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.,
Petitioners,

v.

CPC Patent Technologies PTY LTD.,
Patent Owner.

Case No. IPR2022-01094

Patent No. 8,620,039

PETITION FOR *INTER PARTES* REVIEW OF

U.S. PATENT NO. 8,620,039 (CLAIMS 3-12 and 15-18)

Mail Stop "PATENT BOARD"
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

TABLE OF CONTENTS
(continued)

EXHIBIT LIST

EXHIBITS FILED BY PETITIONERS	
EX-1001	U.S. Patent No. 8,620,039 ("'039 Patent")
EX-1002	Patent Prosecution History of U.S. Patent No. 8,620,039
EX-1003	European Patent Pub. No. EP 0924655A2 to Hsu *et al.* ("Hsu")
EX-1004	World Intellectual Property Organization (WIPO) Int. Pub. No. WO 2003077077A2 (03/077077) to Kirk Sanford ("Sanford")
EX-1005	U.S. Patent No. 6,963,660 to Yoshihiro Tsukamura and Takeshi Funahashi ("Tsukamura")
EX-1006	Declaration of Stuart Lipoff Regarding Invalidity of U.S. Patent No. 8.620,039
EX-1007	Curriculum Vitae of Stuart Lipoff
EX-1008	European Patent Pub. No. EP 0881608A1 to Walter Leu ("Leu Original")
EX-1009	Certified English Translation of European Patent Pub. No. EP 0881608A1 to Walter Leu ("Leu")
EX-1010	U.S. Patent No. 5,790,674 to Robert C. Houvener and Ian P. Hoenisch ("Houvener")

EX-1011	U.S. Patent No. 5,956,415 to McCalley *et al.* ("McCalley")
EX-1012	Claim Construction Order in *CPC Patent Technologies Pty Ltd v. Apple Inc.*, WDTX-6-21-cv-00165-ADA, Dkt. No. 76 ("Apple CC Order")
EX-1013	Joint Claim Construction Statement in *CPC Patent Technologies Pty Ltd v. Apple Inc.*, WDTX-6-21-cv-00165-ADA, Dkt. No. 57 ("Apple Joint CC Statement")
EX-1014	Excerpts from Bloomsbury English Dictionary, 2nd Edition (2004)
EX-1015	Excerpts from The Chambers Dictionary, 4th Edition (2003)
EX-1016	CPC Publicly Filed Infringement Allegations Against Apple regarding U.S. Patent No. 8,620,039
EX-1017	World Intellectual Property Organization (WIPO) Int. Pub. No. WO 2001022351A1 (01/022351) to Gerald R. Black ("Black")
EX-1018	World Intellectual Property Organization (WIPO) Int. Pub. No. WO 2004055738A1 (04/055738) to Svein Mathiassen and Ivar Mathiassen ("Mathiassen")
EX-1019	Excerpts from Algorithms + Data Structures = Programs, Niklaus Wirth (1976) ("Wirth")
EX-1020	Excerpts from The Art Of Computer Programming (Second Edition), Volume 1 Fundamental Algorithms (1973) ("Knuth Vol. 1")

EX-1021	Excerpts from The Art Of Computer Programming, Volume 3 Sorting and Searching (1973) (“Knuth Vol. 3”)
EX-1022	Perfect Hashing Functions: A Single Probe Retrieving Method for Static Sets, Renzo Sprugnoli (1977) (“Sprugnoli”)

I. INTRODUCTION

Petitioners request *Inter Partes* Review ("IPR") of claims 3-12 and 15-18 (the "Challenged Claims") of U.S. Patent No. 8,620,039 ("'039 Patent," EX-1001), purportedly owned by CPC Patent Technologies Pty Ltd. ("Patent Owner"). This petition in IPR2022-01094 is being filed concurrently with IPR2022-01093, together challenging all claims of the '039 Patent. Petitioners request that the schedule, discovery, and hearing of these two IPRs be combined.

II. MANDATORY NOTICES

Real Party-in-Interest: The real parties-in-interest are related entities **ASSA ABLOY AB**, **ASSA ABLOY Inc.**, and its wholly owned subsidiaries **ASSA ABLOY Residential Group, Inc.**, **August Home, Inc.**, **HID Global Corporation**, and **ASSA ABLOY Global Solutions, Inc**. ASSA ABLOY AB is the ultimate parent of all parties-in-interest. None of the entities mentioned in the Related Matters section below were involved in or offered any assistance to the Real-Parties-in-Interest with respect to this IPR.

Related Matters: The '039 Patent has not been asserted against Petitioners in litigation. Petitioners have filed a declaratory judgment action against Patent Owner and Charter Pacific Corporation Ltd. regarding non-infringement of U.S. Patent No. 9,665,705, U.S. Patent No. 9,269,208, and the '039 Patent in *ASSA*

ABLOY AB, et al. v. CPC Patent Technologies Pty Ltd., et al., No. 3-22-cv-00694 (D. Ct.). The '039 Patent was asserted against Apple, Inc. in *CPC Patent Technologies Pty Ltd v. Apple Inc.*, No. 5:22-cv-02553-NC (N.D. Cal., San Jose Division), which was filed on February 23, 2021.[1] To the best of Petitioners' knowledge, the '039 Patent has not been asserted against other parties.

The '039 Patent was challenged in IPR2022-00600, filed by Apple Inc. on February 23, 2022. The IPR is pending pre-institution.

Lead Counsel: Dion Bregman (Reg. No. 45,645); Back-up Counsel: Andrew Devkar (Reg. No. 76,671) and James J. Kritsas (Reg. No. 71,714).

Service: Service of any documents may be made on Morgan, Lewis & Bockius LLP, 1400 Page Mill Road, Palo Alto, CA, 94304 (Telephone: 650.843.4000; Fax: 650.843.4001).

Petitioners consent to e-mail service at: HID-IPRs@morganlewis.com

III. IDENTIFICATION OF CLAIMS AND GROUNDS

'039 Patent: This patent was filed on **August 10, 2006** and has an earliest possible priority date of August 12, 2005. It is subject to the pre-AIA provisions of

[1] *See also* EX-1016.

35 U.S.C. § 102.

Sanford: WIPO Pub. No. WO 2003077077A2 titled "Pin-less card transaction using user image" to Kirk Sanford ("Sanford," EX-1004), was filed March 6, 2003 and published **September 18, 2003**, and is prior art under §102(b).

Hsu: European Patent Pub. No. EP 0924655A2 titled "Controlled access to doors and machines using fingerprint matching" to Shi-Ping Hsu, Bruce W. Evans, Arthur F. Messenger, Denes L. Zsolnay ("Hsu," EX-1003), was filed November 2, 1998 and published **June 23, 1999**, and is prior art under §102(b).

Tsukamura: U.S. Patent No. 6,963,660 titled "Fingerprint collating device and fingerprint collating method" to Yoshihiro Tsukamura and Takeshi Funahashi ("Tsukamura," EX-1005), was filed **August 16, 2000** and granted November 8, 2005, and is prior art under §102(e).

Leu: European Patent Pub. No. EP 0881608A1 titled "Card reading device and method to initiate an event in such a device" to Walter Leu ("Leu," EX-1008 and EX-1009), was filed May 25, 1997 and published **December 2, 1998**, and is prior art under §102(b).

Houvener: U.S. Patent No. 5,790,674 titled "System, method and computer program product for allowing access to enterprise resources using biometric devices" to Robert C. Houvener and Ian P. Hoenisch ("Houvener," EX-1010), was filed July 19, 1996 and granted **August 4, 1998**, and is prior art under §102(b).

McCalley: U.S. Patent No. 5,956,415 titled "Enhanced security fingerprint sensor package and related methods" to Karl W. McCalley, Steven D. Wilson, Dale R. Setlak, Nicolaas W. Van Vonno, Charles L. Hewitt ("McCalley," EX-1011), was filed January 26, 1996 and granted **September 21, 1999**, and is prior art under §102(b).

Petitioners request that the Board find each of the Challenged Claims invalid on the following grounds:

Ground	Prior Art	Statutory Basis	Claims
1	Sanford and Hsu	§103	3, 4, 6-11, 15, 16, and 18
2	Sanford, Hsu, and Tsukamura	§103	3, 4, 6-11, 15, 16, and 18
3	Sanford, Hsu, and Leu	§103	5
4	Sanford, Hsu, Tsukamura, and Leu	§103	5
5	Sanford, Hsu, and Houvener	§103	12
6	Sanford, Hsu, Tsukamura, and Houvener	§103	12
7	Sanford, Hsu, and McCalley	§103	17
8	Sanford, Hsu, Tsukamura, and McCalley	§103	17

IV. CERTIFICATION AND FEES

Petitioners certify that the '039 Patent is available for IPR and that Petitioners are not barred or estopped from requesting this IPR on the grounds identified herein.

Any additional fees may be charged to Deposit Account No. 50-0310 (Order No. 117139-0008).

V. BACKGROUND

A. The '039 Patent

The '039 Patent describes authentication using both a user's card—such as a credit card, smart card, or key-fob—and the "user's biometric signature." EX-1001, Abstract, 1:33-58. For example, the process can be used for authentication at an "Automatic Teller Machine (ATM)" for cash withdrawal. *Id.*, 9:53-59; EX-1006, ¶27.

Figure 3 (below) provides a block diagram of the system, which includes a verification station 127 (yellow box) that receives a user's card information (*e.g.,* information on the credit card) via a "card device reader 112" (blue) and biometric signature (*e.g.,* a fingerprint) via a "biometric reader 102" (red).[2] EX-1001, 7:50-

[2] Emphasis/coloring added throughout.

53. The submitted biometric signature is compared against the biometric signature associated with the card information that is stored in the memory 124 [green]. *Id.*, 7:53-56.

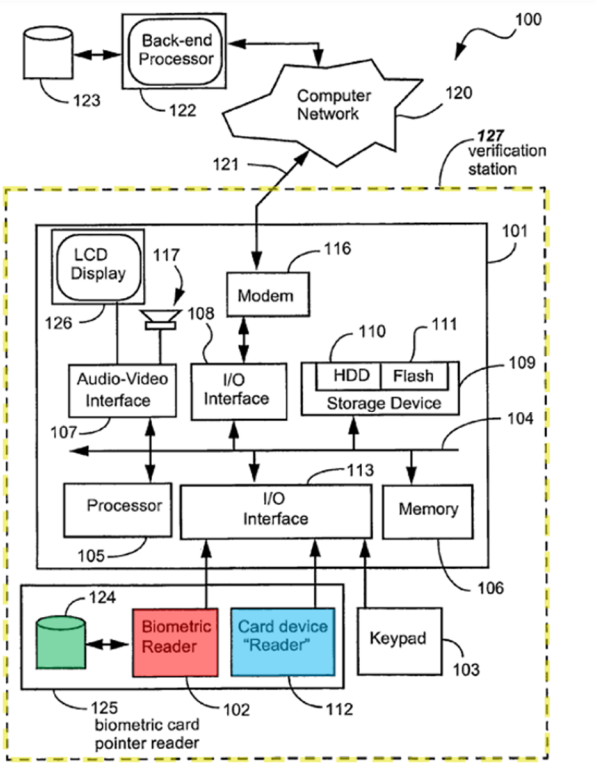


Fig. 3

EX-1001, Fig.3; EX-1006, ¶28.

As illustrated in Figure 4 below, "the card data 604 [yellow] acts as the memory reference which points, as depicted by an arrow 608 [red], to a particular memory location at an address 607 [blue] in the local database 124" in the verification station of Figure 3. *Id.*, 7:31-35. As a result, checking is efficient because only a specific biometric signature is checked, and "[t]here is no need to search the entire database 124 to see if there is a match." *Id.*, 8:34-41.

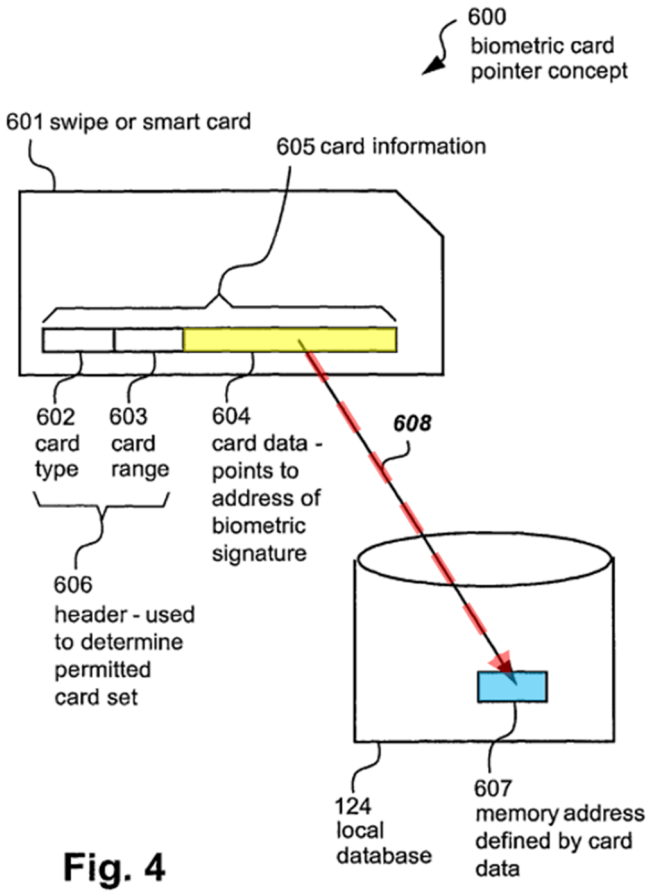


Fig. 4

EX-1001 Fig.4; EX-1006, ¶29.

In finding claim 1 allowable, the Examiner indicated that "[n]one of the prior art teaches or suggests **defining a memory location in a local memory external to card** in dependence **on information received from the card** and when **that memory location is determined to be unoccupied**, **storing** a received **biometric signature** therein." EX-1002, 292. The Examiner further indicated that "none of the prior art teaches or suggest that a verification determines if card information provided to a verification station has previously been provided to that

verification station." *Id.* The claims were allowed without prior art rejections. *Id.*, 291-292, 318. The Examiner was not aware of any of the prior art references herein during prosecution.

VI. LEVEL OF SKILL

A person having ordinary skill in the art ("POSITA") at the time of the alleged invention 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. EX-1006, ¶26.

VII. CLAIM CONSTRUCTION

A. Terms to be Construed

1. Card Information "Defining" / "Defines" a Memory Location

The claims include the following limitation relating to card information defining a memory location:

Claims	Limitation
Independent claims 3, 15 and 18	"**memory location defined** by the provided card information"

This limitation is susceptible to two different interpretations regarding what it

means for the "**memory location**" to be "**defined**" by the card information. EX-1006, ¶43.

First interpretation: a memory location is somehow determined from (or is dependent on) the card information ("First Construction"). Under this interpretation, the system can look up or otherwise determine a specific memory location from a user's card information. EX-1006, ¶44.

Second interpretation: a memory location is specified by the card information itself ("Second Construction"). Under this interpretation, the card information itself must specify the physical memory address where the user's biometric signature is stored, without the need to look up the memory address in a database or other data structure. EX-1006, ¶45.

Petitioners believe the Second Construction was intended by the patentee and should be adopted.[3] The specification, as reflected in Figure 4 (below), states that "**the card data 604** [yellow] acts as the **memory reference** which **points**, as depicted by an arrow 608 [red], **to a particular memory location** at an **address 607** [blue] in the local database 124" in the verification station. *Id.*, 7:31-35.

[3] Patent Owner appears to be asserting infringement claims under the First Construction. *See* EX-1016, p.3.

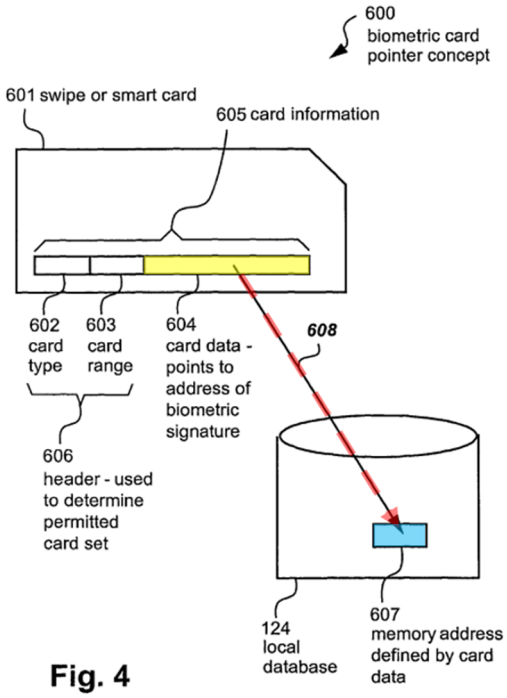


Fig. 4

EX-1001 Fig.4. Moreover, from the "Summary of Invention" and throughout the specification, and in the preamble of various claims, the '039 Patent consistently refers to a "biometric card *pointer* system," *i.e.*, the card acts as a *pointer* (specifies the physical memory address) to the memory location where the user's biometric signature is stored. *E.g.*, EX-1001, claims 1, 13, 14; 2:51-52 ("SUMMARY…Disclosed are arrangements, referred to as Biometric Card *Pointer* (BCP) arrangements or systems…"); 3:46-47 ("biometric card *pointer* system"); 5:17 (same); 5:51 ("FIG. 4 illustrates the biometric card *pointer* concept"); 5:52 ("FIG. 5 is a flow chart of a process for using the biometric card *pointer* arrangement"); 6:31-35 ("The verification station [] comprises…a biometric card *pointer* reader…"); EX-1006, ¶46.

