

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

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.

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

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

DANIELS, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision on Remand
Determining Claims 3–12 and 15–18 Not Unpatentable
35 U.S.C. §§ 144, 318(a)

I. BACKGROUND

On June 13, 2022, ASSA ABLOY AB, ASSA ABLOY Inc., ASSA ABLOY Residential Group, Inc., August Home, Inc., HID Global Corporation, and ASSA ABLOY Global Solutions, Inc., (“ASSA ABLOY” 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”). This proceeding is related to IPR2022-01093, which challenged different claims of the ’039 patent on similar grounds.

In this proceeding, the Petition challenged the patentability of claims 3–12 and 15–18 of the ’039 patent under the following grounds:

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

¹ 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.

² Ex. 1003, European Patent Appl’n No. EP 0924655 A2 (pub. June 23, 1999).

³ Ex. 1004, PCT Appl’n No. PCT/US03/07238 (pub. Sept. 18, 2003).

⁴ Ex. 1005, US Patent No. 6,963,660 B1 (Nov. 8, 2005).

⁵ Ex. 1008, European Patent Appl’n No. EP O 881 608 A1 (pub. Dec. 2, 1986).

⁶ Ex. 1010, US Patent No. 5,790,674 (Aug. 4, 1998).

Ground	Claim(s) Challenged	35 U.S.C. § ¹	Reference(s)/Basis
6	12	103(a)	Hsu, Sanford, Tsukamura, Houvener
7	17	103(a)	Hsu, Sanford, McCalley ⁷
8	17	103(a)	Hsu, Sanford, Tsukamura, McCalley

On February 2, 2023, we instituted an *inter partes* review of all claims challenged in the Petition on all of the asserted grounds. *See* Paper 19 (“Inst. Dec.”). Our Final Written Decision in this proceeding, and in IPR2022-01093, issued January 31, 2024. Paper 37 (“Original Decision”).⁸ The Original Decision in this proceeding determined that Petitioner had shown by a preponderance of the evidence that claims 3–12 and 15–18 are unpatentable. Original Decision 2.

On appeal, the U.S. Court of Appeals for the Federal Circuit reversed our Original Decision and remanded the case for further proceedings. *CPC Pat. Techs. Pty Ltd. v. ASSA ABLOY AB*, No. 2024-1492, 2025 WL 3134960, at *1 (Fed. Cir. Nov. 10, 2025), Paper 43. The Federal Circuit noted that in light of the Court’s affirmance of a separate decision in IPR2022-00600, “our discussion about the errors the Board made in this appeal only extends to claims 3–18, which were not at issue in the other appeal.” *Id.* at *3 n 1.

At the request of the parties, we permitted additional briefing addressing the issues on remand from the Federal Circuit. Paper 42. Petitioner filed an opening brief (Paper 49 (“Pet. Remand Br.”)), and Patent Owner also filed an opening brief (Paper 50 (“PO Remand Br.”)). Both

⁷ Ex. 1011, US Patent No. 5,956,415 (Sep. 21, 1999).

⁸ The procedural history is summarized in the Original Decision.

parties also filed responsive briefs. Paper 52 (“Pet. Responsive Br.”); Paper 53 (“PO Responsive Br.”).

This is a Final Written Decision on Remand addressing the patentability of the challenged claims. To prevail, Petitioner must prove unpatentability by a preponderance of the evidence. *See* 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d). This Final Written Decision on Remand is issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73.

For the reasons discussed below, we determine that Petitioner has failed to show by a preponderance of the evidence that claims 3–12 and 15–18 are unpatentable.

A. Related Matters

In addition to the cases noted above, Petitioner indicated in its Petition 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.

Earlier in this proceeding, Patent Owner indicated 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.

Notably, the ’039 patent was 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, and Apple challenged the ’039 patent in IPR2022-00600 on

different prior art. *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. Our determination in IPR2022-00600 was affirmed by the Federal Circuit. *See CPC Pat. Techs. Pty Ltd. v. Apple, Inc.*, No. 2024-1278, 2025 WL 2248796, at *1 (Fed. Cir. Aug. 7, 2025), *cert. denied*, 146 S. Ct. 368, 223 L. Ed. 2d 197 (2025).

B. 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 3:4–11.⁹ 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.

Figure 4 of the '039 patent is reproduced below.

