobs." Ex. 1001, 1:14-16. More specifically, the '039 patent explains that its disclosure addresses "problems relating to secure access and/or secure processes, by automatically storing a card user's biometric signature in a local memory in a verification station comprising a card reader, [and] a biometric signature reader." *Id.* at 2:53-57. Based on framework and disclosure, we determine that a reasonable field of endeavor involves enrollment and user verification systems including card devices and biometric signatures.

As Petitioner points out, both Sanford and Hsu expressly disclose enrollment and biometric user verification systems that compare a user fingerprint to a stored fingerprint for identity verification purposes. *See*, *e.g.*, Ex. 1003 ¶¶ 4, 13, 20, 24, Fig. 3; *see also* Ex. 1004 ¶¶ 4, 8-9, 16, 36. For example, Hsu explains that "FIG. 2 shows the principal components of the access control unit 14 in block diagram form, including an identification polling transceiver 40, a door controller 42, a fingerprint database 44, and a fingerprint correlator 46." *Id.* at ¶ 20. Similarly, Sanford describes that in "a secure and convenient way for users to access cash from their card without using a PIN

. . . [a]n identifying image of a user is taken and an amount for withdraw is received. If the amount for withdrawal is approved, the ACM verifies the identifying image of the user to an image of the user in a profile." Ex. 1004 ¶ 6. Also, Sanford states that "[o]ther methods of verification known in the art may also be used, such as iris, voice signature, and fingerprint technology." *Id.* ¶ 20.

On the complete record now before us, we are persuaded that Sanford and Hsu are analogous art to the '039 patent as they are directed to the same field of endeavor, which is—enrollment and user verification systems including card reading devices and biometric signatures.

With respect to motivation to combine, Petitioner argues that although Sanford does not expressly disclose "a specific memory structure with a memory location for storing a picture/fingerprint that is defined by card information[,] [t]his is disclosed by Hsu." Pet. 37. To this end, Petitioner argues that

> [b]oth references (and the '039 Patent) teach that the stored fingerprint is associated with a number provided by the user and/or the user's card. Sanford discloses a user's picture (or fingerprint) associated with a user's card number provided by a user. Hsu discloses that the stored fingerprint data is associated with a user number or account number provided by a user's card.

Id. (citing Ex 1003 ¶¶ 18-21, 26).

Appendix E

Petitioner's declarant, Mr. Lipoff, testifies that a person of ordinary skill in the art would have implemented Hsu's database 44 in Sanford's system because "Hsu discloses that '[t]he database is basically a table that associates each user number with a stored fingerprint image, or with selected distinctive attributes or features of the user's fingerprint image.'" Ex. 1006 ¶ 311 (quoting Ex. 1003 ¶ 20, Fig. 4). Mr. Lipoff reasons that combining the references "improve[s] the efficiency of a biometric authentication system by comparing a captured fingerprint with a single stored fingerprint in a one-to-one manner, instead of needing to compare against multiple stored fingerprints in a one-to-many manner." *Id.* ¶ 310.

On this record, we find persuasive Petitioner's explanations for a motivation to combine Sanford and Hsu. Hsu, as Mr. Lipoff testifies persuasively, describes specifically *how* a person of ordinary skill in the art would implement a database in a verification system to associate an account or credit card number with a stored biometric signature. *Id.* ¶¶ 281-294. In addition, Mr. Lipoff provides persuasive reasoning as to why a person of ordinary skill in the art would have looked to Hsu to "perform a database look-up to locate the user's biometric data, including picture/fingerprint and other data, at the specific memory location defined by the card/user number" *Id.* ¶ 313; *see also KSR*, 550 U.S. at 420 (explaining that "any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed").

b) Patent Owner's Arguments

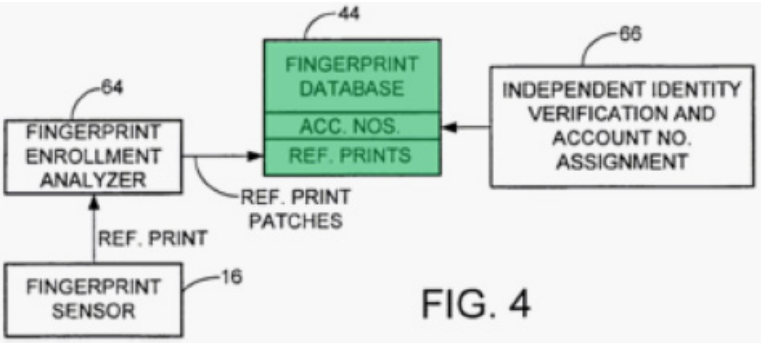
Patent Owner focuses its arguments on limitation 3[C(P)] and 3[C](1)], arguing that "Hsu is devoid of any teaching or suggestion that the user's card information sets or establishes (*i.e.*, defines) the memory location for the user's fingerprint data during enrollment." PO Resp. 11 (citing Ex. 2039 ¶ 46). According to Patent Owner, Hsu does not "set" or "establish" a memory location for the fingerprint data because Hsu mainly describes that "[t]he account number is stored in the database 44 in association with the user's fingerprint image data." *Id.* at 12 (quoting Ex. 1003, 7:1-12). Patent Owner's position is that Hsu does not define any memory location in particular, but "that the user's fingerprint data and account number are presented *at the same time* and are then stored in the database *in association with* each other." *Id.* at 13 (citing Ex. 2039 ¶ 49). In other words, Patent Owner's argument is that, unlike the claimed method, Hsu's card information does not provide data that sets or establishes *where*, i.e., at what memory location or address, the system will *store* the fingerprint data.

c) Analysis

Hsu expressly describes an enrollment process for a user including fingerprint database 44 and describes that "the fingerprint database 44 contains reference fingerprint image data for each user, employee, or customer using the system, and that the reference fingerprint data are associated with corresponding user numbers, or employee or customer account numbers." Ex. 1003 ¶ 26. Hsu's

Appendix E

Figure 4, illustrating the enrollment process, as annotated by Petitioner (Pet. 72), is reproduced below.



Hsu's Figure 4 is a block diagram showing an enrollment process illustrating fingerprint database 44 (highlighted green) including reference prints and related account number for each user or employee. Ex. 1003 ¶ 26.

Based on the description and Figure 4, Hsu tells us a location, that is *where*, i.e., in fingerprint database 44, the fingerprint is to be stored during enrollment. Hsu explains that in the fingerprint database 44 "fingerprint data are associated with corresponding user numbers, or employee or customer account numbers." *Id.* Accordingly, we understand from this description that the user's fingerprint is stored in relation to, i.e., "associated with," the user's employee account number, for example. Still, a key question is *how* is the fingerprint data stored during enrollment. Consistent with our claim construction, the card information must "set" or "establish" where the fingerprint data is to be stored—that is, the location must be "*contingent upon or determined by* the user's

account number itself during enrollment." *See supra*, Section II.C.2. Petitioner relies on Hsu for this teaching. Pet. 28-32. Hsu explains that when a user presents a fingerprint during enrollment "[a]t the same time, the user's identity has to be independently verified, by some means other than fingerprint matching, as indicated in block 66, and the user also presents an account number, employee number or similar identity number." Ex. 1003, 7:4-8. In this way, Hsu describes presenting identification data apart from biometric data, and includes presenting, for example, an employee identification card or badge, including the user's employee number. *See* Ex. 1003 ¶ 11 (describing that "the identification medium carried by each user includes a machine-readable card, and the step of reading data from an identification medium includes reading data from a card reader in which the machine-readable card is placed by the user"). Understanding that during enrollment Hsu stores the user's fingerprint data "associated with" a user's employee number on the card, we further understand that the identification information, e.g., employee number, on the identification card defines, sets, or establishes, *where* the fingerprint is stored; that is—the user's fingerprint data is stored with the database record corresponding to the relevant employee number.