Therefore, a POSITA would have understood that the user's card information itself specifies the physical memory address (such as by acting as a pointer) to the user's biometric signature. EX-1006, ¶47.

The '039 Patent claims are unpatentable under either interpretation. Under the First Construction, the claims are unpatentable under Grounds 1, 3, 5, and 7 (Sanford + Hsu). Under the Second Construction, the claims are unpatentable under Grounds 2, 4, 6, and 8 (Sanford/Hsu + Tsukamura). EX-1006, ¶48.

B. Means-Plus-Function Limitations

Petitioners propose constructions for the means-plus-function limitations in their respective Argument sections below.

Additionally, claim 18 recites "code for" instead of "means for" for some limitations. In the context of these claims and the intrinsic evidence, "code for" is an equivalent recitation for "means for." *See also Cypress Lake Software, Inc. v. Samsung Electronics Am., Inc.*, No. 6:18-cv-00030, Dkt. 174, p36 (E.D. Tex. May 10, 2019) (finding that "'code for' does not connote sufficiently definite structure" and that "the term "code for" is defined only by the function that it performs."). The '039 Patent's otherwise identical language for some "code for" and "means for" terms further confirms that they should be treated equivalently. *Id.* Therefore, Petitioners submit that these "code for" terms are means-plus-function terms under *Williamson* and should be treated the same way as "means for" terms. Petitioners

likewise propose constructions for the "code for" terms in their respective Argument sections.

C. Other Previously-Agreed-On Terms

Patent Owner and Apple agreed to constructions for the following terms, which are not material to unpatentability. EX-1006, ¶¶55-57.

1. "dependent upon"

"plain and ordinary meaning, defined as 'contingent on or determined by'." EX-1013, p.2.

2. "biometric signature"

"plain and ordinary meaning." EX-1013, p.2.

VIII. ARGUMENT

A. GROUND #1: Claims 3, 4, 6-11, 15, 16, and 18 are Rendered Obvious by Sanford and Hsu

1. Claim 3[4]

Preamble 3[P]

Sanford discloses "**a method of securing a process** [*e.g.,* Automated Cash Machine (ACM) cash withdrawal or a PIN-less credit card transaction] **at a**

[4] A full claim listing can be found in the Appendix.

verification station [*e.g.,* Sanford's ACM]." EX-1006, ¶¶268-272.[5]

Just like the '039 Patent, which discloses that a user needs to be verified to access a cash withdrawal process at an ATM (EX-1001, 9:50-59), Sanford discloses "[a]n **automated cashier machine (ACM)** [] that offers a **secure** and convenient way for users to **access cash** from their card without using a PIN." EX-1004, ¶0006. Specifically, "the ACM verifies the identifying image of the user to an image of the user in a profile…using facial biometrics." *Id.*; EX-1006, ¶269.

Sanford illustrates an exemplary system in Figure 1:

[5] For brevity, citations to the expert declaration often appear at the end of paragraphs but apply to the full paragraph in which they are cited.

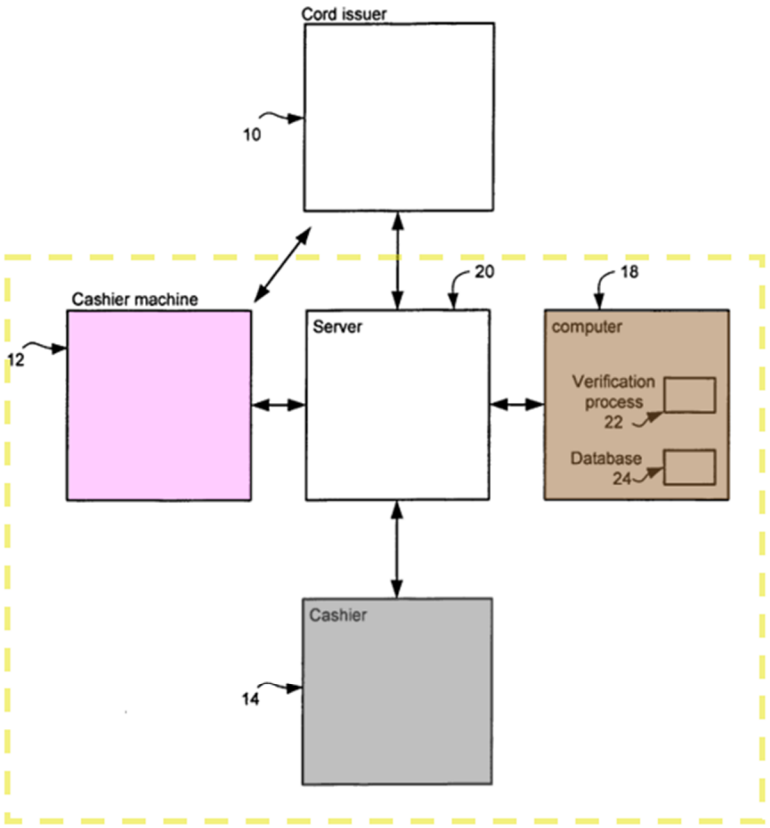


Fig. 1

EX-1004, Fig.1. As shown, the system in the yellow box includes an "automated cashier machine (ACM) 12" (pink), a "server 20," an "ACM computer system 18" (brown), and an "cashier system 14" grey). *Id.*, ¶0014. Sanford further discloses that "ACM 12 [pink], cashier system 14 [grey], …and ACM computer system 18 [brown] are preferably coupled directly and/or indirectly to each other through the

server 20 [grey]."[6] *Id.*, ¶0015; EX-1006, ¶270.

Unless otherwise specified, an ACM indicated by the yellow box (as shown in Fig.1 above), is referred to as Sanford's ACM. Thus, Sanford's ACM includes at least "ACM 12 [that] includes a card reader, a picture taking device, a display device, an input device, and a cash dispenser," a "cashier system 14" that may "include a human operator," and "ACM computer system 18" that "may be any system capable of verifying the picture taken by ACM 12." EX-1004, ¶¶0015-17. "If the [] image is verified, the amount for withdrawal is dispersed [*sic*]." *Id.*, ¶0006. Fig.2 shows "a method for conducting a PIN-less credit card transaction" performed by Sanford's ACM. *Id.*, ¶0024.

[6] A POSITA would have understood that these components of Sanford's system may be present at the same physical facility. EX-1006, ¶270.

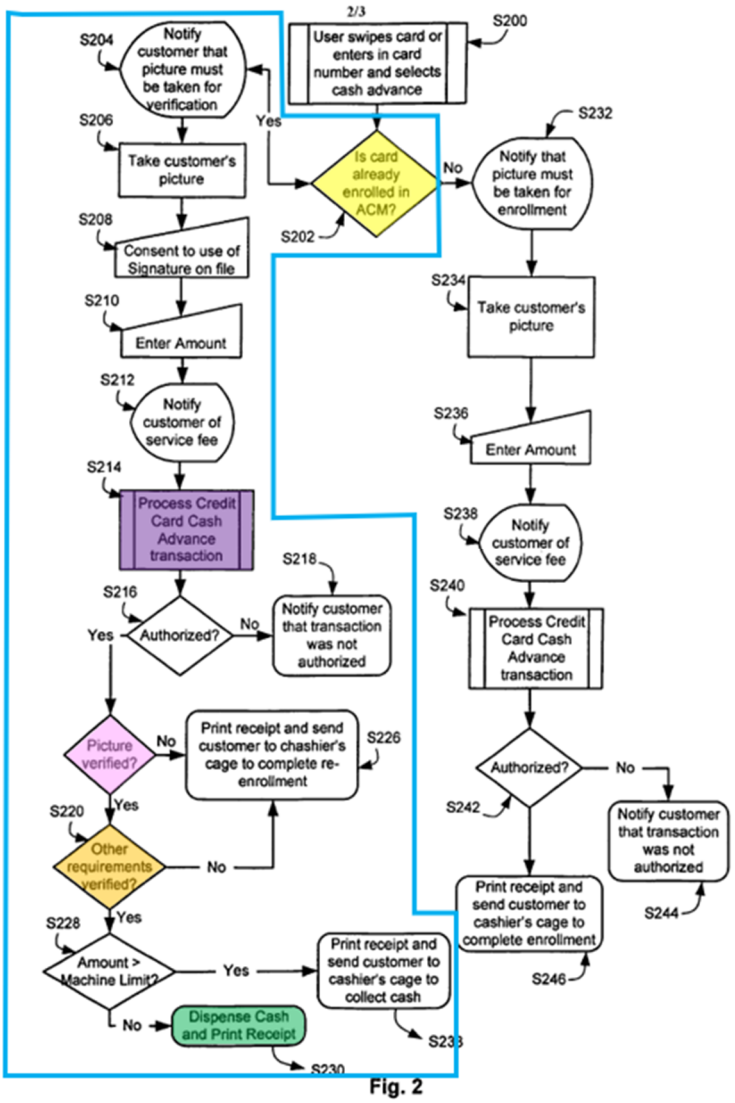


Fig. 2

EX-1004, Fig.2. The process (blue box) includes a series of verification steps. As shown in Figure 2, Sanford discloses that cash dispensing occurs after a user is verified and therefore is a "secured process." *E.g., id*, ¶0025, ¶0028, ¶0031; EX-1006, ¶271.

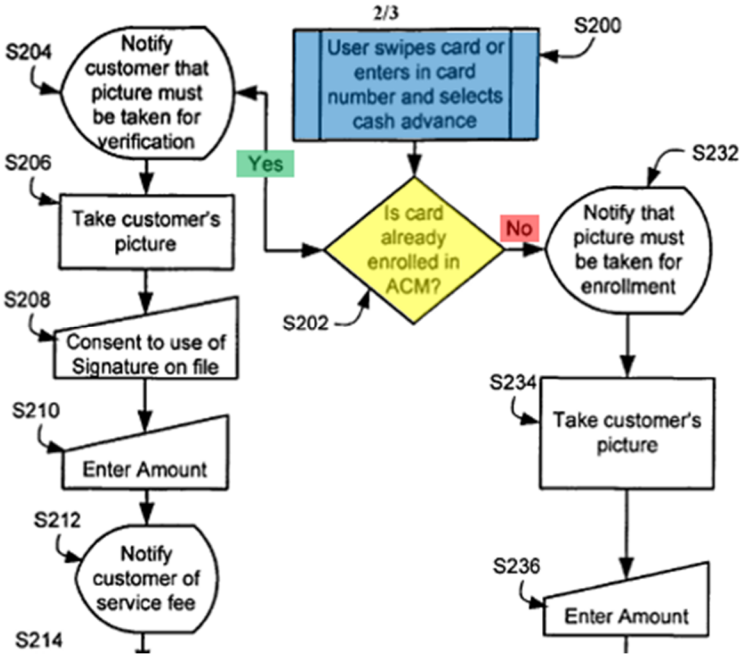
Limitation 3[A]

Sanford discloses "**(a) providing card information** [*e.g.,* credit card account number] **from a card device** [*e.g.,* credit card] **to a card reader** [*e.g.,* card reader] **in the verification station** [*e.g.,* Sanford's ACM]." EX-1006, ¶¶273-277.

The '039 Patent provides that a card device may be of "various types," *e.g.*, a "standard credit card," a "smart card," or a "wireless 'key-fob'." EX-1001, 1:21-23; 1:33-58. Sanford discloses a standard "credit card." EX-1004, Title, ¶0014.

Sanford also discloses that ACM 12 includes a card reader that "may be a magnetic strip reader capable of reading cards with a magnetic strip such as…credit cards." EX-1004, ¶0016. As mentioned for Limitation 3[P], Sanford's ACM includes ACM 12 and its card reader is capable of reading credit cards. EX-1006, ¶275, ¶¶268-272.

Sanford further discloses providing card information from a credit card to the disclosed card reader.



EX-1004, Fig.2 (excerpted). As shown, in step S200 (blue), "[t]he user may begin the process by inserting or swiping a credit card into the credit card reader." *Id.*, ¶0024. The process then determines in the next step S202 (yellow) "if the **credit card account number** of the user is enrolled to use the PIN-less credit card system." *Id.*, ¶0025. Thus, a POSITA would have understood that the credit card account number is provided to the card reader by "inserting or swiping" the card. EX-1006, ¶276.

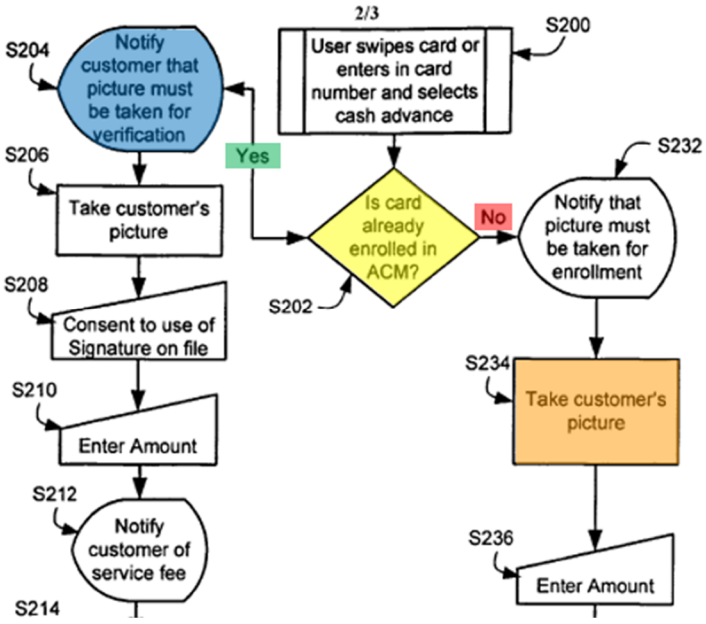
Limitation 3[B]

Sanford discloses "**(b) inputting a biometric signature** [*e.g.,* picture, or fingerprint] **of a user** [*e.g.,* customer] **of the card device** [*e.g.,* credit card] **to a biometric reader** [*e.g.,* camera or fingerprint reader] **in the verification station**

[Sanford's ACM]." EX-1006, ¶¶278-281.

Sanford discloses that "ACM 12 includes… a picture taking device" that "may be any device capable of taking a picture such as a digital camera, traditional camera, or Internet web camera." EX-1004, ¶0016. The picture taken may be verified by "an algorithm based on facial **biometrics**." *Id.*, ¶0019. According to the '039 Patent, a biometric signature may be of various types, such as "fingerprint, **face**, iris, or other unique signature." EX-1001, 7:45-47. Therefore, the user's picture in Sanford is a biometric signature, and the picture taking device is a biometric reader. Like the '039 Patent, Sanford recognizes that in addition to "facial image" (or "faceprint"), other biometric signatures including "iris, voice signature, and **fingerprint** technology" may also be used for verification. EX-1004, ¶0020. A POSITA 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. Thus, Sanford discloses a biometric reader for reading a biometric signature. EX-1006, ¶279.

Moreover, as shown in Fig. 2, if the card is already enrolled, "an identifying image is taken…in step S204 [blue]." EX-1004, ¶0026.



EX-1004, Fig.2 (excerpted). Alternatively, "if the card is not enrolled,… a picture of the customer is [also] taken" in step S234 (orange). *Id.*, ¶0033. Thus, regardless of whether the card is enrolled, the customer must input her biometric signature (*e.g.,* picture, or fingerprint) to proceed. EX-1006, ¶280.

Limitation 3[C]

Sanford discloses "**(c) determining if the provided card information** [*e.g.,* credit card account number] **has been previously provided to** [*e.g.,* enrolled in] **the verification station** [*e.g.,* Sanford's ACM]." EX-1006, ¶¶282-285.

The '039 Patent does not explain what qualifies as "ha[ving] been previously provided to the verification station" other than repeating the claim language in the specification. EX-1001, 4:5-6, 4:14-15; 4:32-33, 4:60, 5:3-4. However, as shown

in the following limitations of claim 3, "if the provided card information **has not been previously provided** to the verification station," "the inputted biometric signature [is stored] in a memory." *Id*., Cl. 3. This describes an enrollment action. "[I]f the provided card information has been previously provided to the verification station," "the inputted biometric signature [is compared] to the biometric signature stored in the memory." EX-1001, Cl. 3. This describes the verification action. Therefore, a POSITA would have understood that "determining if the provided card information has been previously provided to the verification station" means determining if the card has been previously enrolled, which Sanford discloses. As shown in Figure 2, 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-1004, ¶¶0024-25.