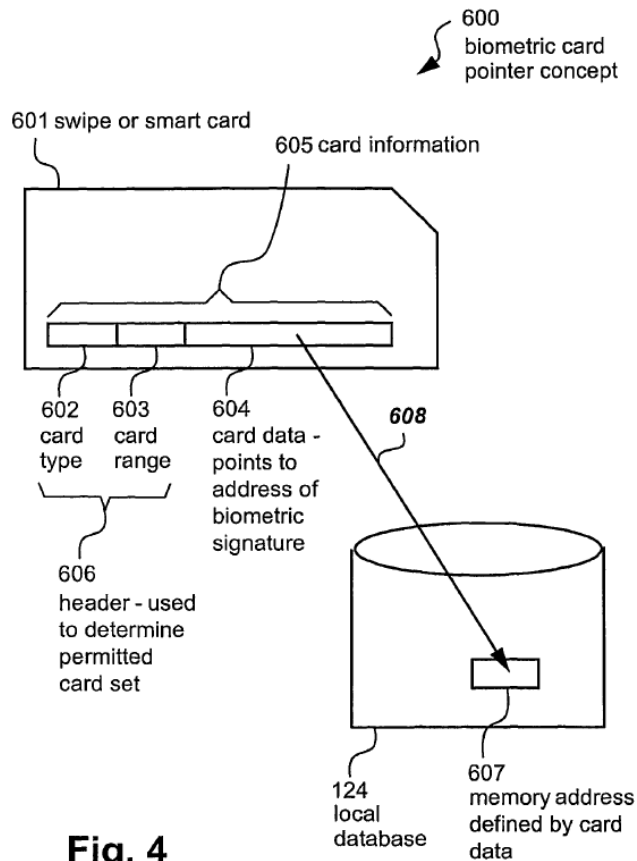


Fig. 4

⁹ 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.

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.

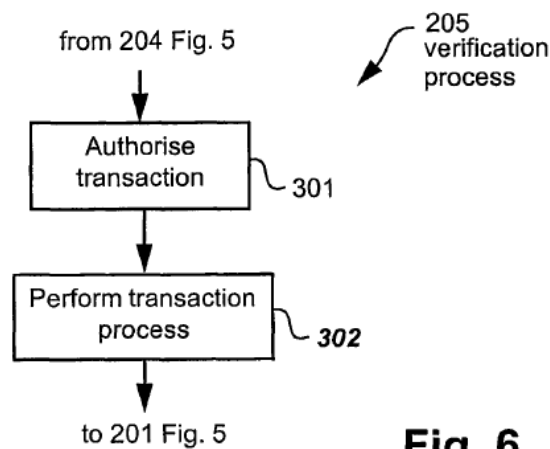


Fig. 6

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

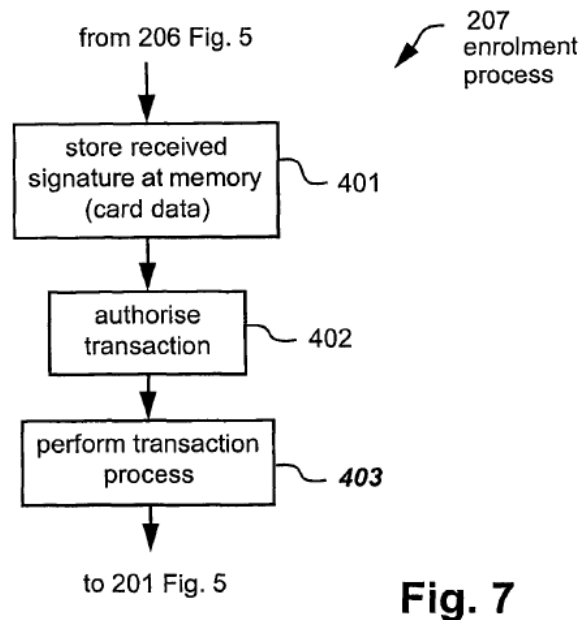


Fig. 7

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).

C. 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 limitation 3(da) in italics:

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

(a) providing card information from a card device to a card reader in the verification station;

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

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

(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;

(e) if the provided card information has been previously provided to the verification station;

(ea) comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

(eb) if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

(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 in claim 3(a)–(ec) 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.

II. ANALYSIS

A. Legal Standards

“In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) as “requiring [*inter partes* review] petitions to identify ‘with particularity . . . the evidence that supports the grounds for the challenge to each claim’”); *see also* 37 C.F.R. § 42.104(b) (requiring a petition for *inter partes* review to identify how the challenged claim is to be construed and where each element of the claim is found in the prior art patents or printed publications relied upon). That burden never shifts to the patentee. *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). Furthermore, Petitioner cannot satisfy its burden of proving obviousness by employing “mere conclusory statements.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016).

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

Consistent with our Original Decision, 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.

Original Decision 36; *see also* IPR2022-00600, Paper 22 at 12 (PTAB October 13, 2023) (Final Written Decision).

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))).

1. *Limitation 3(da)*

The issues on remand revolve essentially around limitation 3(da):

Limitation 3(da) – storing the inputted biometric signature in a memory at a memory location defined by the provided card information;

Ex. 1001, 12:61–63. Considering limitation 3(da) in our Original Decision, we explained 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.

Original Decision 16.

With respect to the similar limitation “*means for* storing the inputted biometric signature in a memory at a memory location defined by the provided card information” in claim 15, in our Original Decision we explained that Petitioner’s proposed construction under 35 U.S.C. § 112(6) was consistent with the record in this case and also consistent with the

District Court proceeding. *Id.* at 18; Inst. Dec. 39–43; *see also* Ex. 1012, 1–4.

2. *Limitation 3(d)*

In the Original Decision we also considered claim limitation 3(d) and determined that “the limitations of claims 3, 15, and 18 to include, at least in part, an enrollment process.” Original Decision 14. However, neither in our Original Decision, nor in this Decision, does the issue of “enrollment” create any particular dispute between the parties.