Given this, we conclude that Patent Owner's position that Hsu does not disclose a memory location "defined by," "set," or "established" by card information is not accurate. *See* PO Resp. 12 (arguing that "[t]here is definitively no teaching or suggestion that the user's account number (or similar identity number) sets or establishes the memory location for the fingerprint data

during enrollment") (citing Ex. 2039 ¶ 48). Patent Owner's argument mainly contrasts the term "associated with," as described in Hsu, with our claim construction that "defined by" means "set" or "established." *Id.* We agree that these are different words, but an ordinary meaning of "associated" is "related, connected, or combined together." MERRIAM WEBSTER ONLINE DICTIONARY, https://www.merriam-webster.com/dictionary/associated (last visited Jan. 9, 2024) (Ex. 3001). Considering common database structures and functions, we are persuaded that Hsu, by "associating" a user's fingerprint data with a database record corresponding to a particular employee, concomitantly discloses "defining," "setting," or "establishing" a memory location for the fingerprint data in relation to the employee account number. Consistent with our understanding of Hsu's disclosure, Mr. Lipoff testifies persuasively that in Hsu "[t]he 'fingerprint image, or [] selected distinctive attributes or features of the user's fingerprint image' are not stored at *any* memory location in the database—rather, it is stored at a memory location associated with the specific user/employee number received from a card." Ex. 1006 ¶ 93 (citing Ex. 1003 ¶ 26).

Patent Owner's counsel made clear, during oral argument, its position that "there's no discussion at all in Hsu that the ID number/card information in enrollment for purposes of storing the signature, stores [fingerprint data] at a specified location—by location specifically specified by the card data." Tr. 42:21-23. But we do not agree with this position. As discussed above, Hsu describes that fingerprint data is stored associated with the card data, e.g., an account or employee number. Ex.

1003 ¶ 26 (describing that "the reference fingerprint data are associated with corresponding user numbers, or employee or customer account numbers"). Consistent with our claim construction, the "association" is the *where*. In other words, we understand that Hsu's associating the fingerprint data with the personal data record in fingerprint database 44 defines, sets, or establishes where the fingerprint data is stored. This occurs, as Hsu explains, because during enrollment the user data such as account or employee number is supplied by the user's card. *See id.* (explaining that during enrollment, in addition to a fingerprint image, "the user also presents an account number, employee number or similar identity number"). We do not consider it a significant leap, or even a leap at all, to understand that associating the fingerprint data according to, that is—"contingent on, or determined by," the user's account number or employee number on Hsu's card or badge, sets or establishes the database record or address location *where* the fingerprint data is stored in Hsu's fingerprint database 44.

Patent Owner also argues that "[i]n contrast to the claimed method, Hsu teaches that the user's fingerprint data and account number are presented *at the same time* and are then stored in the database *in association with* each other." PO Resp. 13 (citing Ex. 2039 ¶ 49). Patent Owner's declarant, Dr. Russ, similarly testifies that "in Hsu, the fingerprint data and the account number are presented together and are then stored together . . . [t]here is no step in Hsu wherein the account number (or the 'card information') first sets or establishes the memory location." Ex. 2039 ¶ 49. This argument takes advantage

of the fact that Hsu does explicitly state a temporal order for "storing . . . the biometric signature" as recited in claim 1. However, as we explained in our claim construction,

> during an enrollment process the claimed "biometric signature," e.g., a fingerprint, is not yet stored in the memory, and no memory location or address has been "defined," as in "set" or "established," in the memory for storing the fingerprint, until card information is received. Once the card information and fingerprint is received during enrollment, the card information provides data that establishes *where*, i.e., at what memory location or address, the system will *store* the fingerprint data.

Section II.C.2. Similarly, in Hsu, the fingerprint data can only be stored once the system has received data indicative of, for instance, an employee number from a user's identification badge, which thus defines a database record with which the fingerprint data can be "associated."

This all makes sense, logically, because Hsu's fingerprint data are not randomly stored, as Mr. Lipoff explains, "in *any* memory location." Ex. 1006 ¶ 93. Hsu's fingerprint data cannot be stored until directed to, i.e. "associated with," a certain database address or record, and in Hsu that is a database record containing the user's identification information. *See* Ex. 1003, 7:7-12 (describing that during enrollment "the user also presents an account number, employee number or similar identity number . . . [t]he account number is stored in the database

44 in association with the user's fingerprint image data"). Accordingly, from a temporal standpoint during enrollment, Hsu must also use card information, e.g., an employee number, to define, set, or establish a memory location with which the fingerprint data can be associated, before storing the fingerprint data. Commensurate with our understanding of Hsu's disclosure, we credit Mr. Lipoff's testimony that even though Hsu does not explain exactly "how a new user record is created" during enrollment, a person of ordinary skill in the art would have "tr[ied] using simple known options for creating database records." Ex. 1032 ¶ 32. Mr. Lipoff explains persuasively that "upon a user enrolling, they provide a previously unseen card/user number, [and] the system then creates a new record for the user, including setting/establishing for the first time the memory location for storing the user's fingerprint." *Id.* ¶ 33.

When asked during his deposition to describe Hsu's database structure and functions, Mr. Lipoff testified consistently with his declaration, explaining essentially that it is the user's employee or account number that defines where the fingerprint data is stored:

> Q. So the account number indicates where the fingerprint is stored because they are stored in association with each other; is that correct?
>
> . . .
>
> A. THE WITNESS: Well, I think it's – it's more than that. The structure that the database,

> as Hsu describes it, I believe—let me see. I think it's in paragraph 20. Let me see if I can find it. Yeah, so in paragraph 20, column 4, the database is basically a table that associates each user number with a stored fingerprint image or selected attributes.
>
> So what this is telling me is the user number, which you—you said we should call the account number, I believe it's the same thing here, is—is a database, and so the user number is defining the memory location in which the stored fingerprint image will be stored because the structure of the database is one, as indicated here in column 4, that starts with the user number telling you where to find the memory location that has the stored fingerprint image.

Ex. 1041, 33:16-34:9. When Patent Owner's counsel pointed out that Hsu's paragraph 20 did not pertain specifically to enrollment, Mr. Lipoff explained that the database structure and function in paragraph 20 also applies to the enrollment process shown in Figure 4:

> A. Paragraph 20 describes the principle [sic] components of the access control unit, which includes the fingerprint database which is the same fingerprint database that's in – that's in – I'm sorry. Same fingerprint database that's in Figure 4. Figure 4 is the previous paragraph of Hsu we were discussing. Paragraph 26 is the enrollment procedure, but by the time you

> get to the enrollment procedure, Hsu, earlier in paragraph 20, defined the structure of that same database—database item 44 in Figure 4.

Id. at 34:19-35:9.

Summarizing its position, Patent Owner argues that "Hsu merely discloses that the user's account number and fingerprint data are stored in association with each other. Hsu offers no other teachings as to how the account number and fingerprint data are stored in the database." PO Resp. 15 (citing Ex. 2039 ¶¶ 53-54). Considering our analysis and the evidence discussed above, we disagree. We are persuaded that Hsu does, in fact, explain *how* the account number and fingerprint data are stored in the fingerprint database. Hsu establishes a memory location for storing the fingerprint data in "association" with an employee or account number, and the "association" is contingent on receiving the employee or account number from Hsu's card or badge during enrollment. *See* Ex 1003, 7:10-12, Fig. 4 (explaining that "[t]he account number is stored in the database 44 in association with the user's fingerprint image data").