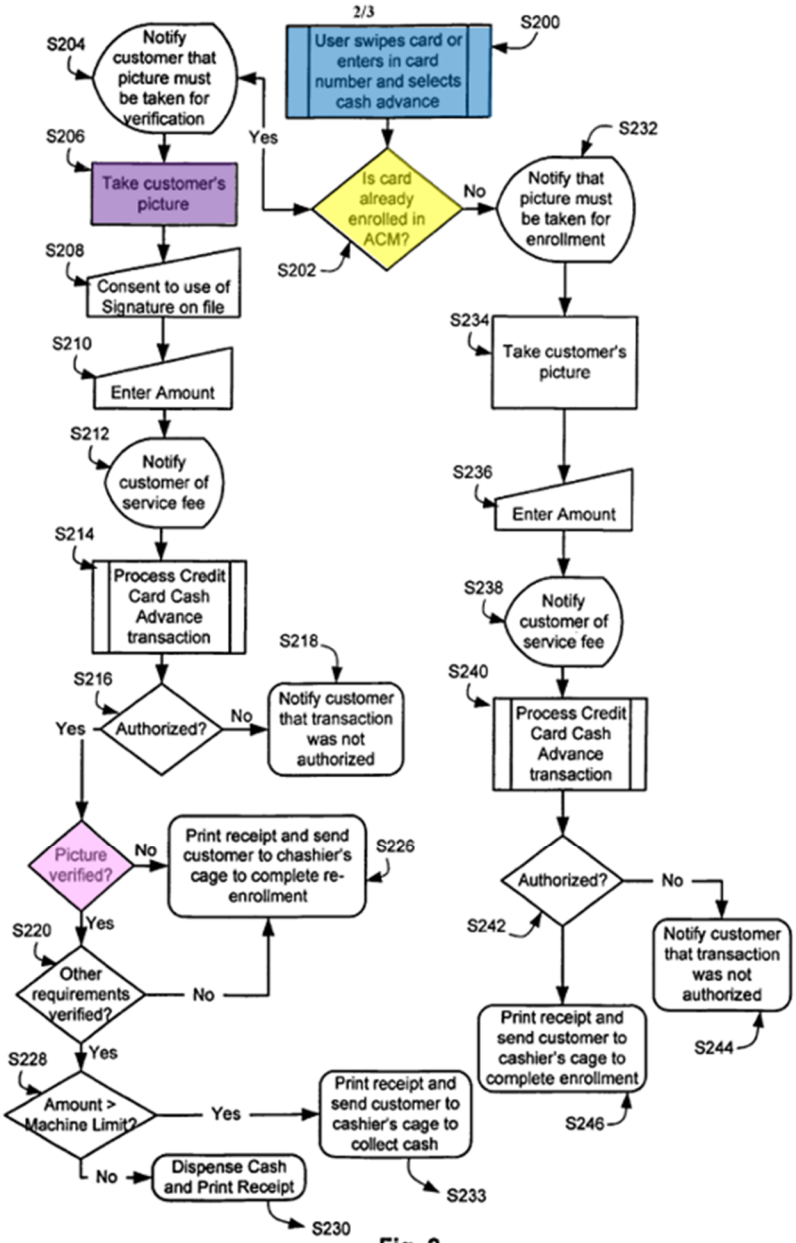


Fig. 2

EX-1004, Fig.2. "**If** the **card is not enrolled**, the **user is enrolled** in a process hereinafter described." *Id.*, ¶0025. "If the card is enrolled, …an identifying image

is taken" at step S206 (purple) for verification at step S219 (pink).[7] *Id.*, ¶0026, ¶0030; EX-1006, ¶283.

Limitation 3[D(P)+D(1)]

Sanford in view of Hsu discloses "**if the provided card information** [*e.g.,* Sanford's credit card account number] **has not been previously provided to** [*e.g.,* not enrolled in] **the verification station** [*e.g.,* Sanford-Hsu system], **(da) storing the inputted biometric signature** [*e.g.,* picture/fingerprint] in a memory [*e.g.,* Sanford's or Hsu's local memory] **at a memory location defined by the provided card information** [*e.g.*, memory location in Hsu's database]." EX-1006, ¶¶286-294.

Sanford discloses "determining if the provided card information has been previously provided to the verification station." *See* Limitation 3[C]. Sanford also discloses the "inputted biometric signature" (*e.g.,* picture, or fingerprint). *See*

[7] Although Sanford does not label step S219 in Fig. 2, the step in pink is the step S219 described in the specification. *See* EX-1004, ¶0030. Further, because the specification does not discuss any step labeled S217, and the step colored in pink is the only unlabeled step between S218 and S220, a POSITA would have understood that the step colored in pink is step S219. EX-1006, ¶284.

Limitation 3[B]; EX-1006, ¶287, ¶¶278-285.

Sanford further discloses that "if the provided card information has not been previously provided to the verification station" (*i.e.,* if the card is not enrolled), the picture (or fingerprint) is stored. EX-1004, ¶0025 ("[I]f the card is not enrolled, the user is enrolled in a process hereinafter described."). As shown in Figure 2, after it is determined that the card is not enrolled at step S202 (yellow), the customer's picture (or fingerprint) is taken at step S234 (purple), and the customer is instructed to complete enrollment at step S246 (orange). EX-1004, ¶¶0024-37.

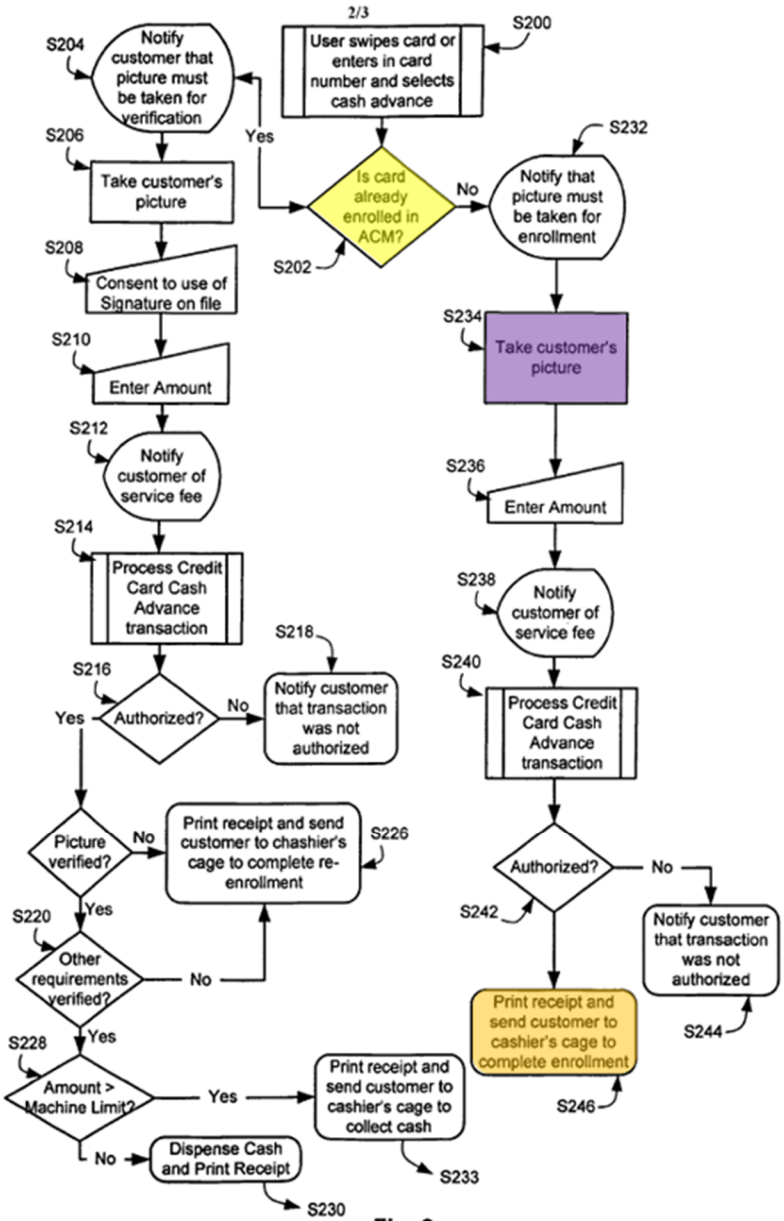


Fig. 2

EX-1004, Fig.2. "The cashier's PC then communicates to ACM computer system 18… to receive the user's image and any other relevant data associated with the original transaction from **ACM database 24**." *Id.*, ¶0040. As shown in Fig.1, ACM database 24 (green) is part of ACM computer system 18 (brown), which is part of Sanford's ACM (yellow):

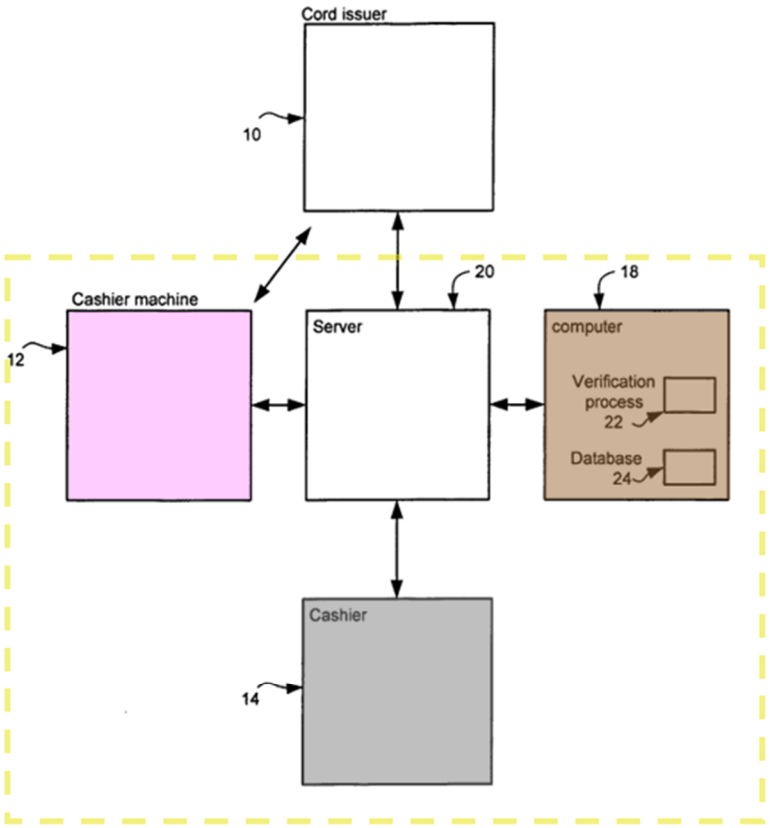


Fig. 1

EX-1004, Fig.1. Therefore, since the cashier's PC retrieves the user's image from ACM database 24, a POSITA would have understood that before such retrieval, the user's image must have been stored in ACM database 24. EX-1006, ¶288.

Moreover, Sanford discloses a verification process 22 (blue) "verify[ing] that the picture taken by ACM 12 matches a picture in database 24." EX-1004, ¶0018; *see also* ¶0021. A POSITA would have understood that such verification process would happen only if the customer's picture (or fingerprint) has been

stored in database 24 during an enrollment process. Therefore, if a customer's credit card were not enrolled in Sanford's ACM, her picture/fingerprint would be stored in database 24 (*i.e.,* in memory) as part of her enrollment process. EX-1006, ¶289.

Although a user's card number is associated with the user's biometric signature (*e.g.,* picture/fingerprint), both being part of a user's profile, Sanford does not provide specific details about how the user's picture or fingerprint is stored in the database. *See* EX-1004, ¶0021; *see also* ¶0018 ("**The picture may be part of a profile** that is verified. **A profile may include an image of the user** or a corresponding entry representing the image that is used to verify the picture taken by ACM 12. Additionally, **a profile may include**…**credit card number**."); EX-1006, ¶290.

Hsu, however, discloses a specific implementation of a database where a user/account/employee number is associated with a biometric signature (*e.g.,* fingerprint). Hsu discloses that the user/account/employee number "is stored in the database 44 in association with the user's fingerprint image data." EX-1003, ¶0026, ¶0020. "The 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." *Id.*, ¶0020; Fig.4; EX-1006, ¶291.

Therefore, a POSITA 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 (*see* full motivation-to-combine after claim 3), 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.

A POSITA 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. EX-1003, ¶0026; ¶0020 ("The 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"). Thus, given a user/card number, Hsu looks up that number in its fingerprint database 44 and determines the specific memory location for storing the associated fingerprint. Therefore, the "memory location" for storing the biometric signature (*e.g.,* fingerprint) the Sanford-Hsu system is "defined by the provided card information." EX-1006, ¶293.

Limitation 3[D(P)+D(2)]

Sanford discloses "**if the provided card information** [*e.g.,* credit card account number] **has not been previously provided to** [*e.g.,* not enrolled in] **the**

verification station [*e.g.*, Sanford-Hsu system], … **(db) performing the process** [*e.g.,* antecedent process from preamble, here Sanford's cash dispensing] **dependent upon the received card information** [*e.g.,* Sanford's credit card account number]." EX-1006, ¶¶295-299.

Notably, "***the*** process" in this limitation is the "process" recited in the preamble. As shown in Figures 5 and 7 of the '039 Patent, such "process" refers to the transaction process (step 403 in Figure 7). EX-1001, 9:62-10:7; Figs.5,7; EX-1006, ¶296.

Sanford discloses that "if the provided card information has not been previously provided to the verification station" (*i.e.,* if the card is not enrolled), the user is enrolled and then a cash dispensing process is performed. As shown in Fig. 2, after determination that the card is not enrolled at step S202 (yellow), "the customer is given instructions [at step S246 (orange)] to proceed to cashier system 14 [which is part of Sanford's ACM] to complete enrollment." EX-1004, ¶0037.

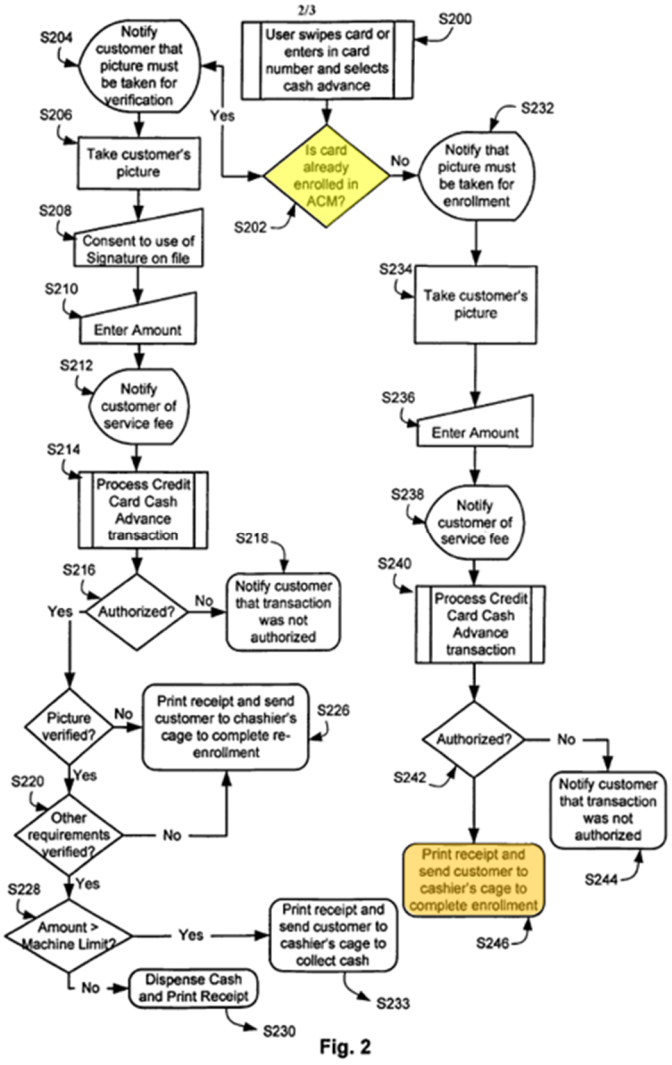


Fig. 2

EX-1004, Fig.2. "The user may then be dispensed the money for the transaction [at] the casino cage upon showing of a valid identification, such as a driver's license, etc," *i.e.,* the claimed process in the preamble. *Id.*, ¶0037; EX-1006, ¶297.

Sanford also discloses that the cash dispensing process is "dependent upon the received card information" (the user's credit card account number). The user uses her card to withdraw money, and a POSITA would have understood that the cash dispensed is debited from her account associated with her card number.

Therefore, Sanford discloses that if the provided card information (*i.e.,* credit card number) has not been previously provided to the verification station" (*i.e.,* if the card is not enrolled), the card/user is enrolled and then a cash dispensing process dependent upon the card number is performed. EX-1006, ¶298.

Limitation 3[E(P)+E(1)]

Sanford in view of Hsu discloses "**if the provided card information** [*e.g.,* Sanford's credit card account number] **has been previously provided to** [*e.g.,* enrolled in] **the verification station** [*e.g.,* Sanford-Hsu system]; **(ea) comparing the inputted biometric signature** [*e.g.,* picture/fingerprint] **to the biometric signature** [*e.g.,* picture/fingerprint] **stored in the memory** [*e.g.,* Hsu's local memory] **at the memory location defined by the provided card information** [*e.g.*, memory location in Hsu's database]." EX-1006, ¶¶300-302.

Sanford discloses "determining if the provided card information has been previously provided to the verification station." *See* Limitation 3[C]. Sanford also discloses that "if the provided card information has been previously provided to the verification station" (*i.e.,* if the card is enrolled), the picture (or fingerprint) is verified at step S219 (pink), as shown in Fig. 2 below.