3. *The Federal Circuit*

The Federal Circuit has not determined that any construction set forth in our First Final Written Decision is erroneous.¹⁰ *See generally ASSA ABLOY AB* 2025 WL 3134960. In addition, the Federal Circuit affirmed our determinations under the same claim constructions with respect to claims 1, 2, 19, and 20 in IPR2022-00600 reciting similar limitations, for example, “defining, dependent upon the received card information, a memory location in a local memory external to the card.” *CPC Pat. Techs.* 2025 WL 2248796.

Also, the parties have not argued any claim constructions contrary to what was determined in our Original Decision. *See generally* Pet. Remand Br.; PO Remand Br. For these reasons we maintain our constructions for these limitations, including “storing the inputted biometric signature in a memory at a memory location defined by the provided card information” as set forth in the Original Decision. Original Decision 12–18.

¹⁰ In the present proceeding, the Federal Circuit reversed our determination of obviousness based on Hsu and Sanford for ground 1, and instructed that the remand is “for consideration of other unpatentability grounds not reached by the Board and not otherwise foreclosed by this decision.” *ASSA ABLOY AB* 2025 WL 3134960 *9.

Initially, because the Federal Circuit reversed our determination as to ground 1 and the Hsu-Sanford combination, we focus this Decision on the remaining grounds 2–8 not reached in our Original Decision.¹¹

D. Ground 2: Claims 3, 4, 6–11, 15, 16, and 18 – Obviousness over Sanford (Ex. 1004), Hsu (Ex. 1003), and Tsukamura (Ex. 1005)

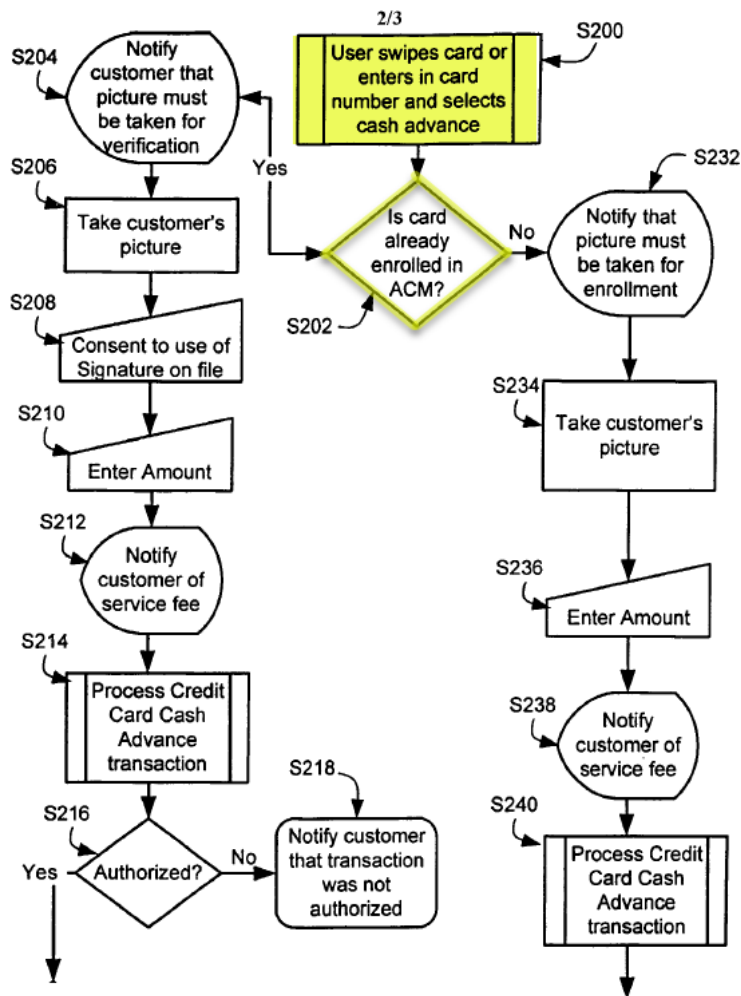
For the reasons below, and on the complete record before us, Petitioner has not shown by a preponderance of the evidence that claims 3, 4, 6–11, 15, 16, and 18 would have been obvious over Sanford, Hsu, and Tsukamura.

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

¹¹ Petitioner argues that we are not foreclosed from also revisiting ground 1 and the combination of Hsu and Sanford. Pet. Remand Br. 1. Regardless of whether this is accurate based on the Federal Circuit’s reversal of our Original Decision considering ground 1 and Hsu, we address Hsu, and Mr. Lipoff’s relevant testimony, in our consideration and analysis of the parties’ briefs on remand *infra*. See *ASSA ABLOY AB* 2025 WL 3134960 *9 (remanding “for consideration of other unpatentability grounds not reached by the Board and not otherwise foreclosed by this decision.”).

fingerprint technology.” *Id.* ¶ 20. The relevant part of Sanford’s Figure 2, as annotated by the Board (in yellow), is reproduced below.