Overall, we are persuaded based on Petitioner's arguments and evidence, including the testimony of Mr. Lipoff, that Hsu's association of a fingerprint with a user's underlying account or employee number in a database record during enrollment discloses limitation 3[D](1), namely "storing the inputted biometric signature in a memory at a memory location defined by the provided card information." Ex. 1001, 12:61-63.

Patent Owner does not present substantive arguments with respect to the remaining limitations 3[P]-[D] and 3[D](2)-[E](3), nor with respect to the combination of Sanford and Hsu. *See* PO Resp. 10-15. Having reviewed the entirety of the record now before us, specifically the disclosures in Hsu and Sanford, we accept Petitioner's arguments and evidence with respect to the remaining limitations as our own. Pet. 12-36. We also find that Petitioner and Mr. Lipoff have provided articulated reasoning with evidentiary underpinning as to why an ordinarily skilled artisan would have been motivated to combine the teachings of Sanford and Hsu. *Id.* at 37-39; Ex. 1006 ¶¶ 108-115.

d) Conclusion as to claim 3

Based on the complete record before us and for the reasons expressed above, we are persuaded that Petitioner has shown by a preponderance of evidence that claim 3 would have been obvious over Sanford and Hsu.

4. Dependent claim 4

Claim 4 depends from claim 3 and recites in part "wherein the card device is one of a card in which the card information is encoded in a magnetic strip;" or alternatively, "a smart card [or] . . . a key fob." Ex. 1001, 13:12-21.

Patent Owner does not provide separate, substantive arguments with respect to claim 4, but mainly argues that claim 4 "contain[s] the 'memory location defined by the

provided card information' limitation examined above." PO Resp. 24. Patent Owner then contends, "As the prior art cited by Petitioners does not teach this limitation, the cited prior art does not render these dependent claims obvious as a result thereof." *Id.*

Petitioner argues that "Sanford also discloses that this card information is encoded in a magnetic strip." Pet. 40 (citing Ex. 1004 ¶¶ 16, 40). Petitioner also argues that Hsu discloses each of the specific cards and key fobs recited in dependent claim 4. *Id.* at 40-41 (citing Ex. 1003 ¶¶ 7, 24). We find Petitioner's evidence persuasive; for example, Hsu describes that "[t]he card may be encoded with data using a magnetic stripe, bar codes, or any other means. Alternatively, the card may be a 'smart card' that includes an electronically readable memory." Ex. 1003, 6:5-9. For dependent claim 4 we have considered and on the complete record before us, in addition to our analysis above, accept as our own, Petitioner's arguments and evidence set forth at pages 40-41 of the Petition. Accordingly, we determine that Petitioner has shown by a preponderance of the evidence that claim 2 would have been obvious over Hsu and Sanford.

5. Dependent claim 6

Claim 6 also depends from claim 3 and recites "wherein the performance of the process in the steps (db) and (eb) comprises outputting at least part of the inputted card information from the verification station." Ex. 1001, 13:28-31.

Appendix E

Patent Owner does not provide substantive arguments with respect to claim 6, but mainly argues that claim 6 "contain[s] the 'memory location defined by the provided card information' limitation examined above." PO Resp. 24. Patent Owner then contends, "As the prior art cited by Petitioners does not teach this limitation, the cited prior art does not render these dependent claims obvious as a result thereof." *Id.*

Petitioner points, *inter alia*, to Sanford's disclosure in Figure 1 that illustrates the cashier machine 12 (verification station) communicating with a card issuer, the card issuer ostensibly being financial institution 16 described in Sanford's specification. Pet. 42-43. With respect to "outputting . . . card information," Mr. Lipoff testifies that a person of ordinary skill in the art "would have understood that when dispensing cash for a user, the user's credit card account number is sent to financial institution 16 (or at least doing so would be obvious)." Ex. 1006 ¶ 324. Mr. Lipoff explains, for example, considering Sanford's Figure 2 as annotated by Mr. Lipoff (Ex. 1003 ¶ 323) and reproduced below, that "if it is determined at step S202 (yellow) that a card is not enrolled, '[i]n step S240 [purple], the transaction is sent for pre-authorization to the financial institution . . . , which may use an Address Verification System (AVS) to help validate the users address.'" *Id.* ¶ 323 (quoting Ex. 1004 ¶ 34).

Appendix E

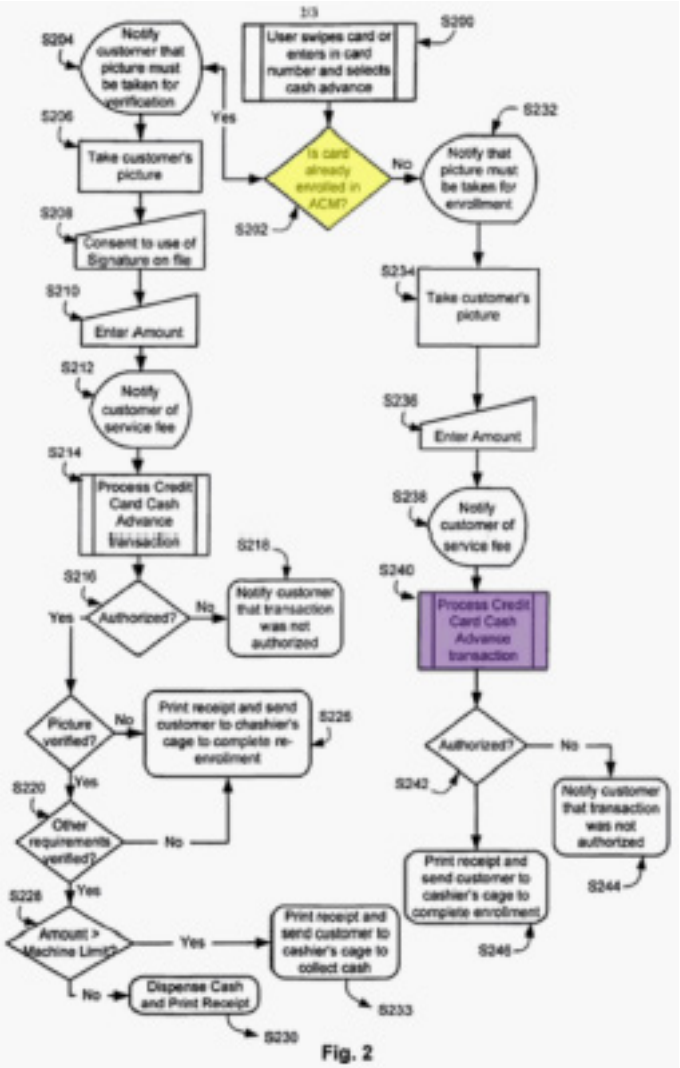


Figure 2 of Sanford illustrates a method for conducting PIN-less credit card transaction in a flow diagram. Ex.

1004 ¶ 24. Mr. Lipoff testifies further that a person of ordinary skill in the art "would have expected that the 'transaction' that is sent to the 'financial institution' would include the credit card account number." *Id.*

Mr. Lipoff's testimony as to claim 6 is unrebutted on this record. For dependent claim 6, we have considered and on the complete record before us, in addition to our analysis above, accept as our own, Petitioner's arguments and evidence set forth at pages 41-44 of the Petition. Accordingly, we determine that Petitioner has shown by a preponderance of the evidence that claim 6 would have been obvious over Hsu and Sanford.