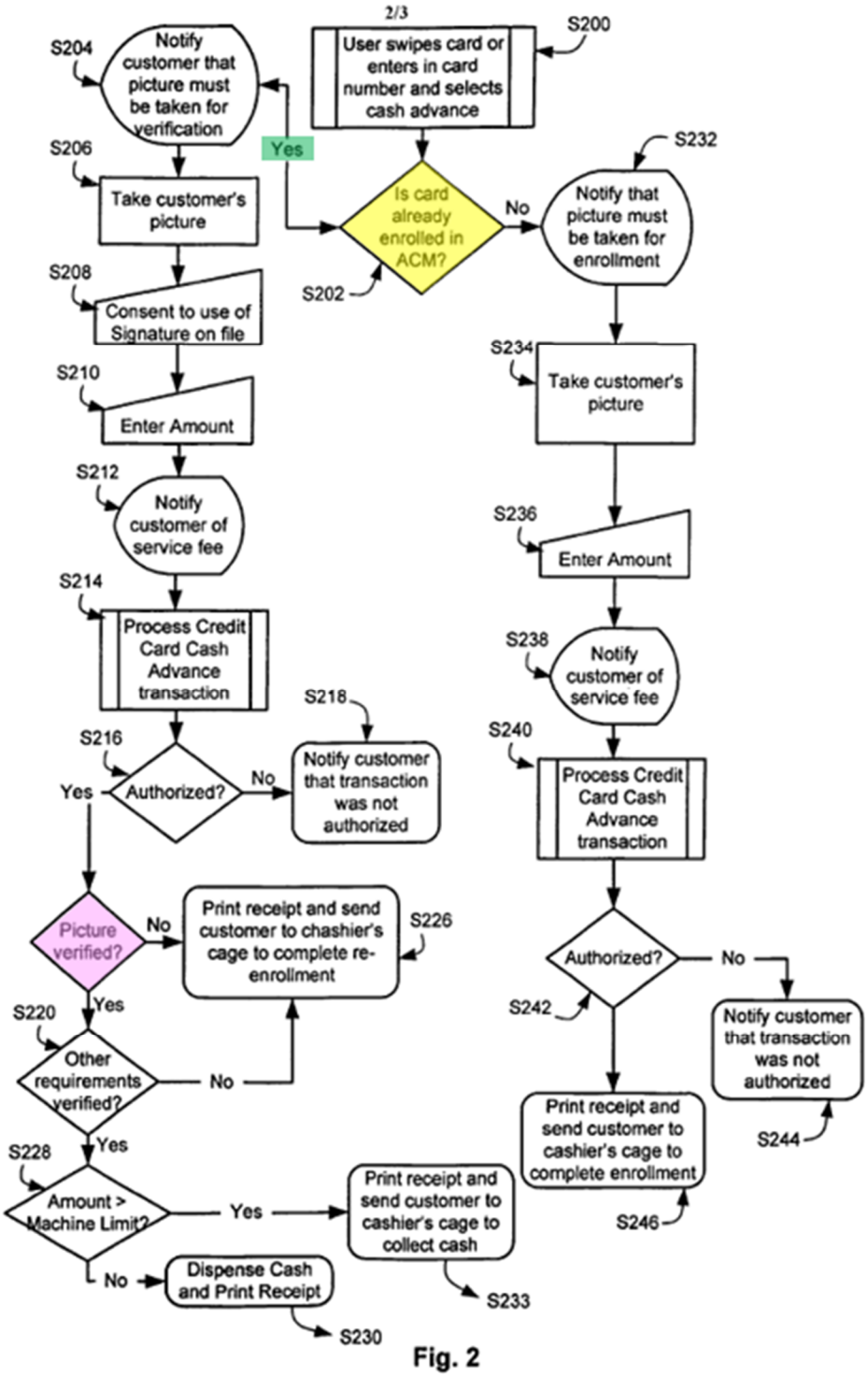


Fig. 2

EX-1004, Fig. 2, ¶0030 ("the process verifies that the identifying image was taken in step S219."). Specifically, "facial biometrics is used to verify the identifying

image that was taken to a user profile on record." *Id.* ¶0030, ¶0019. The "verification process 22 may employ an algorithm based on facial biometrics" and **compares** the **inputted image to a stored picture/fingerprint**. *Id.* ¶0019. As discussed for Limitation 3[D(P)+D(1)], in the Sanford-Hsu system, the stored picture/fingerprint is a biometric signature **stored** "**in** a **memory** [*e.g.,* **Hsu's local memory**] at a memory location defined by the provided card information [*e.g.*, **memory location in Hsu's database defined by Hsu's user number**]," under the First Construction. EX-1006, ¶301, ¶¶282-285, ¶¶286-294.

Limitation 3[E(2)]

Sanford discloses "**if the inputted biometric signature** [*e.g.,* picture/fingerprint] **matches the stored biometric signature** [*e.g.,* picture/fingerprint], **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, ¶¶303-305.

As shown in Figure 2, if the user's picture/fingerprint is verified (pink), *i.e.*, matches the stored picture/fingerprint, Sanford's ACM may dispense cash at step S230 (green) after several intermediate steps. EX-1004, ¶0031.

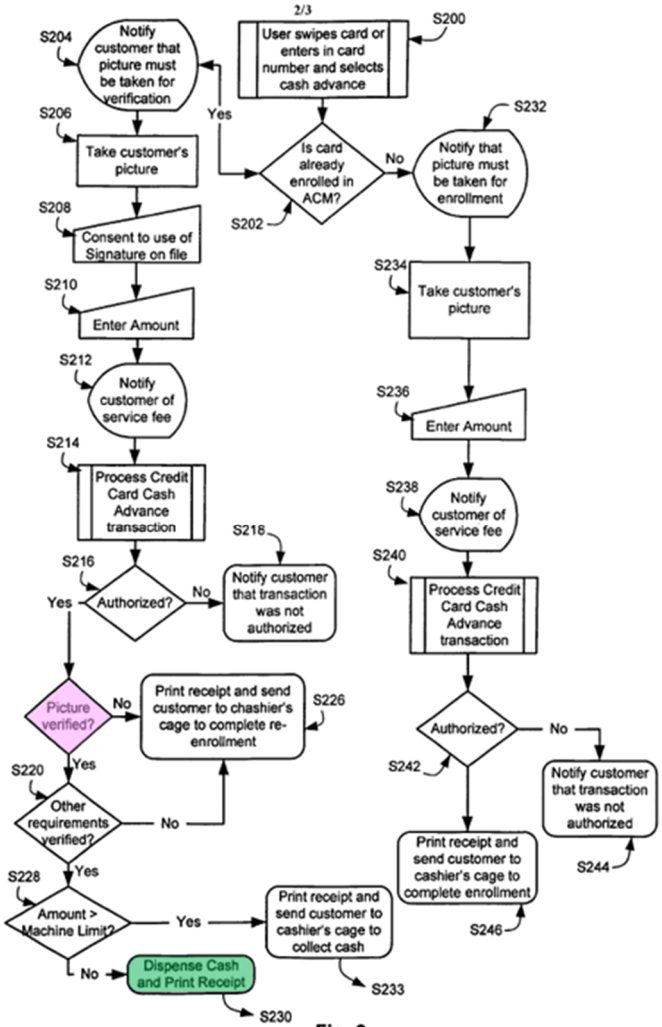


Fig. 2

EX-1004, Fig.2. As discussed for Limitation 3[D(P)+D(2)], cash dispensing is a process dependent upon the received card information. EX-1006, ¶304, ¶¶295-299.

Limitation 3[E(3)]

Sanford discloses "**if the inputted biometric signature** [*e.g.,* picture/fingerprint] **does not match the stored biometric signature** [*e.g.,*

pictures/fingerprints do not match], **not performing the process** [*e.g.,* cash dispensing] **dependent upon the received card information** [*e.g.,* Sanford's credit card account number]." EX-1006, ¶¶306-308.

As shown in Figure 2, if the user's picture/fingerprint is not verified (pink), *i.e.*, does not match the stored picture/fingerprint, "the user is printed out a receipt and given instructions to proceed to the cashier for re-enrollment in step S226 [orange]." EX-1004, ¶0030.

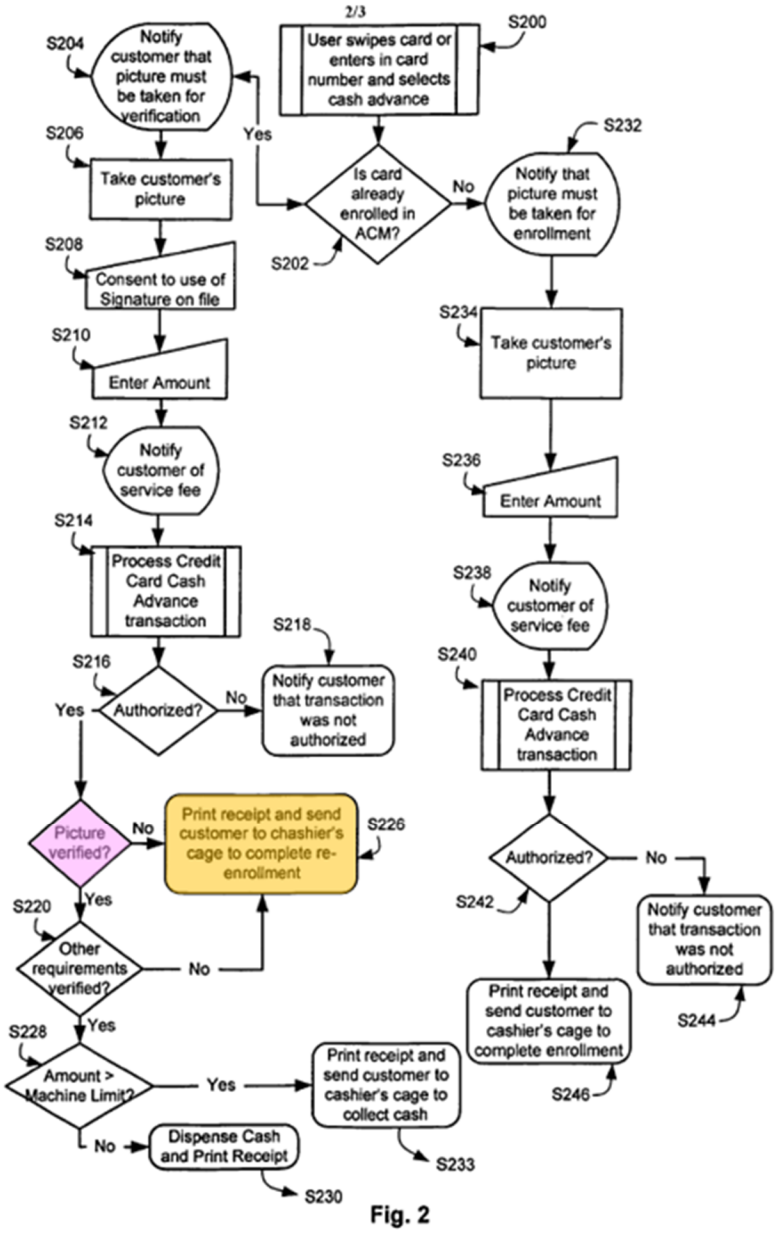


Fig. 2

EX-1004, Fig.2. No cash dispensing process is executed. *See* Preamble 3[P]. As discussed for Limitation 3[D(2)], cash dispensing is a process dependent upon the received card information. EX-1006, ¶307, ¶¶268-272, ¶¶295-299.

Motivation to Combine: Sanford and Hsu

Sanford discloses all limitations in claim 1 except for arguably a specific memory structure with a memory location for storing a picture/fingerprint that is defined by card information. This is disclosed by Hsu. It would have been obvious to modify Sanford's generic database to use Hsu's database and memory structure. EX-1006, ¶309.

The '039 Patent, Sanford, and Hsu are **analogous art** and are in the **same field of endeavor**, *i.e.*, access control with biometric authentication. Both references (and the '039 Patent) are directed to ways of performing efficient biometric authentication, including using fingerprints. Both references (and the '039 Patent) teach authenticating a user by comparing a fingerprint captured by a sensor to a stored fingerprint. EX-1003, Abstract; EX-1004, Abstract. Both 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. EX-1003, ¶¶0018-21. Hsu discloses that the stored fingerprint data is associated with a user number or account number provided by a user's card. EX-1003, ¶0026. Both references (and the '039 Patent) improve 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. EX-1006, ¶310.

A POSITA would have been **motivated** to implement Sanford's generic database 24 as Hsu's database 44. As discussed for Limitation 3[D(P)+D(1)], although Sanford discloses that a user's card number is associated with the user's biometric signature (*e.g.,* picture/fingerprint) in the database, it does not provide specific details about the database's implementation. *See* EX-1004, ¶0021, ¶0018. Hsu describes a specific implementation of such a database where, just like Sanford's credit card account number, Hsu's user/account/employee number is associated with a biometric signature (*e.g.,* fingerprint). 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." *Id.*, ¶0020; *see also* Fig.4; EX-1006, ¶311.

A POSITA would have had a **reasonable expectation of success** in implementing Sanford's database according to Hsu's teachings. A POSITA would have known there are various ways to implement a database suitable for Sanford's system. Indeed, a POSITA would have known that Hsu's database is a logical implementation of Sanford's database which is not described in detail. Sanford discloses that a user's card number is associated with the user's biometric signature (picture/fingerprint). Hsu's database does exactly that. EX-1003, ¶0026 ("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."); Fig.4. Sanford also discloses that the database not only stores a user's biometric signature (picture/fingerprint), but also other "identifying information that uniquely identifies the user, such as a date of birth, driver's license number, passport number, social security number, credit card number, and BIN number of the credit card." EX-1004, ¶0018. Hsu's database also satisfies such requirement. EX-1003, ¶0020 ("The database may also contain other information about the user…"). A POSITA would have understood that implementing Sanford's database as described by Hsu would result in a working system. EX-1006, ¶312.

Therefore, it would have been obvious to implement Sanford's database in view of Hsu. Sanford's credit card numbers and associated pictures/fingerprints would be stored in the database in a table as described by Hsu. Given a card/user number, the system would 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, as required by the First Construction. EX-1006, ¶313.

2. Claim 4

Sanford and Hsu disclose "[a] method according to claim 3, wherein the card

device is ***one of***: **[i]** a card in which the card information is encoded in a magnetic strip; **[ii]** a card in which the card information is encoded in a bar code; **[iii]** a smart card in which the card information is stored in a solid state memory on the smart card; **and [iv]** a key fob adapted to provide the card information by transmitting a wireless signal to the verification station." EX-1006, ¶¶314-317.

Since the preamble recites "one of," only one of the portions [i] to [iv] needs to be disclosed.

Sanford discloses card information "encoded in a magnetic strip." As discussed for Limitation 3[A], Sanford discloses card information, *e.g.*, the user's credit card account number. EX-1004, Title, ¶0014. Sanford also discloses that this card information is encoded in a magnetic strip. EX-1004, ¶0016 ("In a specific embodiment, the 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."); *see also* ¶0040 ("In step B, the cashier swipes or key enters the **credit card** through the card reader on the PC and preferably enters the last four digits of the card number to validate the **magnetic strip card**."). Therefore, a POSITA would have understood the card information in the Sanford-Hsu system (*e.g.,* Sanford's credit card account number) is encoded in a magnetic strip of a card. EX-1006, ¶316. (Although not necessary to satisfy the

claim, Hsu discloses each of [i], [ii], [iii] and [iv] of the claim.[8] *See* EX-1003 ¶0024 (card with "magnetic stripe"); ¶0024 (card with "bar codes"); ¶0024 ("smart card" with "readable memory"); ¶007 (transponder embodiment sending wireless signals). EX-1006, ¶317.)

3. Claim 6

Claim 6 requires "[a] method according to claim 3, 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**," which is disclosed by Sanford and Hsu. EX-1006, ¶¶318-329.

The '039 Patent acknowledges that "outputting at least part of the inputted card information" was known prior to this patent. EX-1001, 1:29-32 ("BACKGROUND…The card information is typically accessed from the card by a corresponding card reader which then **sends the card information to a 'back-end' system** that completes the appropriate transaction or process"). Regardless, Sanford discloses this claim. EX-1006, ¶319.

First, Sanford discloses that "the performance of the process in step[] **(db)**… comprises outputting at least part of the inputted card information from the

[8] Petitioners reserve the right to assert lack of written description in other forums.

verification station." EX-1006, ¶320.

As discussed for Limitation 3[D(P)+D(2)], Sanford discloses "if the provided card information has not been previously provided to the verification station,] (db) performing the process [*e.g.,* cash dispensing] dependent upon the received card information [*e.g.,* Sanford's credit card account number]." EX-1006, ¶321, ¶¶295-299.