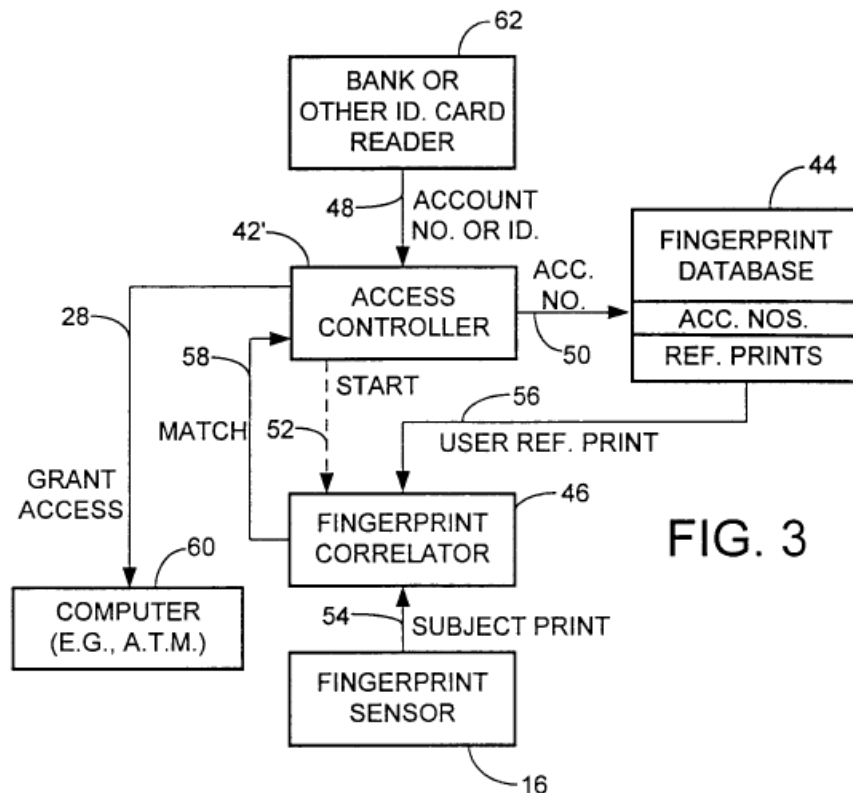


Sanford’s Figure 2 is a block diagram illustrating a method for performing a PIN-less credit card transaction using an ACM (automated cashier machine). *Id.* ¶ 24. After a user swipes a card at step 200, the system determines whether the user’s card information is already stored, i.e. enrolled, and “the 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.



Hsu’s Figure 3 is a block diagram illustrating card reader 62 that reads “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 fingerprint 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.

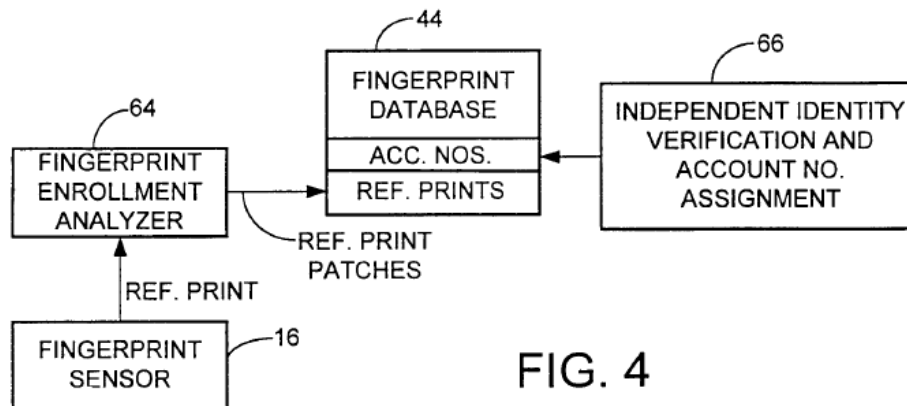


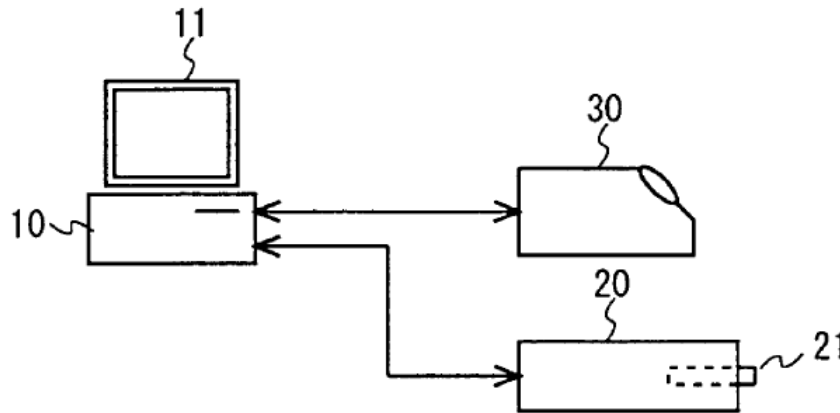
FIG. 4

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. *Tsukamura (Ex. 1005)*

Tsukamura teaches a fingerprint collating device and method to prevent fraudulent fingerprint comparisons. Ex. 1005, Abstract, code (57). As shown in Figure 1 below, Tsukamura’s device compares a user’s fingerprint input via fingerprint collating unit 30 with a stored fingerprint template. *Id.* at 2:33–34.



1

Tsukamura’s Figure 1 illustrates fingerprint collating unit 30 connected through personal computer 10 with card reader 20 and IC (integrated circuit) card 21. *Id.* at 2:18–25. Fingerprint templates can be stored either in the collating unit’s flash memory or on IC card 21. *Id.* at 2:26–32.