6. Dependent claims 7-11

Claims 7-11 depend directly or indirectly from independent claim 3. Just as for claims 4 and 6, Patent Owner does not provide separate, substantive arguments with respect to dependent claims 7-11, but argues again that these dependent claims "contain the 'memory location defined by the provided card information' limitation examined above. As the prior art cited by Petitioners does not teach this limitation, the cited prior art does not render these dependent claims obvious as a result thereof." PO Resp. 24.

Mr. Lipoff's testimony as to dependent claims 7-11 is unrebutted on this record. For dependent claims 7-11, we have considered and on the complete record before us, in addition to our analysis above, accept as our own, Petitioner's arguments and evidence set forth at pages

44-54 of the Petition. Accordingly, we determine that Petitioner has shown by a preponderance of the evidence that claims 7-11 would have been obvious over Sanford and Hsu.

7. Claims 15-16 and 18

Independent claim 15 is an apparatus claim reciting "[a] verification station for securing a process," and includes similar limitations as independent claim 3. Ex. 1001, 14:22. Different from claim 3, claim 15 also recites "a card device reader," "a biometric signature reader," and for the remaining limitations recites "means for" along with the same functional language as in limitations 3[C]-[E].

Patent Owner does not provide separate, substantive arguments with respect to claims 15-16 and 18.

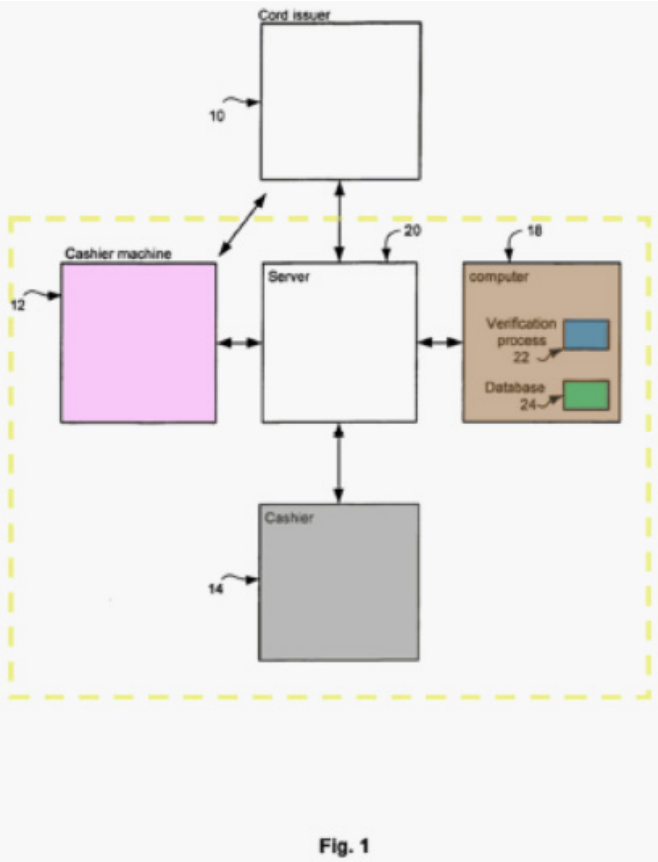
Petitioner argues that besides disclosing a verification station including a card reader, "Sanford discloses that its card reader is part of its ACM [automated cashier machine 12], and is therefore coupled to the ACM." Pet. 54 (citing Ex. 1004 ¶ 16). Petitioner equates Sanford's "picture taking device" with the claimed "biometric signature reader" arguing that "when the biometric signature is provided to the biometric signature reader, it is also provided to Sanford's ACM." *Id.* at 55 (citing Ex. 1006 ¶ 357).

Appendix E

Considering the "means for" limitations in the remainder of the claim, Petitioner points to the requisite function and structure in the prior art, which are consistent with our claim construction (*see supra* Section II.C.4; *see also* Inst. Dec. 39-43). For example, for limitation 15[C], Petitioner explains that the function of this limitation is "determining if the provided card information has been previously provided to the verification station." Pet. 56. According to Petitioner, the structure is, "processor unit 105 running software process(es) 206; and equivalents thereof." *Id.*

Petitioner argues that "as explained for Limitation 3[C], Sanford discloses the recited function." *Id.* (citing Ex. 1006 ¶ 282-285, 361). For the structure, and considering Sanford's Figure 1 reproduced below as annotated by Petitioner, Petitioner asserts that "Sanford discloses that ACM computer system 18 (brown), which is part of Sanford's ACM (yellow), 'includes a processor . . . [which] may be . . . a computer, workstation, mainframe, pocket PC, personal digital assistant, etc.'" *Id.* (quoting Ex. 1004 ¶ 18).

Appendix E



Sanford's Figure 1, as annotated by Petitioner (Pet. 64), illustrates ACM computer system 18 (brown), encompassing verification process 22 (blue) and database 24 (green). Ex. 1004 ¶ 18. Petitioner points out that Sanford expressly describes that "[t]he processor also preferably includes or is in communication with a verification process 22 [blue] and database 24 [green]. Verification process 22 may be a software-implemented

process that communicates with database 24." Pet. 57 (quoting Ex. 1006 ¶ 18).

Apart from its arguments with respect to independent claim 3[D](1), Patent Owner does not dispute Petitioner's evidence that Sanford, and Sanford in view of Hsu, disclose and teach the limitations of independent claim 15. *See generally* PO Resp. And, in addition to being persuaded that Sanford discloses the necessary structure and function intimated by "means for," we find that Sanford renders obvious limitation 15[C] for the same reasons as limitation 1[C]. Based on our review, we find that the complete record fully supports Petitioner's showing that the combination of Hsu and Sanford discloses all the limitations of independent claim 15. *See* Pet. 49-56.

Dependent claim 16 is similar to claim 4, and relates to a "verified access system" including, *inter alia*, "a reader for a card in which the card information is encoded in a magnetic strip." Ex. 1001, 14:51-52. Besides referencing his testimony with respect to claim 4, Mr. Lipoff testifies that similarly "Sanford discloses verification station with card reader and that its 'card reader may be a magnetic strip reader capable of reading cards with a magnetic strip such as, for example, ATM cards, credit cards, debit cards, or smart cards.'" Ex. 1006 ¶ 387 (quoting Ex. 1004 ¶ 16).

Independent claim 18 includes essentially the same limitations as claim 15, except that the preamble to claim 18 recites:

Appendix E

> A non-transitory computer readable medium having recorded thereon a computer program for directing a process or to execute a method for securing a process at a verification station, said program comprising:

Ex. 1001, 14:64-67. And, for example, the limitation of "means for determining if the provided card information has been previously provided to the verification station" in independent claim 15, is recited in independent claim 18 as "code for determining if card information, . . . has been previously provided to the verification station." *Compare id.* at 14:28-29, *with id.* at 15:1-4. Petitioner asserts that "[t]hese 'code for' terms should be construed the same way as 'means for' terms (*see* Section VII.B). Thus, for the same reasons discussed for claim 15, Sanford and Hsu disclose or render obvious claim 18." Pet. 65-66. Mr. Lipoff testifies that "[i]n order for the various components of Sanford and Hsu to perform their functions, a POSITA would have understood and found it obvious that both Sanford and Hsu (and the combined system) include one or more processors running computer programs stored on a non-transitory computer readable medium." Ex. 1006 ¶ 389.