Sanford further discloses that the cash dispensing process, performed after it is determined that the card is **not** enrolled, comprises outputting a card account number from Sanford's ACM. EX-1004, ¶0037. For example, Sanford discloses a financial institution 16 (blue) in Figure 1:

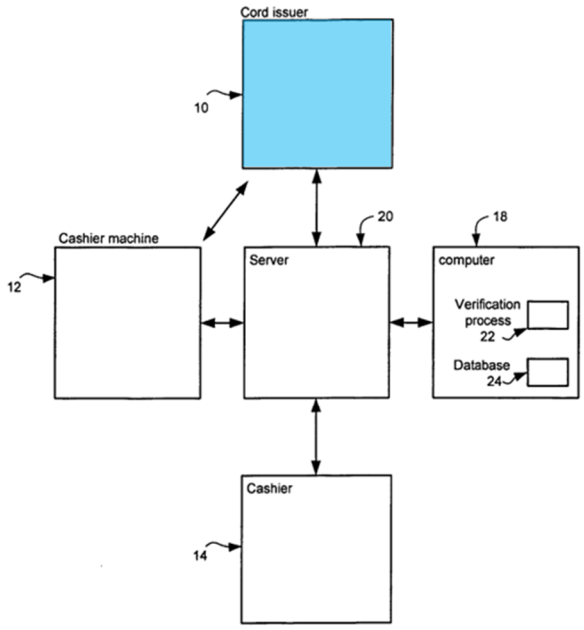


Fig. 1

EX-1004, Fig.1. "Financial institution 16 [blue] may be any institution capable of authorizing a transaction requested by the user…[and] is preferably the issuer of the card the user is using."[9] *Id.*, ¶0023; *see also* ¶0024 ("The PIN-less credit card transaction may be used to **withdraw cash**…credit **from an institution**…from ACM 12."). Therefore, a POSITA 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-1004, ¶0034, Fig.2. If a user is not enrolled, Sanford enrolls the user and then dispenses cash, which requires sending the user's credit card number to the card issuer. EX-1006, ¶¶322-324.

Therefore, Sanford discloses "the performance of the process in step[] (db) [*e.g.,* dispensing money if the card is not enrolled]…comprises outputting [*e.g.,* sending] at least part of the inputted card information [*e.g.,* Sanford's card account number] from the verification station [Sanford-Hsu system]." EX-1006, ¶325.

Second, Sanford discloses "the performance of the process in the step[]… **(eb)** comprises outputting at least part of the inputted card information from the

[9] "Cord issuer 10" in Fig. 1 should have said "Card issuer 10" and refers to "financial institution 16." EX-1004, ¶0014 ("In Fig. 1, a system 10…includes…a financial institution 16…"); ¶0023 ("Institution 16 is preferably the issuer of the card the user is using."); EX-1006, ¶322.

verification station." EX-1006, ¶326.

As discussed for Limitation 3[E(2)], Sanford discloses "if the inputted biometric signature **matches** the stored biometric signature, performing the process [*e.g.,* cash dispensing] dependent upon the received card information [*e.g.,* Sanford's credit card account number]." EX-1006, ¶327, ¶¶303-305.

Sanford further discloses that the cash dispensing process, performed after it is determined that the inputted picture/fingerprint matches the stored picture/fingerprint, comprises outputting the card account number from Sanford's ACM to financial institution 16. *See* above; EX-1006, ¶328.

Therefore, Sanford discloses that "the performance of the process in the step[]… (eb) [*e.g.,* dispensing money if the user is verified] comprises outputting [*e.g.,* sending] at least part of the inputted card information [*e.g.,* Sanford's credit card account number] from the verification station [Sanford-Hsu system]." EX-1006, ¶329.

4. Claim 7

Claim 7 requires "[a] method according to claim 6, wherein at least ***one of*** the steps (db) and (eb) comprise at least ***one of*** the further steps of: **[i]** inputting information from a keypad to the verification station; and **[ii]** outputting at least some of the information input from the keypad," which is disclosed by Sanford and

Hsu. EX-1006, ¶¶330-334.

The claim is satisfied if "one of the steps (db) and (eb)" comprise "one of" steps [i] and [ii]. Therefore, this claim is satisfied if step (db) comprises step [i] or step [ii], or step (eb) comprises step [i] or step [ii]." Sanford discloses that step (db) comprises both steps [i] and [ii]. EX-1006, ¶331.

Sanford discloses that "ACM 12," which is part of Sanford's ACM, "includes… an input device." EX-1004, ¶0016. Such input device "may be a touch screen or **keypad**." *Id.* As shown in Figure 2, "[i]n step S236 [blue], the user is prompted to enter a withdrawal amount." EX-1004, ¶0033.

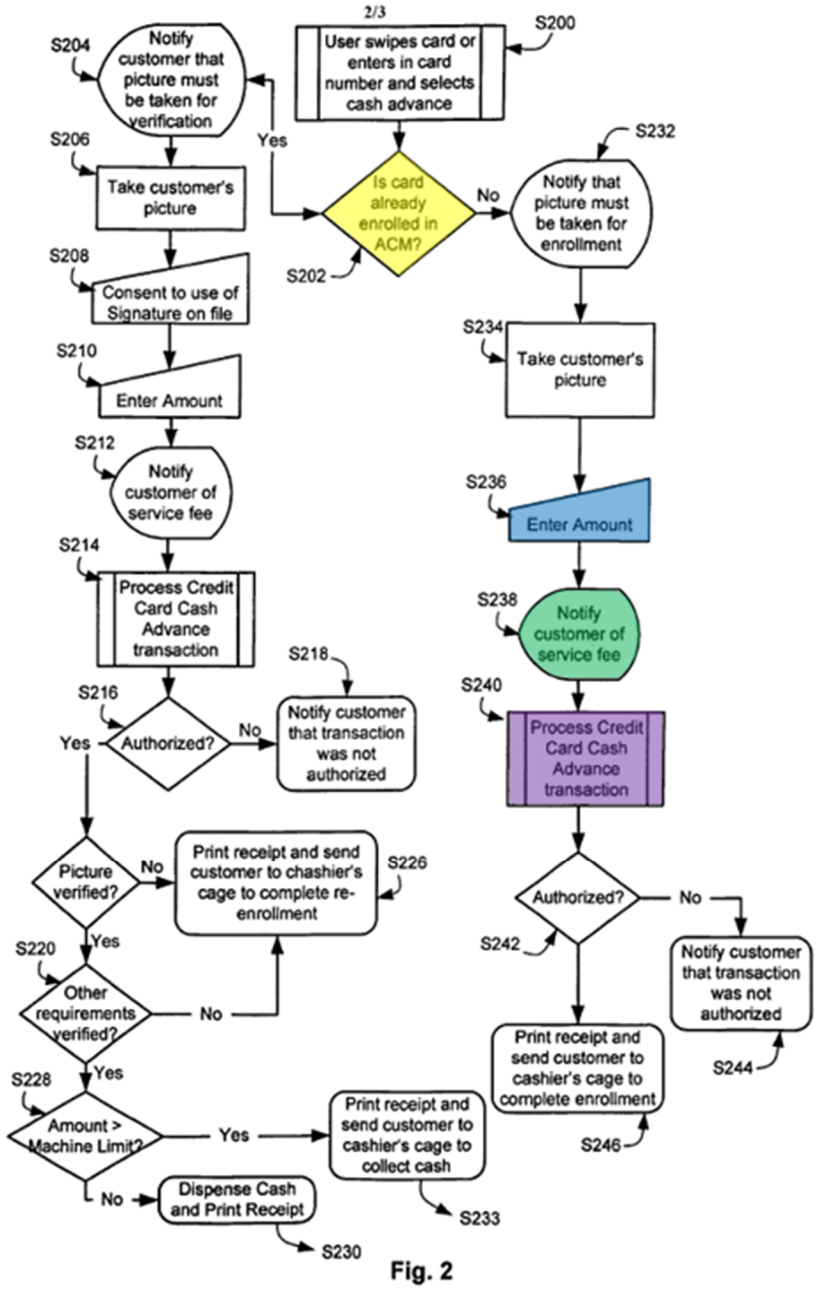


Fig. 2

EX-1004, Fig.2. A POSITA would have understood that the "withdrawal amount" is entered by using Sanford's input device (*e.g.,* keypad). EX-1006, ¶332.

Sanford further discloses that "[o]nce an amount is entered, the user is appraised of any service fees that will be charged and the user acknowledges

acceptance of the service fees in step S238 [green]." EX-1004, ¶0033. A POSITA would have understood that the "service fees" would be dependent upon the "amount [] entered." Additionally, "[i]n step S240 [purple], the transaction is sent for pre-authorization to the financial institution." EX-1004, ¶0034. A POSITA would have understood that the "transaction [] sent for pre-authorization" would also include the "amount [] entered." Finally, when "the user proceeds to a casino cashier [*i.e.*, cashier system 14]…[t]he user may [] be dispensed the money for the transaction." EX-1004, ¶0037. A POSITA would have understood that to dispense the money for the user, the cashier would have to know the "amount [] entered." Therefore, a POSITA would have understood that the "withdrawal amount" entered by using Sanford's keypad is outputted from the keypad so the "service fees" may be determined, the "transaction" can be sent for pre-authorization, and the cashier can dispense the money for the transaction. EX-1006, ¶333.

Therefore, Sanford discloses "step[] (db)…comprises…the further steps of: [i] inputting information [*e.g.,* withdrawal amount] from a keypad to the verification station [*e.g.,* Sanford keypad at ACM]; and [ii] outputting at least some of the information [*e.g.,* withdrawal amount] input from the keypad," which is disclosed by Sanford. EX-1006, ¶334.

5. Claim 8

Claim 8 requires "[a] method according to claim 7, wherein the information outputted is communicated to ***one of***: **[i]** a service provider for providing a service dependent upon receipt of the outputted information; and **[ii]** an apparatus for providing access to a service dependent upon receipt of the outputted information," which is disclosed by Sanford and Hsu. EX-1006, ¶¶335-340.

The claim recites "one of," and therefore only portion [i] or portion [ii] need be disclosed. Sanford discloses both. EX-1006, ¶336.

As discussed for claim 7, Sanford discloses that the "withdrawal amount" entered by a user on a keypad is outputted. For example, "the transaction is sent for pre-authorization to the financial institution." EX-1004, ¶0034. A POSITA would have understood that the "transaction [] sent for pre-authorization" would include the "amount [] entered." Therefore, Sanford discloses that the "withdrawal amount" (outputted information) is sent to the financial institution for pre-authorization. *Id.* Sanford also discloses that the financial institution is "a service provider for providing a service dependent upon receipt of the outputted information." This is because "[f]inancial institution 16 may be any institution capable of authorizing a transaction requested by the user… and is preferably the issuer of the card the user is using." EX-1004, ¶0023. The "issuer of the card" is a service provider for providing credit so that cash can be withdrawn dependent

upon the withdrawal amount provided by a user. EX-1006, ¶337.

Therefore, Sanford discloses that "the information outputted [*e.g.,* withdrawal amount] is communicated to… [i] a service provider [*e.g.,* financial institution] for providing a service [*e.g.,* credit or cash withdrawal] dependent upon receipt of the outputted information [*e.g.,* withdrawal amount]." EX-1006, ¶338.

After entering the "withdrawal amount" using a keypad, when "the user proceeds to a casino cashier [*i.e.*, cashier system 14]…[t]he user may [] be dispensed the money for the transaction." EX-1004, ¶0037. A POSITA would have understood that to dispense the money to the user, the cashier system 14 would have to know the "withdrawal amount." "Cashier system 14 may be any system capable of enrolling a user into ACM computer system 18." EX-1004, ¶0022. A POSITA would have understood that the cashier system 14 is an apparatus for providing access to cash dependent upon the withdrawal amount provided by the user. EX-1006, ¶339.

Therefore, Sanford discloses "the information outputted [*e.g.,* withdrawal amount] is communicated to… [ii] an apparatus [*e.g.,* cash system 14] for providing access to a service [*e.g.,* cash withdrawal] dependent upon receipt of the outputted information [*e.g.,* withdrawal amount]." EX-1006, ¶340.

6. Claim 9

Claim 9 requires "[a] method according to any ***one of*** claims claim 6, 7 and 8 wherein the information outputted is communicated to ***one of***: **[i]** a service provider for providing a service dependent upon receipt of the outputted information; and **[ii]** an apparatus for providing access to a service dependent upon receipt of the outputted information," which Sanford and Hsu disclose. EX-1006, ¶¶351-344.

Claim 9 recites the same limitations as claim 8 except for the preamble: claim 8 depends from claim 7 which depends from claim 6, while claim 9 depends from any of claims 6, 7, and 8. For at least the same reasons that Sanford discloses claim 8, Sanford discloses claim 9. EX-1006, ¶342.

When claim 9 depends from claim 6, the outputted information refers to the user's "credit card account number," as discussed for claim 6. Sanford discloses portion [i] of claim 9. EX-1006, ¶343.

When claim 9 depends from claim 6, Sanford discloses "the information outputted is communicated to…[i] a service provider [financial institution] for providing a service [credit or cash withdrawal] dependent upon receipt of the outputted information [card account number]." *See* claim 6 discussion; EX-1006, ¶344.

7. Claim 10

Claim 10 requires "[a] method according to claim 3, wherein the step (ec) further comprises outputting information indicating that the user of the card device is not authorised [*sic*] authorized," which Sanford and Hsu disclose. EX-1006, ¶¶345-347.

As explained for Limitation 3[E(3)], Sanford discloses "if the inputted biometric signature does not match the stored biometric signature, not performing the process [*e.g.,* cash dispensing] dependent upon the received card information [*e.g.,* Sanford's credit card account number]." EX-1006, ¶346, ¶¶306-308.

Sanford also discloses that not dispensing cash "further comprises outputting information indicating that the user of the card device is not [] authorized." As shown in Figure 2 below, Sanford discloses that if the inputted picture (or fingerprint) is not verified, *i.e.*, does not match the stored picture (or fingerprint), or "[i]f any of the other requirements fail [at step S220 (orange)], the user is printed out a receipt and given instructions to proceed to the cashier for re-enrollment in step S226 [blue]." EX-1004, ¶0030.

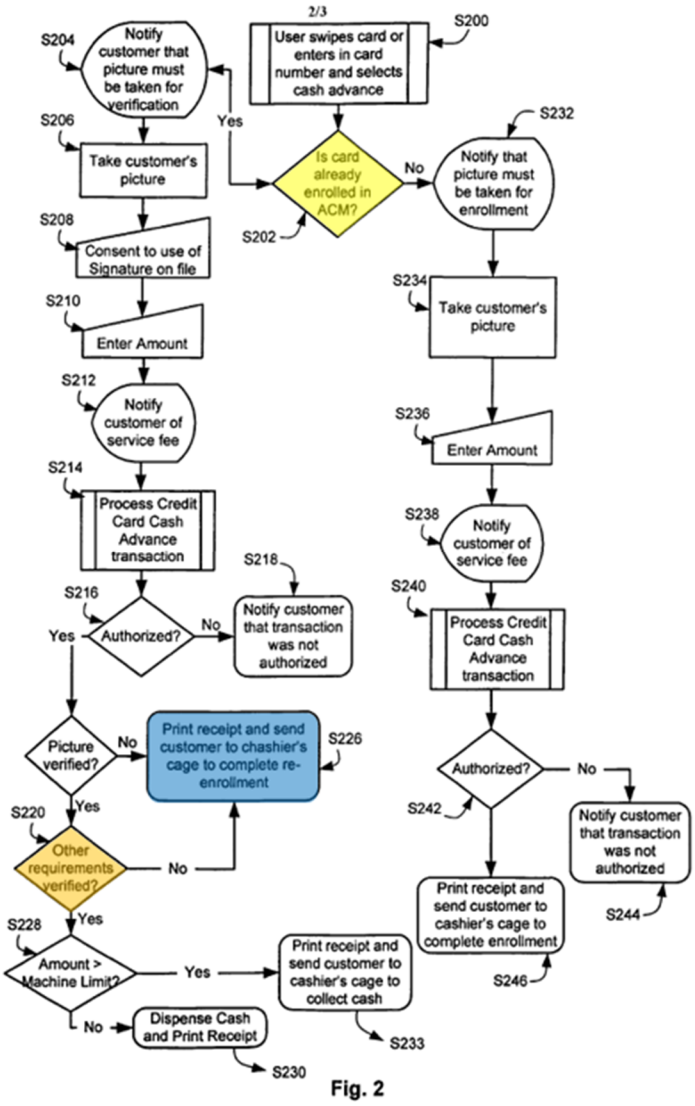


Fig. 2

EX-1004, Fig.2. A POSITA would have understood that the printed receipt and the instructions to proceed for re-enrollment are outputted information indicating the user of the card device is not authorized. EX-1006, ¶347.

8. Claim 11

Sanford discloses claim 11: "[a] method according to claim 10, wherein the

information outputted [*e.g.,* indicating that the user of the card device is not authorized] is communicated to one of: [i] a service provider [*e.g.,* human operator/cashier] for providing a service [*e.g.,* re-enrollment] dependent upon receipt of the outputted information; and [ii] an apparatus [*e.g.,* cashier system 14] for providing access to a service [*e.g.,* re-enrollment] dependent upon receipt of the outputted information." EX-1006, ¶¶348-351.

The preamble recites "one of," and therefore only the first portion [i] or the second portion [ii] need be disclosed. Sanford discloses both. EX-1006, ¶349.

As discussed for claim 10, the printed receipt and the instructions to proceed for re-enrollment are outputted information indicating **the user of the card device is not authorized**. Regarding enrollment, Sanford discloses "[t]he enrollment process is preferably only done once… [with] exceptions." EX-1004, ¶0038. Thus, a POSITA would have understood re-enrollment is a relatively rare process that is not performed regularly. Therefore, when a user follows the instructions and proceeds for re-enrollment, a POSITA would have understood the "[c]ashier system 14… capable of enrolling a user" and the "human operator [at the cashier system 14] to facilitate enrolling the user" may be aware that a user of the card device is not authorized. EX-1004, ¶0022. Unlike the first-time enrollment when the database does not have a user's information, re-enrollment involves overwriting existing data associated with a user, and therefore the cashier system

14 (*i.e.*, an apparatus used by a cashier) and the human operator (*i.e.*, a service provider) would know that the card user is not authorized when attempting to access a transaction and perform re-enrollment dependent upon that knowledge. EX-1006, ¶350.