Tsukamura explains that when a fingerprint is normally, i.e., physically, scanned through collating unit 30, a “fingerprint accepting flag” is set in memory. *Id.* at 4:1–6. Thus, if someone attempts to provide falsified fingerprint data externally into the system, the flag will not be set, and the system will not authenticate. *Id.* at 6:14–22.

When the flag is set, Tsukamura's system provides two collation modes:

1) Internal: System compares the physical scan against fingerprint templates stored in the collating unit 30 flash ROM based on an index number N index; and

2) IC Card: System compares the physical scan against a fingerprint template from the IC card. In both cases the system performs the same flag-gated comparison with the physical fingerprint scan.

Id. at 3:35–5:2. Tsukamura explains with respect to the Internal mode that:

[w]hen the fingerprint collation is performed by using a fingerprint template Temp registered within the fingerprint collating unit 30, the user uses the personal computer 10 to start a fingerprint collation process and input an index number N index. The personal computer 10 sends a finger print collation instruction Ref and the index number N index *specified by the user* to the fingerprint collating unit 30 in response to this.

Id. at 3:39–46 (emphasis added). Tsukamura's Figure 3 is reproduced below illustrating how fingerprint templates are stored in fingerprint collating unit 30 flash ROM. *Id.* at 3:25–35.

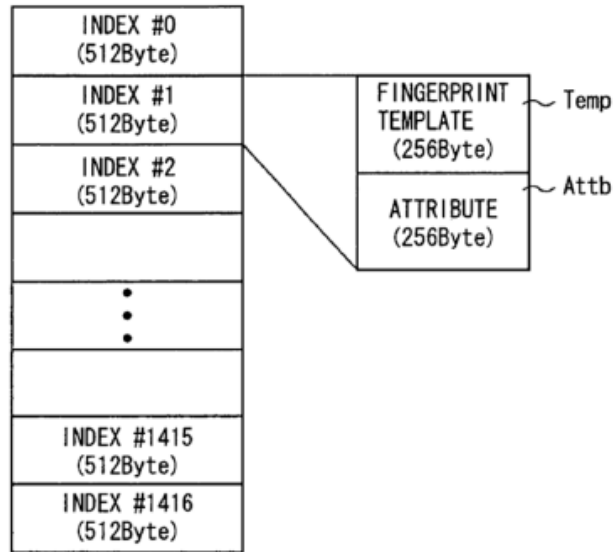


FIG. 3

Figure 3 “is a diagram showing a stored state of fingerprint data.” *Id.* at 2:9–10.

In the IC card mode, collation controller 34 reads the user’s fingerprint and stores it in RAM 36. *Id.* at 4:40–50. Tsukamura explains next that

collation controller 34 reads the fingerprint template Temp registered within the IC card 21 via the personal computer 10, and stores the fingerprint template Temp at an index #0 in the collation flash ROM 35. And the collation controller 34 reads the fingerprint template Temp from the index #0 in the collation flash ROM 35, and performs the collation between the fingerprint template Temp and the fingerprint image data D37.

Id. at 4:51–58.

Subsequently, Tsukamura describes that, for either mode, collation of the fingerprint can only be performed “when the collating fingerprint accepting flag has been set.” *Id.* at 5:16–17. Therefore, according to

Tsukamura, the flag is *not* set “if the read fingerprint information is entered externally and illicitly, [and] the personal authentication is not performed. Consequently, it is possible to provide the fingerprint collating device which can prevent an illicit use of fingerprint.” *Id.* at 5:30–34.

4. *Independent claim 3 and claim limitation 3(da)*

Because the resolution as to claim limitation 3(da) is dispositive in this case on remand, we consider mainly the elements of claim limitation 3(da).

3(da) storing the inputted biometric signature in a memory at a memory location defined by the provided card information;

In our Original Decision, we explained that

[b]ased 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.

Original Decision 33–34. Further, considering Hsu’s disclosure in light of the testimony of Petitioner’s declarant, Mr. Lipoff’s, we determined that a person of ordinary skill in the art would have understood

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.

Id. at 36.

On appeal, the Federal Circuit determined that “Hsu’s disclosure offers nothing to suggest that its card information ‘tells you’ where to store

the fingerprint data.” *ASSA ABLOY AB*, 2025 WL 3134960 at *3. Reversing our determinations as to Hsu, the Court found that the testimony of Petitioner’s declarant, Mr. Lipoff, “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.” *Id.* at 8. Therefore, on remand, a central question is whether Petitioner has shown sufficiently that Tsukamura cures this deficiency. Petitioner has not.

In the Petition, Tsukamura is relied upon for teaching a specific location for storing fingerprint data. *See* Pet. 69 (Petitioner stating that “**Tsukamura’s index number specifies the physical memory location in the memory.**”) (citing Ex. 1005, 2:34–36, 2:46–47, 3:28–32, Fig. 2; Ex. 1006 ¶¶ 394–395). Petitioner argues that “[t]hus, Tsukamura discloses defining, dependent upon the “index number N index,” a memory location for storing a biometric signature (*e.g.*, a fingerprint template), *i.e.*, the memory location is specified by the index number.” *Id.* In support, Petitioner’s declarant, Mr. Lipoff, testifies that “[i]f the Tsukamura implementation were used for Sanford-Hsu database, each user/account number would specify a different entry (index number) in the database. Ex. 1006 ¶ 394.