Mr. Lipoff's testimony as to what a person of ordinary skill in the art would have understood in regards to the known internals, programming instructions, and memory structure for a biometric card enrollment and verification system is unrebutted on this record.

For independent claim 18, Petitioner's arguments and evidence are in all other respects the same as the arguments and evidence presented with respect to independent claim 15, as Petitioner and Mr. Lipoff specifically refer back to the respective arguments and evidence for the similar limitations in claim 15. Pet. 66.

We have considered, and on the complete record before us, accept as our own, Petitioner's arguments and evidence set forth at pages 54-66 of the Petition as to claims 15-16 and 18. Accordingly, we determine that Petitioner has shown by a preponderance of the evidence that claims 15-16 and 18 would have been obvious over Sanford and Hsu.

E. Ground 2: Claims 3, 4, 6-11, 15, 16, and 18 – Obviousness over Sanford, Hsu, and Tsukamura (Ex. 1005)

Because we determine that claims 3, 4, 6-11, 15, 16, and 18 would have been obvious over the combination of Sanford and Hsu, we need not address these same claims as obvious over the combination of Sanford, Hsu, and Tsukamura.

F. Ground 3: Claim 5 – Obviousness over Sanford, Hsu, and Leu (Ex. 1008)[14]

Dependent claim 5 recites:

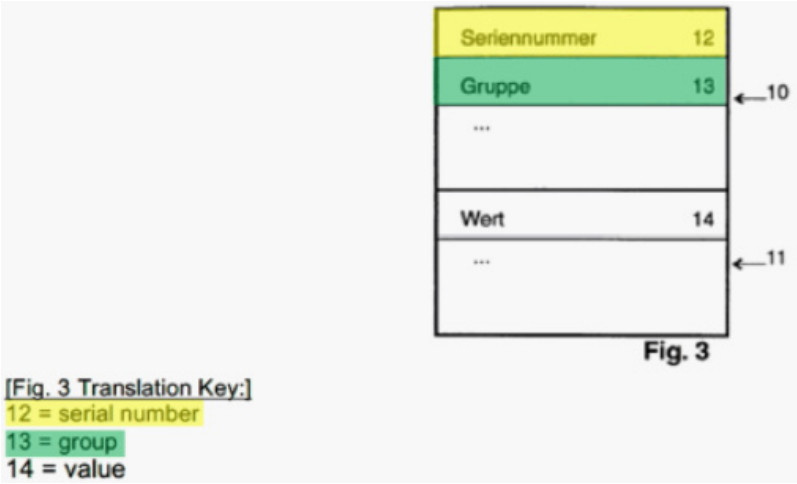
A method according to claim 3, wherein:

---

14. Ex. 1009 is the English translation of Ex. 1008.

> the card information provided in the step (a) comprises a header and card data; and
>
> the steps (c), (d) and (e) are only performed if the header indicates that the card belongs to a set of cards associated with the verification station.

Ex. 1001, 13:22-27. Petitioner argues that "Leu discloses a card reader device that reads a card and verifies the card information to determine whether an event (*e.g.*, indicating whether or not the user has achieved a lottery prize") can be triggered." Pet. 81 (citing Ex. 1009, 1:26-29; 1:20-27). Figure 3 of Leu, illustrating a card memory, is reproduced below including Petitioner's annotations (Pet. 82).



Leu's Figure 3 illustrates "the memory of the card" including a non-volatile memory divided into regions 10 and 11. Ex. 1009, 2:5. Leu explains that "[v]alues that can

no longer be changed after the card is sold are contained in the region 10, while the data in the region 11 can still be changed." Ex. 1009, 3:9-12.

Mr. Lipoff explains that Leu describes a serial number 12 (yellow) different for every card, and "[a] group memory 13 (green) 'indicates whether a card is a lottery ticket card or a conventional card.'" Ex. 1006 ¶ 423 (quoting Ex. 1009 3:20-22). Mr. Lipoff testifies that "since the group number and the serial number are stored on the card and are to be read by a card reader device . . . , they are both card information." *Id.* Mr. Lipoff testifies further that in Leu "the determination of whether a card user has won a lottery prize is only performed if the group number indicates that the card belongs to a first set of cards (*i.e.*, lottery cards) and not a second set of cards (*i.e.*, normal prepaid cards)." *Id.* ¶ 426. Thus, according to Mr. Lipoff, "because the card reader is able to interpret the first set of cards (lottery ticket cards) to determine whether a user has won a lottery prize, a POSITA would have understood the first set of cards (lottery ticket cards) are associated with the card reader (verification station)." *Id.*

Petitioner argues that a person of ordinary skill in the art would have combined Leu with Sanford because "Sanford, and Leu are **analogous art** and in the same field of using a card to make transactions. Sanford teaches using a credit card to withdraw cash and Leu teaches using a prepaid card to purchase telephone services." Pet. 86. Mr. Lipoff testifies that "Leu discloses that the disclosed prepaid cards use the same technology as 'credit cards,' which are disclosed in both the '039 Patent and

Sanford." Ex. 1006 ¶ 249 (citing Ex. 1009, 2:14-29; Ex. 1001, 1:14-16; Ex. 1004, Title). Mr. Lipoff testifies further, that a person of ordinary skill in the art

> implementing the Sanford-Hsu (or Sanford-Hsu-Tsukamura) system would have been motivated to perform a preliminary check to determine whether the card being read is a "valid" credit card (*e.g.*, can be interpreted by the card reader and is suitable for cash withdrawal) because, if the system cannot interpret the card or the card is not suitable for cash withdrawal, the system would never dispense money for a card user.

Id. ¶ 430.

Patent Owner does not provide separate, substantive arguments with respect to claim 5 or the motivation and reasons to combine Leu with Sanford and Hsu.

In this proceeding, for claim 5, Petitioner's arguments and Mr. Lipoff's testimony are unrebutted. We have considered, and on the complete record before us, accept as our own, Petitioner's arguments and evidence set forth at pages 80-87 of the Petition as to claim 5. Accordingly, we determine that Petitioner has shown by a preponderance of the evidence that claim 5 would have been obvious over Sanford, Hsu, and Leu.

G. Ground 5: Claim 12 – Obviousness over Sanford, Hsu and Houvener (Ex. 1009)

Dependent claim 12 recites:

A method according to claim 3, comprising the further steps of:

> (f) storing the card information provided by successive instances of the step (a); and
>
> (g) outputting the information stored in the step (f) for audit purposes.

Ex. 1001, 13:61-66. Petitioner argues that "Houvener discloses 'stor[ing] the users PIN and the data from the specific transaction as a transaction record.'" Pet. 88 (quoting Ex. 1010, 7:58-60). Petitioner argues that Houvener discloses an audit process where it is described that "if there is ever a question as to the voracity of the identification process, the system can recreate a transaction and identify not only the person initiating the transaction but the clerk who was responsible." *Id.* (quoting Ex. 1010, 7:60-65). Mr. Lipoff testifies that a person of ordinary skill in the art would have "understood that the stored transaction records in Houvener need to include sufficient information to allow the system to 'recreate a transaction' and 'identify . . . the person initiating the transaction.'" Ex. 1006 ¶ 438. Mr. Lipoff testifies that a person of ordinary skill in the art "who looked to further improve the Sanford-Hsu system would have understood that additional fraudulent actions may

be uncovered when considering a series of transactions and therefore look for teachings like Houvener." *Id.* ¶ 441. Including Houvener's specific transaction data storage and auditing capabilities would be considered, according to Mr. Lipoff, because a person of ordinary skill in the art "would have understood that Sanford discloses the well-known practices of logging card user activities, including card information and biometric information, for auditing purposes" to reduce credit card fraud. *Id.* ¶ 442 (citing Ex. 1004 ¶ 43).