9. Claim 15

Preamble 15[P]

Sanford discloses "[a] **verification station for securing a process**, [Stanford's verification station comprising] **the verification station comprising**." *See* Limitation 3[P]; EX-1006, ¶353, ¶¶268-277.

Limitation 15[A]

Sanford discloses "**a card device reader for receiving card information from a card device coupled to the verification station**." *See* Limitation 3[A]. Sanford discloses that its card reader is **part of** its ACM (EX-1004, ¶0016), and is therefore **coupled to** the ACM (the same way that claim 15 requires that the verification station comprises the card reader but is also coupled to it).[10] EX-1006,

[10] Sanford also discloses the card is **coupled to** the card reader and therefore **coupled to** the ACM. EX-1004, ¶0016; EX-1006, ¶355.

¶¶354-355.

Limitation 15[B]

The claim requires "**a biometric signature reader for receiving a biometric signature provided to the verification station**," which Sanford discloses. EX-1006, ¶¶356-357.

As explained for Limitation 3[B], Sanford discloses "(b) inputting a biometric signature [*e.g.,* picture/fingerprint] of a user [*e.g.,* customer] of the card device [*e.g.,* credit card] to a biometric reader [*e.g.,* picture taking device, or fingerprint sensor] in the verification station [Sanford's ACM]." EX-1006, ¶¶278-281. Therefore, Sanford discloses that a biometric signature is **provided to** a biometric signature reader. Because the biometric signature reader is **part of** the ACM (EX-1004, ¶0016), when the biometric signature is **provided to** the biometric signature reader, it is also **provided to** Sanford's ACM. EX-1006, ¶357.

Limitation 15[C]

The claim requires "***means for* determining if the provided card information has been previously provided to the verification station**," which Sanford discloses. EX-1006, ¶¶358-362.

Petitioners propose the following construction, which follows an agreed

construction between Apple and Patent Owner (*see* EX-1013, 3):

> **Function**: determining if the provided card information has been previously provided to the verification station
>
> **Structure**: processor unit 105 running software process(es) 206; and equivalents thereof.

See EX-1001, 6:49-59; 8:5-21; 8:61-9:37; Figs. 5, 7.

First, as explained for Limitation 3[C], Sanford discloses the recited **function**. EX-1006, ¶361, ¶¶282-285.

Second, Sanford discloses the same or equivalent **structure**. 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." EX-1004, ¶0018.

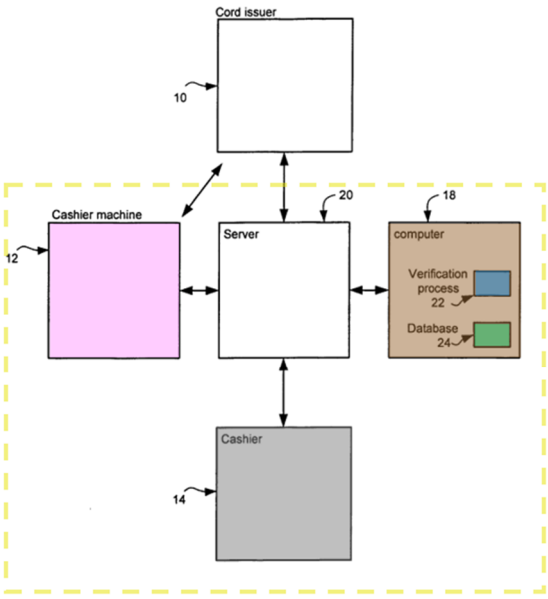


Fig. 1

EX-1004, Fig.1. "The **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." *Id.*, ¶0018. Thus, a POSITA would have understood the recited function is similarly performed by the processor executing software. EX-1006, ¶362.

Limitation 15[D(P)+D(1)]

The claim requires "***means*, if the provided card information has not been previously provided to the verification station, *for*: storing the inputted biometric signature in a memory at a memory location defined by the provided card information**," which is disclosed by Sanford and Hsu. EX-1006,

¶¶363-367.

Petitioners propose the District Court's construction for the substantially identical limitation: "means for storing, if the memory location is unoccupied, the biometric signature at the defined memory location":

> **Function**: [if the provided card information has not been previously provided to the verification station,] storing the inputted biometric signature in a memory at a memory location defined by the provided card information
>
> **Structure**: a computer system with a processor unit 105 running software process(es) 401 and at least one of: a storage device 109 or memory 106. Structure is found in '039 Patent, col. 6, line 66 – col. 7, line 23; col. 5, lines 13-18 & lines 19-22 & 23-30; Fig. 7, step 401.

EX-1012, p.2.

First, for the same reasons explained for Limitations 3[D(P)+D(1)], the combined Sanford-Hsu system discloses the recited **function**. EX-1006, ¶366, ¶¶286-294.

Second, the combined Sanford-Hsu system discloses the same or equivalent **structure**. The construction requires a computer system with a processor to perform the recited storing function. A POSITA would have understood that

Sanford's processor that is "in communication with… database 24" reads data from and writes data to the database. EX-1004, ¶0018. "Verification process 22 may be a **software- implemented** process that communicates with database 24." *Id.* Therefore, a POSITA would have understood the recited function is performed by Sanford's processor executing software. EX-1006, ¶367.

Limitation 15[D(P)+D(2)]

The claim requires "***means*, if the provided card information has not been previously provided to the verification station, *for*: performing the process dependent upon the received card information**," which Sanford discloses. EX-1006, ¶¶368-372.

Petitioners propose the following construction:

> **Function**: [if the provided card information has not been previously provided to the verification station,] performing the process dependent upon the received card information
>
> **Structure**: an ATM capable of receiving from a user the required amount of cash and the relevant account information and dispensing cash.

EX-1001, 9:50-59; 10:3-5; Figs. 6, 7.

First, for the same reasons explained for Limitations 3[D(P)+D(2)], Sanford

discloses the recited **function**. EX-1006, ¶371, ¶¶295-299.

Second, Sanford discloses the same or equivalent **structure**. Sanford discloses that "[a]utomated cashier machine 12 is capable of taking a picture of a person, and dispensing money" and "[i] n another embodiment, cashier machine 12 is an ATM machine capable of taking a picture of a person." EX-1004, ¶0016. Sanford further explains how to withdrawal money from an ATM: "In order for a patron to use an ATM machine, the patron must have an issued ATM card and a PIN (Personal Identification Number). The patron can then insert the ATM card into the ATM machine, enter their PIN, and withdraw money from the ATM." *Id.*, ¶0004. As explained for Limitation 3[D(2)], it would have been obvious to a POSITA to integrate the cashier system 14, that is also capable of printing a receipt and dispensing cash (EX-1004, ¶0037), into Sanford's ACM, as Sanford expressly says the ACM can be an ATM. Thus, Sanford's ACM is an ATM capable of dispensing cash. EX-1006, ¶372.

Limitation 15[E(P)+E(1)]

The claim requires "***means*, if the provided card information has been previously provided to the verification station, *for*: comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information**," which is disclosed

by Sanford and Hsu. EX-1006, ¶¶373-378.

Petitioners propose the following construction:

> **Function**: [if the provided card information has been previously provided to the verification station,] comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information
>
> **Structure**: a computer system with a processor 105 executing an application that compares an inputted biometric signature to a stored biometric signature.

EX-1001, 6:49-7:8; 7:50-8:4; 8:5-21; 9:42-49.

First, for the same reasons explained for Limitations 3[E(P)+E(1)], the Sanford-Hsu system discloses the recited **function**. EX-1006, ¶376, ¶¶300-302.

Second, the combined Sanford-Hsu system discloses the same or equivalent **structure**. Sanford discloses:

> "In one embodiment, **ACM computer system 18 includes a processor**. … **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 in order to **verify that the picture taken by ACM 12 matches a picture in database 24**."

EX-1004, ¶0018. A POSITA would have understood that "verify[ing] that the

picture taken by ACM 12 matches a picture in database 24" is "comparing" the two pictures. *Id.* Sanford also discloses that the verification process uses an "algorithm based on facial biometrics," such as "Principal Component Analysis (PCA)" or "Local feature Analysis (LFA)." *Id.*, ¶¶0019-20; EX-1006, ¶377.

Moreover, Hsu discloses "perform[ing] the matching function very rapidly by using special-purpose hardware in the form of an application-specific integrated circuit (ASIC)." EX-1003, ¶0023. A POSITA would have understood that ASICs at the time typically included processors and memories for executing programs. Therefore, a POSITA would have understood the verification process in Hsu (comparing an inputted fingerprint to a stored fingerprint) is accomplished by at least one processor executing an application. EX-1006, ¶378.[11]

Limitation 15[E(2)]

The claim requires "[***means… for***:] **if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information**," which Sanford discloses. EX-1006,

[11] The '039 Patent recognizes it was known in the art to use a processor to compare newly inputted information with stored information. EX-1001 2:23-31; EX-1006, ¶378.

¶¶379-381.

Petitioners propose the following construction:

> **Function**: if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information
>
> **Structure**: an ATM capable of receiving from a user the required amount of cash and the relevant account information and dispensing cash.

EX-1001, 9:50-59; 10:3-5; Figs. 6, 7.

As discussed for Limitation 3[E(2)], Sanford discloses the **function**. EX-1006, ¶¶303-305. As discussed for Limitation 15[D(2)], Sanford also discloses the same or equivalent **structure**. EX-1006, ¶¶368-372, ¶381.

Limitation 15[E(3)]

The claim requires "[***means… for***:] **if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information**," which Sanford discloses. EX-1006, ¶¶382-384.

Petitioners propose the following construction:

> **Function**: if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information
>
> **Structure**: an ATM capable of receiving from a user the required amount of cash and the relevant account information and dispensing cash.

EX-1001, 9:50-59; 10:3-5; Figs. 6, 7.

As discussed for Limitation 3[E(3)], Sanford discloses the **function**. EX-1006, ¶¶306-308. As discussed for Limitation 15[D(2)], Sanford also discloses the same or equivalent **structure**. EX-1006, ¶¶368-372. Such structure performs the recited function because it does not dispense money if the user verification process fails, as explained for Limitation 3[E(3)]. EX-1006, ¶306-308.

10. Claim 16

Claim 16 requires "[a] verification station according to claim 15, wherein the card device reader is ***one of***: **[i] a reader for** a card in which the card information is encoded in a **magnetic strip**; **[ii] a reader for** a card in which the card information is encoded in a **bar code**; **[iii] a reader for** a smart card in which the card information is stored in a **solid state memory** on the smart card; and **[vi] a receiver** for a **key fo**b adapted to provide the card information by transmitting a wireless signal to the verification station," which is disclosed by Sanford and Hsu.

EX-1006, ¶¶385-387.

Since the claim recites "one of," only one of portions [i] to [iv] need be disclosed.

Sanford discloses the first portion [i]. As discussed for Limitation 15[A], 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." *Id.*, ¶0016; *see also* ¶0040. A POSITA would have understood that credit cards have their credit card account number encoded in a magnetic strip. EX-1006, ¶387. (Although not necessary to disclose the claim, Hsu discloses and renders obvious each of [i] through [iv].[12] *See* discussion at claim 4, incorporated here. EX-1006, ¶¶314-317.)

11. Claim 18

Claim 18 recites a subset of claim 15 except that claim 18 recites "code for" limitations instead of the equivalent "means for" limitations. These "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

[12] Petitioners reserve the right to assert lack of written description in other forums.

render obvious claim 18, as summarized below: (EX-1006, ¶388)

Claim 18 Limitation	**Description**	**Claim 15 Limitation**
18[P][13]	"a method for securing a process"	15[P]
18[A]	"code for determining"	15[C]
18[B(P)]	"if the provided card information has not been previously provided"	15[D(P)]
18[B(1)]	"[code… for] storing"	15[D(1)]
18[B(2)]	"[code… for] performing"	15[D(2)]
18[C(P)]	"if the provided card information has been previously provided"	15[E(P)]
18[C(1)]	"[code… for] comparing"	15[E(1)]
18[C(2)]	"[code… for] performing"	15[E(2)]
18[C(3)]	"[code… for] not performing"	15[E(3)]

[13] Claim 18 also recites "non-transitory computer readable medium" in its preamble. For the 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.

B. GROUND #2: Claims 3, 4, 6-11, 15, 16, and 18 are Rendered Obvious by Sanford, Hsu, and Tsukamura

1. Claim 3

As explained in Ground 1, incorporated here, Sanford in view of Hsu discloses claim 1 under the First Construction. *See* Section VII.A.1 and discussion for Limitations 3[D(1)] and 3[E(1)]. EX-1006, ¶390.

If this limitation means "a memory location is specified by the card information" (Second Construction), Sanford in view of Hsu and Tsukamura renders obvious claim 3. EX-1006, ¶391.

Limitation 3[D(P)+D(1)]

Sanford in view of Hsu and Tsukamura discloses **"if the provided card information** [*e.g.,* Sanford's credit card account number**] has not been previously provided to** [*e.g.,* not enrolled in] **the verification station** [*e.g.,* Sanford-Hsu-Tsukamura system], **(da) storing the inputted biometric signature** [*e.g.,* picture/fingerprint] **in a memory** [*e.g.,* Tsukamura's local memory] **at a memory location defined by the provided card information** [*e.g.*, Tsukamura's memory location indexed by Sanford's credit card account number]." EX-1006, ¶¶392-396.

A POSITA would have understood there are many ways to implement Hsu's "table that associates each user number with a stored fingerprint image" in

Sanford's system. EX-1003, ¶0020. If Hsu's user/account number is deemed not to define the **memory address** where the user's fingerprint is stored in Hsu's database, the implementation in Tsukamura does so, and it would have been obvious to modify Sanford-Hsu in view of Tsukamura for the reasons below. EX-1006, ¶393.

Tsukamura discloses a simple and efficient structure for "stored…fingerprint data" in Figure 3. EX-1005, 2:9-10.

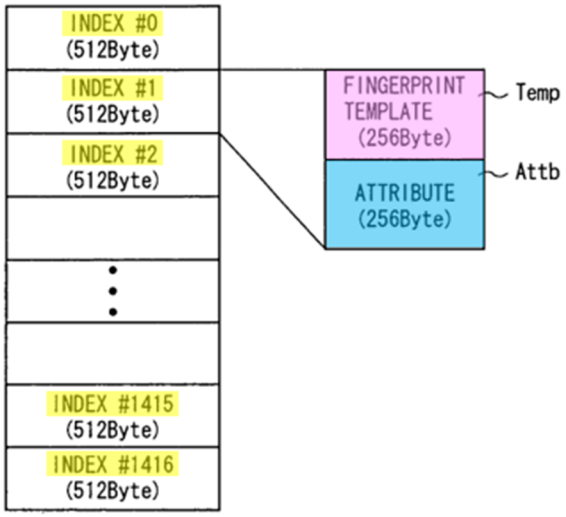


FIG. 3

EX-1005, Fig.3. The memory in Figure 3 stores multiple fingerprint data entries and each entry has a fixed length (*e.g.*, 512 bytes) and is stored consecutively within the memory. As shown, "the fingerprint template Temp [pink] and an attribute Attb [blue] associated with the fingerprint template Temp [are registered]

at an index (address) specified by the index number N index [yellow] within the collation flash ROM 35," which is a component of the fingerprint collating unit 30—*i.e.*, local memory external to the card. *Id.*, 2:46-47, 3:28-32, Fig.2; *see also* 2:34-36 ("each fingerprint template [is] identified by an index number N index."). As such, **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. 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.

Following claim 3 is a detailed motivation-to-combine combine discussion of Sanford-Hsu in view of Tsukamura. EX-1006, ¶395.

Limitation 3[E(P)+E(1)]

Sanford in view of Hsu and Tsukamura discloses "**if the provided card information** [*e.g.,* Sanford's credit card account number] **has been previously provided to** [*e.g.,* enrolled in] **the verification station** (*e.g.,* Sanford-Hsu-Tsukamura system] (**ea) comparing the inputted biometric signature** [*e.g.,* picture/fingerprint] **to the biometric signature** [*e.g.,* picture/fingerprint] **stored in**

the memory [*e.g.,* Tsukamura's local memory] **at the memory location defined by the provided card information** [*e.g.*, Tsukamura's memory location defined by index/credit card account number]," for the same reasons explained for Limitation 3[D(P)+D(1)] (Ground 1) and the additional reasons explained for Limitation 3[D(P)+D(1)] (Ground 2). EX-1006, ¶397, ¶¶286-294, ¶¶392-396.

Motivation to Combine Sanford-Hsu and Tsukamura

The '039 Patent, Sanford, Hsu, and Tsukamura are in **the same field of endeavor**, *i.e.*, access control using biometric authentication. All references (and the '039 Patent) are directed to performing efficient biometric authentication, including using fingerprints. All references (and the '039 Patent) teach authenticating a user by comparing a fingerprint captured by a sensor to a stored fingerprint. EX-1003, Abstract; EX-1004, Abstract; EX-1005, Abstract. All 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 using a user's picture (or fingerprint) associated with a user's credit card number. EX-1003, ¶¶0018-21. Hsu discloses the stored fingerprint data being associated with a user number/account/employee number from a user's card. EX-1003, ¶0026. Tsukamura discloses the stored fingerprint data being associated with an index number provided by a user. EX-1005, 2:34-36. In this way, all three references

(and the ’039 Patent) improve 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, which was well-known before the ’039 Patent. EX-1006, ¶398; ¶¶225-227.