Tsukamura’s index number N index does not teach or suggest much more than Hsu’s 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.” *Compare* Ex. 1004, code (57), *with* Ex. 1005, 4:7–11. That is, both references arguably teach defining, *i.e.*, setting or establishing, a certain location in a database for biometric data. For example, as described above, Tsukamura’s fingerprint template Temp is

stored in flash ROM 35 at a defined *index number N index* in the database. *Id.* 4:7–11, 50–54. However, neither Petitioner, nor Mr. Lipoff, persuasively explain how or why Tsukamura’s fingerprint template Temp is set or established “at a memory location defined by the provided card information” as recited in claim limitation 3(da).

Taking a close look at Petitioner’s testimonial evidence as to claim 3, we first note Mr. Lipoff testifies that

Tsukamura’s index number specifies the physical memory location in the memory. Thus, Tsukamura discloses defining, dependent upon the “index number N index,” a memory location for storing a biometric signature (*e.g.*, a fingerprint template), *i.e.*, the memory location is specified by the index number, under the Second Construction. In my opinion, if the Tsukamura implementation were used for Sanford-Hsu database, each user/account number would specify a different entry (index number) in the database.

Ex. 1006 ¶ 394. This is consistent with our understanding of Tsukamura, and we can agree that Tsukamura teaches defining—that is, setting or establishing—a location for storing the biometric signature at “index number N index.” *See* Ex. 1005, 4:7–11. But, concomitant with the Federal Circuit’s point, such an associative link does not sufficiently explain how one of ordinary skill in the art would have understood Tsukamura’s *IC card information* to define “as in ‘set’ or ‘establish[.]’” a memory location, as our claim construction requires. *See* Section II.C.3.

For instance, Tsukamura explains for the mode where fingerprint template Temp is stored in fingerprint collating unit 30

the user uses the personal computer 10 to start a fingerprint collation process and input an index number N index. The personal computer 10 sends a fingerprint collation instruction Ref and the index number N index specified by the user to the fingerprint collating unit 30 in response to this.

Ex. 1006, 5:39–46. In this mode, it is the user and personal computer that specify the index number N index. Alternatively, in the IC card mode, “[t]he collation controller 34 reads the fingerprint template Temp registered within the IC card 21 via the personal computer 10, and stores the fingerprint template Temp at an index #0 in the collation flash ROM 35.” *Id.* at 6:50–54. Thus, neither mode in Tsukamura tells us that it is the IC card information that defines—that is, “sets or establishes”—the index number N index where fingerprint template Temp is stored.

Nor does Mr. Lipoff’s testimony, describing that the fingerprint is stored index number N index, provide sufficient evidence explaining why one of ordinary skill in the art would have considered the IC card information to provide the index number N index. *See* Ex. 1032 ¶ 35 (Mr. Lipoff testifying that “it would have been obvious to assign Tsukamura’s index number as the user/account/employee number in the Sanford-Hsu system”). In fact, Mr. Lipoff further states that Tsukamura’s IC card disclosure “has no bearing on my unpatentability analysis because Petitioners do not rely on Tsukamura’s IC card 21 for disclosing the claimed ‘card information.’ Tsukamura is relied on under Ground 2 solely for its memory configuration.” *Id.*

Tsukamura, therefore, does not cure the underlying problem with Hsu and Sanford, namely the lack of substantial evidence “that Hsu’s card information determines the memory location of the biometric data.” *ASSA ABLOY AB*, 2025 WL 3134960 at *3. Accordingly, Petitioner has not shown by a preponderance of the evidence that independent claim 3 is obvious over Hsu, Sanford, and Tsukamura.

5. *Independent claim 15*

Independent claim 15 includes the same limitation as claim 3 discussed above, specifically, “storing the inputted biometric signature in a memory at a memory location defined by the provided card information.” Ex. 1001, 14:32–34. For the same reasons as claim 3, Petitioner has not shown by a preponderance of the evidence that claim 15 is obvious over Sanford, Hsu, and Tsukamura. Pet. 76–79

6. *Dependent claims 4, 6–11, 16, and 18*

Because claims 4, 6–11, 16, and 18 each depend either directly or indirectly from either independent claim 3 or independent claim 15, for the reasons discussed above Petitioner has not shown that these claims would have been obvious in view of Hsu, Sanford, and Tsukamura. Pet. 76, 79–80.

E. Grounds 3–4: Dependent Claim 5 – Obviousness over Sanford, Hsu, and Leu (Ex. 1003), and Sanford, Hsu, Tsukamura, and Leu

Claim 5 depends directly from claim 3 and further requires that “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, 13:23–27.

For these limitations, Petitioner relies on Leu for teaching a verification station where “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). Petitioner does not rely on Leu for teaching or disclosing “storing the inputted biometric signature in a memory at a memory location defined by the provided card information,” as recited in

independent claim 3. Ex. 1001, 14:32–34; *see generally* Pet. 80–87.

Therefore, Leu does not cure the underlying problem with either the Hsu, Sanford, or Hsu, Sanford, and Tsukamura combinations with respect to limitation 3(da). Therefore, Petitioner has not shown by a preponderance of the evidence that claim 5 would have been obvious over Sanford, Hsu and Leu, or Sanford, Hsu, Tsukamura, and Leu.