Patent Owner does not provide separate, substantive arguments with respect to claim 12 or the motivation and reasons to combine Houvener with Sanford and Hsu.

In this proceeding, for claim 12, Petitioner's arguments and Mr. Lipoff's testimony are unrebutted. We have considered, and on the complete record before us, accept as our own, Petitioner's arguments and evidence set forth at pages 87-91 of the Petition as to claim 12. Accordingly, we determine that Petitioner has shown by a preponderance of the evidence that claim 12 would have been obvious over Sanford, Hsu, and Houvener.

H. Ground 7: Claim 17 – Obviousness over Sanford, Hsu, and McCalley (Ex. 1010)

Dependent claim 17 recites:

> A verification station according to claim 15, wherein the memory is incorporated in a tamper-proof manner in the verification station.

Ex. 1001, 14:61-63. Providing an annotated version of McCalley's Figure 22, reproduced below, Petitioner argues that "McCalley's 'overall package may include a tamper resistant housing 191 [yellow] as would be readily understood by those skilled in the art." Pet. 92 (quoting Ex. 1011, 10:49-59).

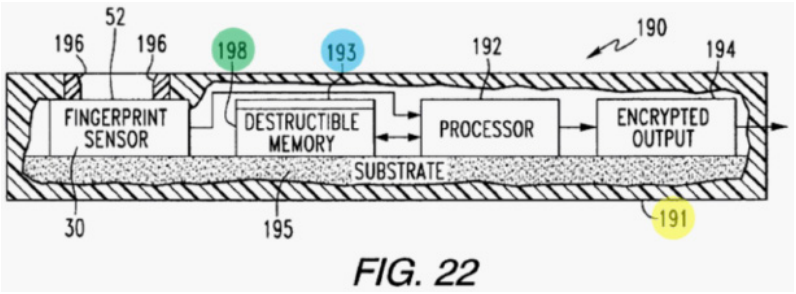


FIG. 22

McCalley's Figure 22 as annotated by Petitioner (Pet. 92) illustrates in partial cross-section tamper resistant housing 191 encompassing fingerprint sensor 30, memory 198, processor 192, and encrypted output 194. Ex. 1011, 10:45-54. Petitioner argues that "The '039 Patent, McCalley, Sanford, Hsu and Tsukamura are analogous art and are in the same field of endeavor, *i.e.*, access control using biometric technology. All references (and the '039 Patent) aim to provide more secured access." Pet. 93. Mr. Lipoff testifies that "[e]specially in the context of an ATM, as disclosed by Sanford, it was well-known that tamper-proof configuration was beneficial to prevent fraud." Ex. 1006 ¶ 454. Mr. Lipoff testifies further that a person of ordinary skill in the art "would have therefore looked to McCalley for details on how to make the system tamper-proof, such as having a tamper-proof housing." *Id.*

Mr. Lipoff explains that "having a tamper-proof housing and making memories self-destructible, [were] methods commonly in use at the time of the '039 Patent." *Id.* ¶ 455.

Patent Owner does not provide separate, substantive arguments with respect to claim 17 or the motivation and reasons to combine McCalley with Sanford and Hsu.

In this proceeding, for claim 17, Petitioner's arguments and Mr. Lipoff's testimony are unrebutted. We have considered, and on the complete record before us, accept as our own, Petitioner's arguments and evidence set forth at pages 91-94 of the Petition as to claim 17. Accordingly, we determine that Petitioner has shown by a preponderance of the evidence that claim 17 would have been obvious over Sanford, Hsu, and McCalley.

I. Grounds 4, 6, and 8: Claims 5, 12, and 17 – Obviousness over Sanford, Hsu, Tsukamura, and one of Leu, Houvener, and McCalley

Because we determine that claims 5, 12, and 17 would have been obvious over Sanford, Hsu, and one of Leu, Houvener or McCalley, we need not address these same claims are obvious over Sanford, Hsu, Tsukamura and one of Leu, Houvener or McCalley.

J. Patent Owner's Continued 315(b) Arguments

In its Response, Patent Owner reiterates its 315(b) argument that we previously addressed in our Institution Decision. PO Resp. 25-32; Inst. Dec. 10-35. Now, Patent

Owner argues that in our prior decision we placed too much weight on a lack of control of the proceedings by Apple, and that "[r]ather, a key to the RPI analysis is whether Apple and Petitioners have a structured, preexisting business relationship and whether Apple would receive more than a merely generalized benefit if trial is instituted." PO Resp. 29-30 (citing *Applications in Internet Time, LLC v. RPX Corp.*, 897 F.3d 1336, 1351 (Fed. Cir. 2018)) ("*AIT*").

As an initial matter, we think that Patent Owner's argument mischaracterizes, or at least oversimplifies, the holding in *AIT*. In *AIT*, the Federal Circuit admonished the Board for (1), making "certain factual findings that are not supported by substantial evidence," and (2) "fail[ing] to adhere to the expansive formulation of 'real party in interest' that is dictated by the language, structure, purpose, and legislative history of § 315(b)." *AIT*, 897 F.3d at 1351. The Federal Circuit explained in *AIT* that the Board failed to appreciate, among other things, the specific nature of the relationship between RPX and Salesforce, "that RPX, . . . is a for-profit company whose clients pay for its portfolio of 'patent risk solutions.'" *Id.* The Court stated that "the Board did not consider these facts, which, taken together, imply that RPX can and does file IPRs to serve its clients' financial interests, and that a key reason clients pay RPX is to benefit from this practice in the event they are sued by an NPE." *Id.* at 1352. As discussed below, we have not overlooked the facts and evidence surrounding the parties' relationship nor failed to consider the parties' litigation efforts in the district courts. To the extent Patent Owner has raised valid arguments that may have not been clearly addressed by the Board, we provide the following additional analysis.

With respect to point (1), it is important, factually, that the developer-distributor business relationship between Petitioner and Apple contrasts sharply with the specific intent of the NPE patent portfolio litigation relationship between RPX and Salesforce. As we described in our Institution Decision, Petitioner's product "Yale Smart Locks," including "the Yale Assure Lock uses a software application ('App') on one's mobile phone, here on an iPhone sold by Apple, to lock and unlock doors. The App is developed by Petitioner, or one of its business partners, and distributed to iPhone users through the Apple App store." Inst. Dec. 16. The Developer Agreement (the "Agreement") between Petitioner and Apple mainly provides "a limited license" to use Apple software "to develop and test" the developer's software applications for integration on Apple's iOS platforms. Ex. 2009. Importantly, different from *AIT*, in this case we have before us no facts or evidence showing that the intent, express or otherwise, of the Agreement between Petitioner and Apple is *fundamentally* based on protecting one party or the other from patent litigation.[15] To the extent Patent Owner now argues that we did not appreciate all of its arguments and evidence as to the parties' underlying actions in related district court proceedings, we address that matter in due course below. Before doing so, we turn to point (2), and whether, in this

15. We acknowledge that the Agreement contains representations and warranties of noninfringement, as well as indemnification clauses. Ex. 2009, 16, 41-43. We consider that these clauses are perhaps best understood, at least from Apple's perspective as a distributor, as mechanisms to avoid liability should the need arise, rather than tools exerting control or perpetuating an agency relationship with Petitioner.

case, our Institution Decision appropriately considered the "expansive formulation of 'real party in interest.'" *See AIT*, 897 F.3d at 1351.