Both the Sanford-Hsu system and Tsukamura disclose storing biometric information (*e.g.,* picture or fingerprint) during an enrollment process. Hsu’s database for storing fingerprints in the Sanford-Hsu system is an indexed database in a memory:

> “the fingerprint database 44 contains reference fingerprint image data for each user, employee, or customer…and...the reference fingerprint data are associated with corresponding user numbers, or employee or customer account numbers.”

EX-1003, ¶0026.

> “***The 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-1003, ¶0020.

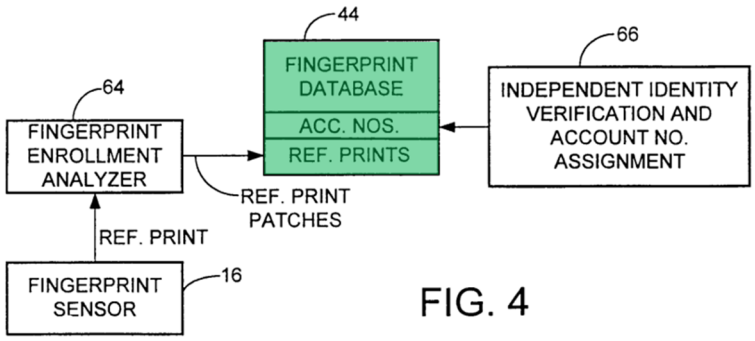


FIG. 4

EX-1003, Fig. 4. It was common knowledge to a POSITA that there were multiple ways of generating and storing a table that associates each user number with a stored fingerprint. EX-1006, ¶229-232. Tsukamura teaches one of the simplest and most efficient ways of doing so by **storing** fingerprints consecutively in memory at indexed locations, as shown in Figure 3 below.

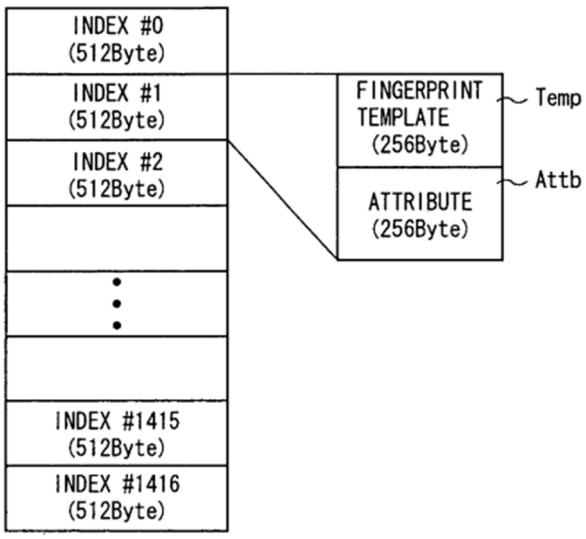


FIG. 3

EX-1005, Fig.3; 3:28-32 ("the collation controller 34 **registers** the fingerprint template Temp and an attribute Attb associated with the fingerprint template Temp **at an index (address) specified by the index number N index within the collation flash ROM 35**". Since each entry in Tsukamura's memory is fixed length (*i.e.,* 512 bytes), the memory location for any user's fingerprint is defined based on the index number. *Id*.; EX-1006, ¶399.

Tsukamura also discloses **retrieving** fingerprints based on the index number for verification. EX-1005, 4:7-11 ("the collation controller 34 as collating means **reads** the fingerprint template Temp **specified by the index number N index from the collation flash ROM 35** and collates the fingerprint image data D37 with the read fingerprint template Temp.").[14]

[14] A POSITA would have understood that "collate" here means "compare" or "verify." Tsukamura discloses a "fingerprint **collation** process" (EX-1005, 3:36) as a different process from a "fingerprint **registration** process" (*id.* 2:39), and Tsukamura uses "collate" as synonymous with "compare." *See, e.g.*, EX-1005 4:7-11; *see also* Abstract. Dictionary definitions also confirm that "collate" can mean "compare." *See, e.g.,* EX-1014, p.737 ("COMPARE INFORMATION"); EX-1015, p.299 ("to bring together for comparison; to examine and compare"); EX-1006, ¶401.

Thus, when storing/retrieving the fingerprint associated with a particular user, Tsukamura writes/reads directly to/from the memory location defined by the index number, without the need to first locate that index number within a more complicated table/database. A POSITA would have understood that writing/reading directly to/from a physical memory location is faster than writing/reading to/from a logical database because it does not require searching and/or memory space transformation before accessing the physical memory location. EX-1006, ¶402.

Since the Sanford-Hsu system specifically aims for speed,[15] a POSITA implementing the Sanford-Hsu system would have been motivated to use Tsukamura's memory structure for storing Sanford-Hsu's pictures/fingerprints to further improve the speed and efficiency of the system. A POSITA would also have understood that Tsukamura's memory configuration is one of the simplest implementations of Hsu's database because it is laid out contiguously in physical memory, is highly efficient, and need only store the fingerprints and not the

[15] "In particular, the invention provides a high level of security because of its use of fingerprint matching, but does not sacrifice **speed** or convenience of operation because preliminary identification is provided by the user and fingerprint matching can, therefore, be achieved **rapidly**." EX-1003, ¶0013.

corresponding index numbers. EX-1005, Fig.4; EX-1006, ¶403.

Further, when assigning a credit card account number in the Sanford-Hsu-Tsukamura system, it would have been obvious to use Tsukamura's index numbers that define locations in memory. Sanford, Hsu, and Tsukamura all disclose a user providing his/her number. EX-1004, ¶0024 ("The user may… insert[] or swip[e] a credit card… [or] enter a credit card account number."); EX-1003, ¶0026 ("the user [] presents an account number, employee number or similar identity number."); EX-1005, 3:45-46 ("the index number N index specified by the user"). Thus, it would have been obvious to assign Tsukamura's index number as the credit card account number in the Sanford-Hsu system. For example, assume there are ten (10) users in the Hsu-Tsukamura system. In Tsukamura, the index numbers for these 10 users would be 0, 1, 2,…, 9, which would be assigned as the card account numbers in the Sanford-Hsu system. Thus, when storing/retrieving the fingerprint for account number 3 from Tsukamura's memory, the index number is the number 2. EX-1006, ¶404.

A POSITA would have had a **reasonable expectation of success** in using Tsukamura's memory structure in Sanford-Hsu's database. Both Tsukamura and Sanford-Hsu store and allow access to a user's fingerprint based on a number (*e.g.,* card account number, or index number) provided by a user. Implementing Tsukamura's memory structure and index numbers in Sanford-Hsu's database

would result in a working system having improved speed and efficiency. Therefore, a POSITA would have had a reasonable expectation of success in using Tsukamura's memory structure for Sanford-Hsu's database to efficiently store and retrieve pictures/fingerprints. EX-1006, ¶405.

2. Claims 4, 6-11

As explained in Ground 1, incorporated herein, Sanford in view of Hsu discloses claims 4 and 6-11. For the same reasons, Sanford in view of Hsu and Tsukamura also discloses these claims. EX-1006, ¶406, ¶¶314-351.

3. Claim 15

As explained in Ground 1, incorporated herein, Sanford in view of Hsu discloses claim 15 under the First Construction. *See* Section VII.A.1 and discussion for Limitations 15[D(1)] and 15[E(1)]. EX-1006, ¶407.

If the term means "a memory location is specified by the card information" (Second Construction), Sanford in view of Hsu and Tsukamura discloses claim 15. EX-1006, ¶408.

Limitation 15[D(P)+D(1)]

The claim requires "***means***, if the provided card information has not been

previously provided to the verification station, ***for*: storing the inputted biometric signature in a memory at a memory location defined by the provided card information**," which is disclosed by Sanford, Hsu, and Tsukamura. EX-1006, ¶¶409-411.

First, for the same reasons explained for Limitation 3[D(P)+D(1)] (Ground 2), the Sanford-Hsu-Tsukamura system discloses the recited **function**. EX-1006, ¶413, ¶¶392-396.

Second, the Sanford-Hsu-Tsukamura system discloses the same or equivalent **structure**. In addition to the reasons explained for Limitation 15[D(P)+D(1)] (Ground 1) and incorporated here, Tsukamura discloses that "[t]he CPU 31 reads a control program from the program flash ROM 33 and **executes the control program in the program RAM 32** to control the whole of the fingerprint collating unit 30." EX-1005, 2:50-53. A POSITA would have understood that RAM stands for Random Access Memory and is a type of memory. Therefore, a POSITA would have understood that the Sanford-Hsu-Tsukamura system performs the storing function using a processor and memory. EX-1006, ¶411.

Limitation 15[E(P)+E(1)]

The claim requires "***means***, if the provided card information has been previously provided to the verification station, ***for***: **comparing the inputted**

biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information," which is disclosed by Sanford, Hsu, and Tsukamura. EX-1006, ¶¶412-141.

First, for the same reasons explained for Limitation 3[E(P)+E(1)] (Ground 2), the Sanford-Hsu-Tsukamura system discloses the recited **function**. EX-1006, ¶413, ¶397.

Second, the Sanford-Hsu-Tsukamura system discloses the same or equivalent **structure**. In addition to the reasons explained for Limitation 15[E(P)+E(1)] (Ground 1) and incorporated here, Tsukamura illustrates in Fig. 2 different components of a fingerprint collating unit 30, which includes a processor (*i.e.,* CPU 31, brown).

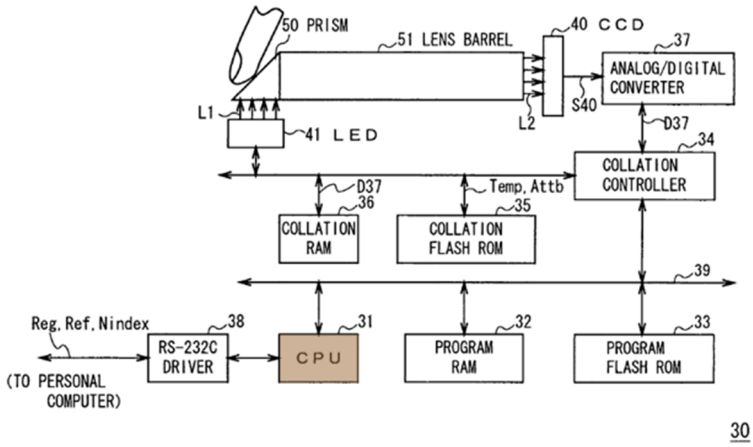


FIG. 2

EX-1005, Fig.2. Because CPU 31 in Tsukamura "control[s] the whole of the fingerprint collating unit 30" (EX-1005, 2:50-53), a POSITA would have found it

obvious to use the same CPU to control the Sanford-Hsu-Tsukamura system, including comparing an inputted fingerprint with a stored fingerprint. EX-1006, ¶414.

4. Claim 16

For the same reasons as in Ground 1, Sanford in view of Hsu and Tsukamura discloses this claim. EX-1006, ¶415, ¶¶385-387.

5. Claim 18

For the same reasons as in Ground 1, Sanford in view of Hsu and Tsukamura discloses claim 18. EX-1006, ¶416. ¶¶388-389.

Regarding Limitation 18[C(1)], Tsukamura also discloses the "code for" performing the recited function. Tsukamura discloses regarding Figure 2: "[t]he CPU 31 [brown] reads a **control program** from the program flash ROM 33 [blue] and executes the **control program** in the program RAM 32 [yellow] to control the whole of the fingerprint collating unit 30 [green]." EX-1005, 2:50-53.

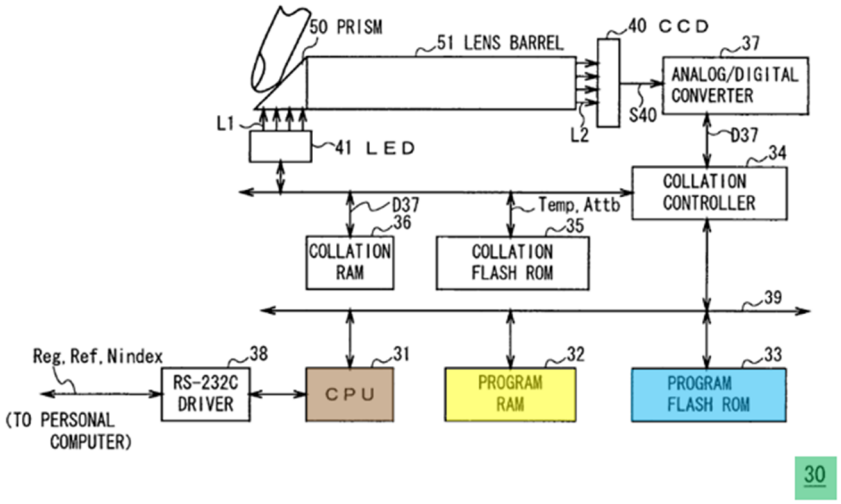


FIG. 2

EX-1005, Fig.2. Since CPU 31 (brown) "control[s] the whole of the fingerprint collating unit 30," including "collating the read fingerprint information with the registered fingerprint information to effect personal authentication," Tsukamura's "**control program**" includes the "**code for**" fingerprint verification. EX-1005, Abstract, 2:50-53; EX-1006, ¶417.

C. GROUNDS #3 AND #4: Claim 5 is Rendered Obvious

The discussion below explains that the limitations of claim 5 are rendered obvious by Leu. EX-1006, ¶¶418-432.

Ground 3 incorporates the below analysis in the context of the Sanford-Hsu system (Ground 1) in view of Leu. Ground 1 is incorporated here. EX-1006, ¶419.

Ground 4 incorporates the below analysis in the context of the Sanford-Hsu-Tsukamura system (Ground 2) in view of Leu. Ground 2 is incorporated here. EX-1006, ¶420.

Claim 5 requires "[a] method according to claim 3, wherein: 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."

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. EX-1009, 1:26-29; 1:20-27.[16] Thus, Leu's card reader device is a verification station. EX-1006, ¶422.

Leu discloses in Figure 3 a memory configuration for its card. EX-1009, 2:5.

[16] EX-1009 is an English translation of EX-1008 (Leu). Citations to Leu are made to EX-1009.

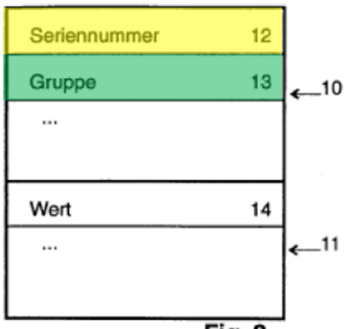


Fig. 3

[Fig. 3 Translation Key:]
12 = serial number
13 = group
14 = value

EX-1009, Fig.3. The memory is divided into multiple sections. A serial number memory 12 (yellow) "contains a serial number that is different for each card." *Id.*, 3:13-16. A group memory 13 (green) "indicates whether a card is a lottery ticket card or a conventional card." *Id.*, 3:20-22. Since the group number and the serial number are stored on the card and are to be read by a card reader device (*id.*, 3:47-4:6), they are both card information. EX-1006, ¶423.

Leu further discloses a process illustrating how an event (*e.g.,* determining "whether or not the user has achieved a lottery prize") is triggered based on the group number and the serial number. EX-1009, 1:26-29; EX-1006, ¶424.

For example, the serial number stored in the serial number memory 12 is used for a similar check. As shown in Fig. 5, "[i]n step 24 [yellow], the serial number from the corresponding serial number memory 12 is compared with those contained in the table according to Figure 4." EX-1009, 4:2-4; Fig.4; 3:29-31

("Figure 4 shows a detail of the memory 6 of the reader device. In this region, there is a list of the serial numbers that are authorized for a prize.").

Fig. 5

[Fig. 5 Translation Key:]
20 = check the group of the card
22 = authorized group?
nein = no
24 = compare the serial number of the card with the list
36 = on list
28 = check the value of the card
30 = value = 0?

EX-1009, Fig.5. Similarly, the determination of whether a card user has won a lottery prize (Point B, green) is **only performed if** the serial number indicates that "the card belongs to the subgroup." *Id.*, 1:32-35. Thus, since the card reader can interpret the serial number and determine whether the card belongs to a subset of cards, a POSITA would have understood the subset of cards is associated with the card reader (verification station). EX-1006, ¶425.

As another example, as shown in Fig. 5, the group number is checked at steps 20 and 22 (blue).

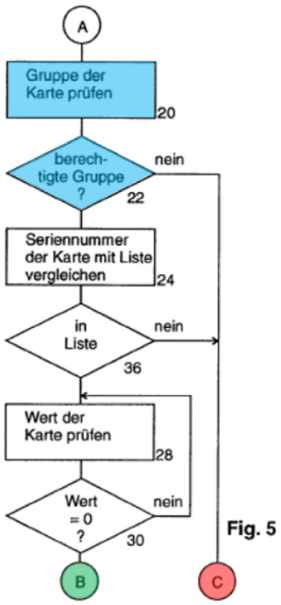


Fig. 5

[Fig. 5 Translation Key:]
20 = check the group of the card
22 = authorized group?
nein = no
24 = compare the serial number of the card with the list
36 = on list
28 = check the value of the card
30 = value = 0?