F. Grounds 5–6: Dependent Claim 12 – Obviousness over Sanford, Hsu, and Houvener (Ex. 1010), and Sanford, Hsu, Tsukamura, and Houvener

Claim 12 depends directly from claim 3 and further requires the 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, 13:63–66.

For these limitations Petitioner argues that “Houvener discloses a biometric verification system with ‘**audit** capabilities’ . . . [s]pecifically, Houvener discloses ‘**stor[ing]** the users PIN and the data from the specific transaction as a transaction record.’” Pet. 88 (quoting Ex. 1010 Abstract, 7:58–60). Petitioner’s declarant, Mr. Lipoff, testifies that “a POSITA would have understood that Houvener discloses storing success transaction records to ‘monitor transaction patterns’ and output these records for audit purposes (*e.g.*, fraud detection).” Ex. 1006 ¶ 438.

Petitioner does not rely on Houvener for teaching or disclosing “storing the inputted biometric signature in a memory at a memory location defined by the provided card information,” as recited in independent claim 3. Ex. 1001, 14:32–34; Pet. 87–91. Houvener does not cure the underlying problem with either the Hsu, Sanford, or Hsu, Sanford, and Tsukamura combinations with respect to limitation 3(db). Therefore, Petitioner has not

shown by a preponderance of the evidence that claim 12 would have been obvious over Sanford, Hsu and Houvener, or Sanford, Hsu, Tsukamura, and Houvener.

G. Grounds 7–8: Dependent Claim 17 – Obviousness over Sanford, Hsu, and McCalley (Ex. 1011), and Sanford, Hsu, Tsukamura, and McCalley

Claim 17 depends directly from independent claim 15 and adds “wherein the memory is incorporated in a tamper-proof manner in the verification station.” Ex. 1001, 14:61–63.

Petitioner argues that “McCalley discloses a ‘fingerprint sensor package’ that ‘include[s] a reference fingerprint memory for storing reference fingerprint information . . . [s]pecifically, 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, Abstract, 10:49–59). Petitioner provides an annotated version of McCalley’s Figure 22, reproduced below.

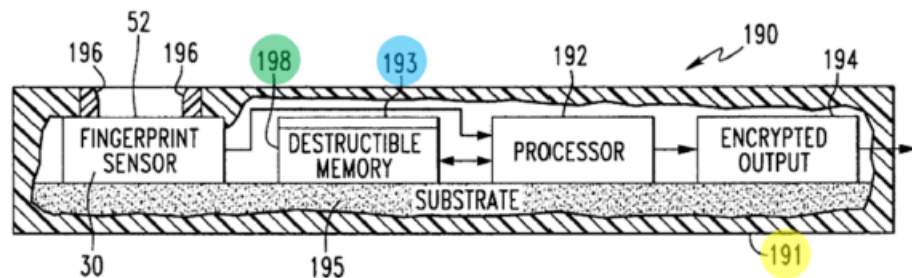


FIG. 22

In McCalley’s Figure 22, Petitioner annotates memory 198 in green and memory 193 in blue within housing 191 in yellow.

Petitioner does not rely on McCalley for teaching or disclosing “storing the inputted biometric signature in a memory at a memory location

defined by the provided card information,” as recited in independent claim 3. Ex. 1001, 14:32–34; *see generally* Pet. 91–94. McCalley does not cure the underlying problem with either the Hsu, Sanford, or Hsu, Sanford, and Tsukamura combinations with respect to limitation 3(db). Therefore, Petitioner has not shown by a preponderance of the evidence that claim 17 would have been obvious over Sanford, Hsu and McCalley, or Sanford, Hsu, Tsukamura, and McCalley.

H. The Parties’ Remand Briefs

On remand from the Federal Circuit, we authorized the parties respective briefing to address the “unpatentability grounds not reached by the Board and not otherwise foreclosed by [the Federal Circuit’s] decision,” specifically grounds 2–8. *ASSA ABLOY AB*, 2025 WL 3134960 at *4; *see also* Paper 42. For the sake of completeness, and in the context of the Federal Circuit decision, we address the parties’ main arguments in their respective remand briefs. *See generally* Pet. Remand Br.; PO Remand Br.; Pet. Responsive Br.; PO Responsive Br.

The Federal Circuit majority explained that “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.” *ASSA ABLOY AB*, 2025 WL 3134960 at *7. The majority decision explained that “associated” data was insufficient because “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.” *Id.* at *8–9. To this end, Petitioner makes several arguments based on an over-arching assertion, namely that Mr. Lipoff’s “[e]xpert testimony—that the Federal Circuit majority did not consider—bridges this ‘associate’ with ‘set’/‘establish’ gap.” Pet. Remand Br. 5; Pet. Responsive Br. 1–6.

Petitioner contends that we should again consider ground 1 in the context of the complete record, “that the Federal Circuit did not fully consider.” Pet. Responsive Br. 2. And, to the contrary, Patent Owner argues that “[t]he Board properly . . . consider[ed] the Grounds set forth in the Petition (Paper 2) that the Board did not reach in its Final Written Decision (Paper 37).” PO Responsive Br. 1. A plain reading of the decision indicates to us that Federal Circuit did—in fact—consider the entire record. *See, e.g., ASSA ABLOY AB, 2025 WL 3134960* at *8 (stating that “[s]till missing is any non-conclusory testimony that Hsu’s card information determines the memory location of the biometric data”). However, to be fully responsive, we address Petitioner’s arguments and evidence on remand as to ground 1.