In *AIT*, the Federal Circuit explained that the "Board's determination that Salesforce was not a real party in interest under § 315(b) relied on an impermissibly narrow understanding of the common-law meaning of the term." *Id.* at 1357. For one thing, the Court pointed out that "an agent with an ownership interest in the subject matter of the suit, or one who is the trustee of an express trust or a party in whose name a contract has been made for the benefit of another, may qualify as a real party in interest." *Id.* In this proceeding, Patent Owner has failed to point to any persuasive evidence, apart from software compatibility with Apple's iOS platforms as discussed in the Agreement, that Apple has any overt interest, influence, development or design influence over Petitioner's "Yale Smart Locks" products or App. In addition, Patent Owner has produced no evidence that Apple holds any ownership interest, assets, or expressly administers any property rights as a trustee or agent for the benefit of Petitioner indicative of real party in interest relationships under common law.

Essentially the entirety of the evidence of the business relationship in this proceeding is contained within the Agreement, which we already discussed in detail in our Institution Decision. Inst. Dec, 10-35. For example, there is an indemnification clause that requires Petitioner to

> [u]pon Apple's request, defend, Apple, its directors, officers, employees, independent contractors and agents (each an "Apple Indemnified Party") from any and all claims, losses, liabilities, damages, taxes, expenses and costs, including without limitation, attorneys' fees and court costs (collectively, "Losses"), incurred by an Apple Indemnified Party and arising from or related to . . . any claims that Your Covered Product or the distribution, sale, offer for sale, use or importation of Your Covered Product (whether alone or as an essential part of a combination), Licensed Application Information, metadata, or Pass Information violate or infringe any third party intellectual property or proprietary rights;

Id. at 43. There is no evidence in this case that Apple has invoked its rights under this clause, nor has Patent Owner argued or explained how this clause or the parties' actions before the Board and in the underlying district court litigation implicate a common law agency relationship between the parties. An agency relationship could potentially occur if Apple were to request Petitioner to step in and defend it. Yet Patent Owner has provided no argument or persuasive evidence that such is the case here. Apple has, in fact, committed to its own defense by filing its own IPR, e.g., IPR2022-00600, against Patent Owner. Moreover, compelling evidence provided by Petitioner in this case is exactly the opposite, as Petitioner avers under penalty of perjury in interrogatory responses that "[t]here have been no communications between Petitioners and Apple, directly or through counsel,

relating to indemnification or obligation to indemnify based on assertion of . . . U.S. Patent No. 8,620,039) (*id.* at 11-12)." Ex. 1023, 8-9, 14.

We recognize that Apple may derive some benefit if additional claims of the '039 patent are determined to be unpatentable in this proceeding. This derived benefit does not, however, make Apple an RPI to this proceeding. *See WesternGeco LLC v. ION Geophysical Corp.*, 889 F.3d 1308, 1321 (Fed. Cir. 2018) (stating in the context of the broader concept of privity that "[a]s a general proposition, we agree with the Board that a common desire among multiple parties to see a patent invalidated, without more, does not establish privity").

On the facts and evidence before us in this proceeding, it is the Agreement, analyzed here and in our Institution Decision that best explains the business relationship between the parties. The Agreement sets forth with reasonable clarity the specific expectations of the parties; mainly that (a) Petitioner is allowed "a limited license to use the Apple Software and Services provided to You under this Program to develop and test Your Applications on the terms and conditions set forth in this Agreement," and (b) "Applications that meet Apple's Documentation and Program Requirements may be submitted for consideration by Apple for distribution via the App Store, Custom App Distribution, or for beta testing through TestFlight." Ex. 2009, 1. Accordingly, the evidence leads us to conclude that Apple is a distributor of Petitioner's App for use with Petitioner's "Yale Smart Lock" products, and without more, that is about all that can be said about the relationship.

Appendix E

We turn, below, to particular facts in this case that Patent Owner argues the Board overlooked in our Institution Decision.

During oral argument Patent Owner's counsel raised a specific issue concerning our earlier conclusion in our Institution Decision that Apple is *not* a real party in interest to this proceeding or a privy with Petitioner. Inst. Dec. 28; Tr. 45-46. Counsel contends "there is an inconsistency between [Petitioner's], you know, assertions regarding Apple in the [Declaratory Judgment] complaint. And then in defending the RPI position." Tr. 45:20-23. Specifically, counsel explained that they "didn't see that the Board specifically considered our argument that it's relevant that ASSA ABLOY filed the DJ complaint with respect to the 039 patent, even though the 039 patent had never been raised by Patent Owner to ASSA ABLOY." *Id.* at 46:3-6. Counsel further argued that the present "situation mirror[s] the situation in the *Worlds v. Bungie* case, where a very similar fact pattern was considered relevant by the [F]ederal [C]ircuit." *Id.* at 46:7-9; *see also Worlds Inc. v. Bungie, Inc.*, 903 F.3d 1237, 1239 (Fed. Cir. 2018) ("*Bungie*") (determining that because "the Board erred in its real-party-in-interest analysis, we vacate its decisions and remand for proceedings consistent with this opinion").

Our analysis of Patent Owner's section 315(b) time bar arguments in our Institution Decision covers over 20 pages and considers in detail evidence submitted by both parties regarding business relationships and the Apple Developer License Agreement, i.e., the "Agreement," (Ex. 2009)

including warranties, indemnification, product inspection and insurance, between Petitioner and Apple. Inst. Dec. 10-35. For example, as it relates to Patent Owner's issue raised here, we noted that "[i]n the Declaratory Judgment complaint, Petitioner states, '[CPC] is also engaged in an aggressive litigation campaign that includes Apple Inc. ('Apple'), *a business partner* of [Petitioner]." *Id.* at 15. We explained that

> [t]he business relationship between Apple and Petitioner is that Petitioner, or one of the named entities collectively referred to as Petitioner, makes products that interface with Apple products and may be sold on Apple's website. For example, ASSA ABLOY Residential Group, Inc., a named entity included as a Petitioner in this proceeding, makes and sells security locks under the brand name "Yale" . . . the Yale Assure Lock uses a software application ("App") on one's mobile phone, here on an iPhone sold by Apple, to lock and unlock doors. The App is developed by Petitioner, or one of its business partners, and distributed to iPhone users through the Apple App store.

Id. at 15-16. Thus, in our Institution Decision we did consider the fact that Petitioner, in its Declaratory Judgment Complaint, admitted to being a business partner with Apple. We also considered the fact that, as part of the business relationship, Petitioner entered into the Agreement. *Id.* at 16. We considered critical clauses in the Agreement, such as the representations and warranties clause explaining that "[w]e do *not* consider Section 3.2(d)

to be a 'warranty.' It is not a guarantee that products will not infringe. It is a representation of the developer's current 'knowledge and belief.' It is far different from the obligations created by the App developer's agreement in *Bungie*." *Id.* at 20.

As discussed above, we determined that the Agreement did in fact contain an indemnification clause, which *could* be implemented "upon Apple's request." *Id.* at 23-26. However, also different from the facts in *Bungie*, in this case we have sworn interrogatories provided by Petitioner presenting strong evidence that "[t]here have been no communications between Petitioners and Apple, directly or through counsel, relating to indemnification or obligation to indemnify based on assertion of . . . U.S. Patent No. 8,620,039." *Id.* at 26 (quoting Ex. 1023, 11-12).