EX-1009, Fig. 5. "If the card is not a lottery card on the basis of this value [*i.e.*, group number] (Step 20), checking is stopped at Point C and the card is used as a normal prepaid card." *Id.*, 3:53-55. Otherwise, "an event [*e.g.,* it is determined that a user has won a lottery prize] [may be] triggered at Point B [green]." *Id.*, 4:10. Thus, 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). Such use of "group number" is the same as the "card type" described in the '039

Patent, where the header that includes the "card type" information is used to "determine if the card 601 is to be processed according to the disclosed BCP approach or not." EX-1001, 7:35-38. 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). EX-1006, ¶426.

It was well-known to use header-data when transmitting information. EX-1006, ¶427. Since the serial number memory 12 (yellow) and the group memory 13 (green) are the top two entries in the memory table shown in Fig. 3, a POSITA would have understood that the corresponding serial number and/or group number are included in the header section and the rest of the card information (*e.g.*, the card value) is included in the data section. *Id*.

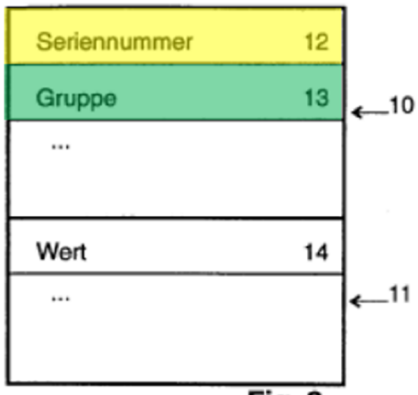


Fig. 3

[Fig. 3 Translation Key:]
12 = serial number
13 = group
14 = value

EX-1009, Fig.3.

It would have been obvious to transmit card information in the Sanford-Hsu system in a header-data format such as disclosed by Leu. EX-1006, ¶428.

The '039 Patent, 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, both of which are discussed in the '039 Patent. EX-1001, 1:25-29 ("The card information is used for various secure access purposes including **drawing cash** from an Automatic Teller Machine (ATM), **making a purchase on credit**, updating a loyalty point account and so on."); EX-1009, 1:6-13. Moreover, 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-1009, 2:14-29; EX-1001, 1:14-16; EX-1004, Title; EX-1006, ¶429.

A POSITA 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. Indeed, the '039 Patent recognizes that a card being read needs to be suitable for the card reader. EX-1001, 1:23:25 ("The

card devices all contain card information that is accessed by 'coupling' the card device to an **associated** reader device."); *see also* 2:28:30 ("check… that the card itself is valid."). Such preliminary checking saves system resource and operation time by skipping a series of steps (*e.g.*, authentication, cash withdrawal, and/or enrollment) that are unnecessary for a "invalid" credit card. EX-1006, ¶430.

Leu performs a similar preliminary check based on a group number and/or a serial number, which allows skipping a series of steps (steps 26 and 30 in Figure 5, steps in Figure 6) that are meaningless for "conventional cards" (instead of "lottery ticket cards"). A POSITA would have been motivated to look to Leu's teaching regarding how to implement such a preliminary check in the Sanford-Hsu system. EX-1006, ¶431.

Further, a POSITA would have had a **reasonable expectation of success** in this combination because Leu expressly teaches a specific configuration of data and a particular type of checking, which were commonly in use at the time of the '039 Patent, and when combined with the Sanford-Hsu system, would have resulted in a working system. EX-1006, ¶432.

D. GROUNDS #5 AND #6: Claim 12 is Rendered Obvious

The discussion below explains that the limitations of claim 12 are rendered obvious by Houvener. EX-1006, ¶¶433-445.

Ground 5 incorporates the below analysis in the context of the Sanford-Hsu system (Ground 1) in view of Houvener. Ground 1 is incorporated here. EX-1006, ¶434.

Ground 6 incorporates the below analysis in the context of the Sanford-Hsu-Tsukamura system (Ground 2) in view of Houvener. Ground 2 is incorporated here. EX-1006, ¶435.

Claim 12 requires "(f) **storing the card information** [*e.g.,* Sanford's credit card account number] **provided by successive instances of the step (a)**; **and (g) outputting the information** [*e.g.,* Sanford's credit card account number] **stored in the step (f) for *audit* purposes**."

Houvener discloses a biometric verification system with "**audit** capabilities". EX-1010, Abstract. Specifically, Houvener discloses "**stor[ing]** the users PIN and the data from the specific transaction as a transaction record." *Id.*, 7:58-60. Houvener further discloses:

> "Thus, 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 for positively identifying the individual initiated the transaction."

EX-1010, 7:60-65.

> "In addition, the system could be configured to incorporate an **off-line fraud detection** routine to monitor **transaction patterns** in order to identify out of norm fraud patterns."

EX-1010, 7:65-8:1.

Therefore, 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). A POSITA would also 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-1010, 7:60-65; EX-1006, ¶438.

It would have been obvious to implement Houvener's audit trail and fraud detection in the Sanford-Hsu (or Sanford-Hsu-Tsukamura) system. EX-1006, ¶439.

The '039 Patent, Houvener, 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 solve the problem of fraudulent transactions and provide a more secure system. EX-1006, ¶440.

A POSITA implementing the Sanford-Hsu system would have been

motivated to look to Houvener. A POSITA 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. Moreover, Hsu discloses that "[t]he database may also contain other information about the user, such as a history of access to the door 12." EX-1003, ¶0020. Since Hsu discloses an access control unit that can provide access to both a door and an ATM (EX-1003, ¶0001), a POSITA would have understood that Hsu stores not only the "history of access **to the door**" but also the "history of access **to the ATM**" (*i.e.*, history of transactions). A POSITA would have looked to teachings of Houvener to make use of the "history" data disclosed by Hsu. EX-1006, ¶441.

Similarly, Sanford also aims to "reduce[] fraudulent use of credit cards" by "having an identifying image captured." EX-1004, ¶0043. A POSITA would have understood that Sanford discloses the well-known practices of logging card user activities, including card information and biometric information, for auditing purposes. EX-1006, ¶442.

A POSITA would have had a **reasonable expectation of success** in this combination because Houvener expressly teaches storing and outputting transaction records for audit purposes, which were commonly in use at the time of the '039 Patent, and when combined with the Sanford-Hsu system, would result in

a working system. EX-1006, ¶443.

Further, Hsu already discloses storing "history" data in the database. Therefore, a POSITA would have understood that the Sanford-Hsu system utilizes or at least is capable of utilizing such history data. Houvener provides a specific way (and a common way) to make use of Hsu's history data. A POSITA would have understood that any modification of the Sanford-Hsu (or Sanford-Hsu-Tsukamura) system would be limited and well-known. EX-1006, ¶444.

When combining Houvener with the Sanford-Hsu (or Sanford-Hsu-Tsukamura) system, a POSITA would have understood that the card information (*e.g.,* Sanford's credit card account number) provided by step (a) in claim 3 is part of the stored transaction record. That is because Sanford's credit card account number is an obvious piece of information for "recreat[ing] a transaction" and "identify[ing]… the person initiating the transaction" as disclosed by Houvener. EX-1010, 7:60-65; EX-1006, ¶445.

E. GROUNDS #7 AND #8: Claim 17 is Rendered Obvious

The discussion below explains that the limitations of claim 17 are rendered obvious by McCalley. EX-1006, ¶¶446-455.

Ground 7 incorporates the below analysis in the context of the Sanford-Hsu system (Ground 1) in view of McCalley. Ground 1 is incorporated here. EX-1006,

¶447.

Ground 8 incorporates the below analysis in the context of the Sanford-Hsu-Tsukamura system (Ground 2) in view of McCalley. Ground 2 is incorporated here. EX-1006, ¶448.

Claim 17 requires a "**memory** [that] is incorporated in a **tamper-proof** manner in the verification station [*e.g.,* Sanford-Hsu system]."

McCalley discloses a "fingerprint sensor package" that "include[s] a reference fingerprint memory for storing reference fingerprint information." EX-1011, Abstract. Specifically, McCalley's "overall package may include a **tamper resistant housing 191** [yellow] as would be readily understood by those skilled in the art." *Id.*, 10:49-59.

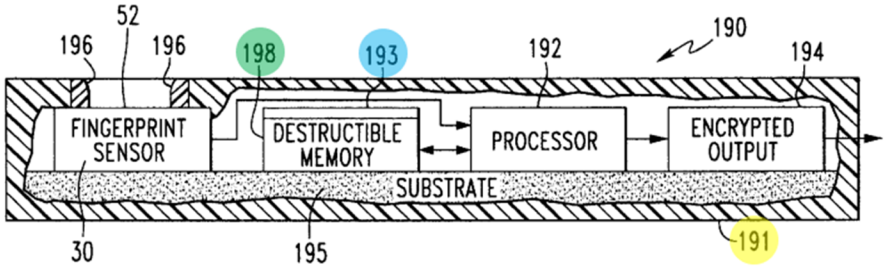


FIG. 22

EX-1011, Fig.22. McCalley also discloses that "the **memory 198** [green]…may be made to **destruct**…upon breach of the housing 191." *Id.*, 12:51-55, 12:58-67 ("The **memory 193** [blue] may also **self-destruct or empty its contents** upon exposure to light or upon removal of a sustaining electrical current."); EX-1006,

¶450.

Accordingly, McCalley discloses a memory that is incorporated in a tamper-proof manner by keeping memories in a tamper-resistant housing (temper-proof physically) and/or by making memories "destruct or be rendered secure upon breach of the housing" (tamper-proof electronically). EX-1011, 12:62, 12:53-54; EX-1006, ¶451. This is the same as described in the '039 Patent. EX-1001, 2:56-58 ("the local biometric signature memory (preferably in a mechanically and electronically tamper-proof form)"); 6:13-16.

It would have been obvious to incorporate the memory in the Sanford-Hsu (or Sanford-Hsu-Tsukamura) system in a tamper-proof manner as taught by McCalley. EX-1006, ¶452.

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. In addition, both the Sanford-Hsu (or Sanford-Hsu-Tsukamura) system and McCalley's fingerprint sensor package include a fingerprint sensor and a memory for storing captured fingerprint data. EX-1006, ¶453.

A POSITA implementing these systems would have been motivated to look to McCalley. For example, Sanford discloses that "[u]sing the ACM for PIN-less credit card transactions reduces fraudulent use of credit cards." EX-1004, ¶0043.

Especially in the context of an ATM, as disclosed by Sanford, it was well-known that tamper-proof configuration was beneficial to prevent fraud. A POSITA would have therefore looked to McCalley for details on how to make the system tamper-proof, such as having a tamper-proof housing. In addition, the Sanford-Hsu (or Sanford-Hsu-Tsukamura) system provides a biometric verification function. A POSITA would have been motivated to look to McCalley for (well-known) teachings about how to protect the components, such as the database for storing confidential biometric data, that support the biometric verification. EX-1006, ¶454.

A POSITA would have had a **reasonable expectation of success** in this combination because McCalley teaches having a tamper-proof housing and making memories self-destructible, methods commonly in use at the time of the '039 Patent, and when combined with the Sanford-Hsu system, would result in a working system. EX-1006, ¶455.

IX. CONCLUSION

Trial should be instituted, and the Challenged Claims should be cancelled as unpatentable.

Dated: June 13, 2022

Respectfully Submitted,

/ Dion M. Bregman /
Dion Bregman (Reg. No. 45,645)

U.S. PATENT NO. 8,620,039 – Claim Listing

No.	Claim Elements
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.
2[P]	A method of obtaining verified access to a process, the method comprising the steps of:
2[A]	storing a biometric signature according to the enrolment method of claim 1;
2[B]	subsequently presenting card information and a biometric signature; and
2[C]	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.
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.
Claim 4	A method according to claim 3, wherein the card device is one of: a card in which the card information is encoded in a magnetic strip; a card in which the card information is encoded in a bar code; a smart card in which the card information is stored in a solid state memory on the smart card; and a key fob adapted to provide the card information by transmitting a wireless signal to the verification station.
Claim 5	A method according to claim 3, wherein: 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.
Claim 6	A method according to claim 3, 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.
Claim 7	A method according to claim 6, wherein at least one of the steps (db) and (eb) comprise at least one of the further steps of: inputting information from a keypad to the verification station; and outputting at least some of the information input from the keypad.
Claim 8	A method according to claim 7, wherein the information outputted is communicated to one of: a service provider for providing a service dependent upon receipt of the outputted information; and an apparatus for providing access to a service dependent upon receipt of the outputted information.
Claim 9	A method according to any one of claims claim 6, 7 and 8 wherein the information outputted is communicated to one of: a service provider for providing a service dependent upon receipt of the outputted

	information; and an apparatus for providing access to a service dependent upon receipt of the outputted information.
Claim 10	A method according to claim 3, wherein the step (ec) further comprises outputting information indicating that the user of the card device is not authorised authorized.
Claim 11	A method according to claim 10, wherein the information outputted is communicated to one of: a service provider for providing a service dependent upon receipt of the outputted information; and an apparatus for providing access to a service dependent upon receipt of the outputted information.
Claim 12	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.
13[P]	A biometric card pointer enrolment system comprising:
13[A]	a card device reader for receiving card information;
13[B]	a biometric reader for receiving the biometric signature;
13[C]	means for defining, dependent upon the received card information, a memory location in a local memory external to the card;
13[D]	means for determining if the defined memory location is unoccupied; and
13[E]	means for storing, if the memory location is unoccupied, the biometric signature at the defined memory location.
14[P]	A biometric card pointer verified access system comprising:
14[A]	the biometric card pointer enrolment system of claim 13; and
14[B]	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 if said subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.
15[P]	A verification station for securing a process, the verification station comprising:
15[A]	a card device reader for receiving card information from a card device coupled to the verification station;
15[B]	a biometric signature reader for receiving a biometric signature provided to the verification station;

15[C]	means for determining if the provided card information has been previously provided to the verification station;
15[D(P)]	means, if the provided card information has not been previously provided to the verification station, for:
15[D(1)]	storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and
15[D(2)]	performing the process dependent upon the received card information;
15[E(P)]	means, if the provided card information has been previously provided to the verification station, for:
15[E(1)]	comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;
15[E(2)]	if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and
15[E(3)]	if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.
Claim 16	A verification station according to claim 15, wherein the card device reader is one of: a reader for a card in which the card information is encoded in a magnetic strip; a reader for a card in which the card information is encoded in a bar code; a reader for a smart card in which the card information is stored in a solid state memory on the smart card; and a receiver for a key fob adapted to provide the card information by transmitting a wireless signal to the verification station.
Claim 17	A verification station according to claim 15, wherein the memory is incorporated in a tamper-proof manner in the verification station.
18[P]	A non-transitory computer readable medium having recorded thereon a computer program for directing a processor to execute a method for securing a process at a verification station, said program comprising:
18[A]	code for determining if card information, provided to a card device reader incorporated into the verification station, has been previously provided to the verification station;
18[B(P)]	code, if the provided card information has not been previously provided to the verification station, for:
18[B(1)]	storing a biometric signature, inputted to a biometric signature reader incorporated into the verification station, in a memory incorporated

	into the verification station, at a memory location defined by the provided card information; and
18[B(2)]	performing the process dependent upon the received card information;
18[C(P)]	code, if the provided card information has been previously provided to the verification station, for:
18[C(1)]	comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;
18[C(2)]	if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and
18[C(3)]	if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.
19[P]	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:
19[A]	code for receiving card information;
19[B]	code for receiving the biometric signature;
19[C]	code for defining, dependent upon the received card information, a memory location in a local memory external to the card;
19[D]	code for determining if the defined memory location is unoccupied; and
19[E]	code for storing, if the memory location is unoccupied, the biometric signature at the defined memory location.
20[P]	A non-transitory computer readable medium having recorded thereon a computer program for directing a processor to execute a method of obtaining verified access to a process, the program comprising:
20[A]	code for storing a biometric signature according to the enrolment method of claim 19;
20[B]	code for subsequently presenting card information and a biometric signature; and
20[C]	code for 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.

CERTIFICATION OF COMPLIANCE WITH TYPE-VOLUME LIMITS

This Petition includes 13,956 words as counted by Microsoft Word and is therefore in compliance with the 14,000-word limit established by 37 C.F.R. 42.24(a)(1)(i). Accordingly, pursuant to 37 C.F.R. 42.24(d), lead counsel for the Petitioners hereby certify that this petition complies with the type-volume limits established for a petition requesting IPR.

Dated: June 13, 2022

Respectfully Submitted,

/ Dion M. Bregman /
Dion Bregman (Reg. No. 45,645)

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. 42.6(4) and 42.105, lead counsel for Petitioners hereby certify that on June 13, 2022, copies of this Petition and all supporting exhibits were sent via Priority Mail Express to the correspondence address of record for the '039 patent:

Crowell/BGL
P.O. Box 10395
Chicago, IL 60610

A courtesy copy of this Petition and supporting exhibits was also served via email on June 13, 2022 on Patent Owner's counsel of record in the district court litigation against Apple involving this patent:

Ben Roxborough (ben.roxborough@klgates.com)
George C. Summerfield (george.summerfield@klgates.com)
James A. Shimota (jim.shimota@klgates.com)
Stewart Mesher (stewart.mesher@klgates.com)
Elizabeth Abbott Gilman (beth.gilman@klgates.com)
Jonah Heemstra (jonah.heemstra@klgates.com)

Dated: June 13, 2022

Respectfully Submitted,

/ Dion M. Bregman /
Dion Bregman (Reg. No. 45,645)