In ground 1 and the Sanford–Hsu combination, Petitioner argues that, during his deposition, Mr. Lipoff described Hsu’s “‘user number is defining the memory location in which the stored fingerprint image will be stored because the structure of the database is one . . . that starts with the user number telling you where to find the memory location that has the stored fingerprint image.’” Pet. Remand Br. 5 (quoting Ex.2041, 34:3–12). Second, Petitioner argues that in Mr. Lipoff’s second declaration he

opined that “upon a user enrolling, they provide a previously unseen card/user number, 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,” and that “this simple and obvious option would satisfy Limitation 1[C]’s ‘defining’ step.”

Id. (quoting Ex. 1032 ¶ 3[3]).¹²

¹² Petitioner mistakenly cites to paragraph 34 of Mr. Lipoff’s second declaration. *See* Ex. 1032 ¶ 34 (Mr. Lipoff introducing rebuttal of Petitioner’s “unpatentability showings under Ground 2”).

Third, Petitioner argues that even if Hsu does not teach the physical memory address where the fingerprint is stored, Tsukamura does. *Id.* at 6. Petitioner points to Mr. Lipoff’s testimony that a “POSITA would know that Tsukamura’s index number specifies the physical memory address in the memory.” *Id.* (quoting Ex. 1006 at ¶¶ 215).¹³

We do not find these arguments persuasive because they do not overcome the issue raised by the Federal Circuit and the specific language of claim limitation 3(da), namely “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). As for Hsu, for example, Mr. Lipoff’s testimony from his second declaration, above, contends that “the system then creates a new record for the user” based on an “unseen card/user number.” Ex. 1032 ¶ 33. The Federal Circuit deemed such testimony conclusory:

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.

ASSA ABLOY AB, 2025 WL 3134960 at *8. Indeed, it is this same testimony from Mr. Lipoff’s second declaration that the Federal Circuit explained was lacking as to Hsu. *Id.* (citing Ex. 1032 ¶ 33). Petitioner’s citations to the record and Mr. Lipoff’s testimony do not persuade us that either the Federal Circuit, or the Board, has overlooked evidence sufficient to show that Hsu’s card information, alone or in combination with Sanford,

¹³ Somewhat contradictory to this position, Petitioner stated in its Reply that “the Petition does not rely on Tsukamura’s IC card 21 for disclosing the claimed ‘card information.’ Tsukamura is relied on under Ground 2 solely for its memory configuration.” Reply 16 (citing Pet. 67–69).

determines the memory location of the biometric data. As for Tsukamura, discussed in detail above, Petitioner’s arguments and evidence on remand, including Mr. Lipoff’s testimony, e.g., that “Tsukamura’s index number acts as a pointer to a specific memory location for storing the fingerprint,” (Ex. 1032 ¶ 38), still fail to account for limitation 3(da) requiring the “card information” to set or establish the memory location. Section II.D–G.

Patent Owner’s Opening Brief on Remand argues that “[w]hile Petitioner asserted that ‘Tsukamura’s index number acts as a pointer to a specific memory location for storing the fingerprint . . .’ (Paper 25 at 16), this falls short of disclosing that *during enrollment* some ‘card information’ itself ‘sets or establishes’ that memory address.” PO Remand Br. 6. For all the reasons above, we agree with Patent Owner.

III. CONCLUSION

Neither Hsu or Tsukamura, alone or in combination, teaches claim limitation 3(da), or the same respective limitations in independent claims 15 and 18, for the reasons discussed above.

Considering all the challenged claims, we determine that Petitioner has failed to meet 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)/ Basis	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		3, 4, 6–11, 15, 16, 18

Claim(s)	35 U.S.C. §	Reference(s)/ Basis	Claim(s) Shown Unpatentable	Claims Not Shown Unpatentable
5	103(a)	Sanford, Hsu, Leu		5
5	103(a)	Sanford, Hsu, Leu, Tsukamura		5
12	103(a)	Sanford, Hsu, Houvener		12
12	103(a)	Sanford, Hsu, Tsukamura, Houvener		12
17	103(a)	Sanford, Hsu, McCalley		17
17	103(a)	Sanford, Hsu, Tsukamura, McCalley		17
Overall Outcome				3–12, 15–18

III. ORDER

For the reasons given, it is

ORDERED that, based on a preponderance of the evidence, claims 3–12 and 15–18 of the '039 patent have not 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.

IPR2022-01094
Patent 8,620,039 B2

For PETITIONER:

Lionel M. Lavenue
Cory C. Bell
Bradford C. Schulz
FINNEGAN, HENDERSON, FARABOW, GARRETT, & DUNNER LLP
lionel.lavenue@finnegan.com
cory.bell@finnegan.com
bradford.schultz@finnegan.com

PATENT OWNER:

Matteo D. Pedini
Steven M. Coyle
Nicholas A. Geiger
CANTOR COLBURN LLP
mpedini@cantorcolburn.com
scoyle@cantorcolburn.com
ngeiger@cantorcolburn.com