Patent Owner now urges us to also consider the fact that its cease-and-desist letters to Petitioner, i.e., the "Yale Letters" (Exs. 2005, 2006), never threatened Petitioner with infringement of the '039 patent, only U.S. Patent Nos. 9,665,705 and 9,269,208. *See* Prelim. Resp. 7 (Patent Owner arguing that it "never raised or otherwise mentioned the '039 Patent to Yale or any of the Petitioners at any time.") (citing Ex. 2008). This is a concern, Patent Owner contends, because Petitioner filed its Declaratory Judgment Complaint admitting to a business relationship with Apple as well as this IPR, and both proceedings challenge the '039 patent. *See* Ex. 2007 ¶ 2 (Petitioner stating in its Declaratory Judgment Complaint that "[t]he ASSA ABLOY Entities seek a declaration of non-infringement of U.S. Patent Nos. 9,269,208 ("the '208 Patent"), 9,665,705

("the '705 Patent"), and 8,620,039 ("the '039 Patent") (collectively, the "Patents-in-Suit")").

This argument is frankly somewhat undeveloped in Patent Owner's explanations of the facts and background in its Preliminary Response. Prelim. Resp. 5-10. We acknowledge that Petitioner was apparently never overtly threatened with infringement of the '039 patent. Ex 2005; Ex. 2006. Yet Patent Owner fails to persuasively explain *why* Petitioner's challenges to the '039 patent in the Declaratory Judgment Complaint weigh in favor of finding privy or a real party in interest relationship between Petitioner and Apple. *See* Prelim. Resp. 7 (Patent Owner arguing largely that "Patent Owner never raised or otherwise mentioned the '039 Patent to Yale or any of the Petitioners at anytime."). As we understand the argument, Patent Owner alleges that because it never threatened Petitioner with the '039 patent, Petitioner is now, without provocation, doing Apple's bidding and working at Apple's behest by challenging the '039 patent in the Declaratory Judgment Complaint and in these *inter partes* review proceedings. It is also not clearly explained why the inclusion of Petitioner's related entities of ASSA ABLOY Global Solutions, Inc. ('Hospitality'), and HID Global Corporation, in these IPR proceedings as real parties in interest and also in the Declaratory Judgment Complaint, matters as to the relationship between Petitioner and Apple. *See* Prelim. Resp. 8 (arguing that "Petitioners also filed the Declaratory Judgment Complaint as to HID and Hospitality, whom Patent Owner had never contacted regarding the patents or technology at issue") (citing Ex. 2005; Ex. 2006; Ex. 2008).

Two things can be true, Petitioner can have a business relationship with Apple and both parties can have a legitimate interest in defending themselves separately in litigation. We do not find anything in Petitioner's Declaratory Judgment Complaint that alters our prior decision in this regard. The fact that Petitioner and each of its entities were not explicitly threatened with infringement allegations in the Yale Letters as to the '039 patent does not mean that Patent Owner would never assert infringement against Petitioner based on the '039 patent claims. Ex. 2005; Ex. 2006. This is especially true in light of the fact that Patent Owner asserted the '039 patent against Apple in *CPC Patent Technologies Pty Ltd v. Apple Inc.*, No. 3:22-cv-02553, apparently due to or resulting from the products that Petitioner makes, uses, and sells through Apple's electronic device platforms. Ex. 2007 ¶ 44 ("On February 23, 2021, [Patent Owner] asserted all three of the Patents-in-Suit against Apple.").

On the facts here, we conclude that filing a declaratory judgment action or an *inter partes* review to challenge the claims of a patent, i.e., the '039 patent, that was asserted against a third party based on products made by Petitioner, is a reasonable litigation strategy for Petitioner independently. The declaratory judgment action filing itself does not demonstrate some sort of heightened collusion even where a benefit inures to a party with whom Petitioner has a business relationship. Patent Owner has not explained, for instance, that but for Apple's technology or actions, Petitioner has no actionable reason to challenge the patentability of the '039 patent claims. *See*, *generally*, Prelim. Resp. Also, by way of example, Patent Owner

argues in its Preliminary Response that in the Declaratory Judgment Complaint, "Petitioners further asserted that 'it is highly likely that Charter Pacific will sue the Assa Abloy Entities *on the same patents that have been asserted against Apple*." Prelim. Resp. 22 (quoting Ex. 2007 ¶ 30). In our view, this assertion is primarily offered in the Complaint to show Petitioner's apprehension of litigation because it admittedly makes, uses, and sells products potentially covered by the claims in the same three patents through Apple's platforms. Patent Owner does not explain persuasively why Petitioner would not have been concerned about infringing the '039 patent, nor why such apprehension shows any more intimate relationship than we considered in our Institution Decision. The mere fact that an accused infringer, in this case Petitioner, files a declaratory judgment action explaining its business relationship with Apple and offering reasons supporting the declaratory judgment action with respect to the same three patents that Apple is accused of infringing, does not, without more, establish persuasive additional information or substantive facts that we failed to consider in our original analysis.

Overall, and on the complete record before us, we do not find that any of Petitioner's assertions in its Declaratory Judgment Complaint change our underlying conclusion that Petitioner and Apple are not in privy or real parties in interest. *See* Inst. Dec. 34 (determining that "[t]he totality of the evidence before us does not establish anything other than a traditional business relationship between Apple and Petitioner.").

III. CONCLUSION[16]

For the reasons discussed above, we determine Petitioner meets its burden of establishing, by a preponderance of the evidence, that the challenged claims are unpatentable, as summarized in the following table:

Claim(s)	35 U.S.C. §	Reference(s)/	Claim(s) Shown Unpatentable	Claims Not Shown Unpatentable
3, 4, 6-11, 15, 16, 18	103(a)	Sanford, Hsu	3, 4, 6–11, 15, 16, 18	
3, 4, 6-11, 15, 16, 18	103(a)	Sanford, Hsu Tsukamura[17]		
5	103(a)	Sanford, Hsu, Leu	5	

16. 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).

17. Because Petitioner's contentions regarding the obviousness of claims 3, 4, 6-11, 15, 16, and 18 in view of Sanford and Hsu are dispositive of these challenged claims, we do not reach asserted ground 2. *See In re Gleave*, 560 F.3d 1331, 1338 (Fed. Cir. 2009).

5	103(a)	Sanford, Hsu, Leu, Tsukamura[18]		
12	103(a)	Sanford, Hsu, Houvener	12	
12	103(a)	Sanford, Hsu, Tsukamura, Houvener[19]		
17	103(a)	Sanford, Hsu, McCalley	17	
17	103(a)	Sanford, Hsu, Tsukamura, McCalley[20]		

18. Because Petitioner's contentions regarding the obviousness of claim 5 in view of Sanford, Hsu and Leu are dispositive of these challenged claims, we do not reach asserted ground 4. *See In re Gleave*, 560 F.3d. at 1338.

19. Because Petitioner's contentions regarding the obviousness of claim 12 in view of Sanford, Hsu and Houvener are dispositive of these challenged claims, we do not reach asserted ground 6. *See In re Gleave*, 560 F.3d. at 1338.

20. Because Petitioner's contentions regarding the obviousness of claim 17 in view of Sanford, Hsu and McCalley are dispositive of these challenged claims, we do not reach asserted ground 8. *See In re Gleave*, 560 F.3d. at 1338.

Appendix E

III. ORDER

For the reasons given, it is

ORDERED that, based on a preponderance of the evidence, claims 1, 2, 13, 14, 19, and 20 of the '039 patent have been shown to be unpatentable; and

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

For PETITIONER: Dion Bregman, Andrew Devkar, and James Kritsas - MORGAN LEWIS & BOCKIUS LLP

For PATENT OWNER: Andrew Ryan - CANTOR COLBURN LLP