

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

DECLARATION OF STUART LIPOFF

U.S. PATENT NO. 8,620,039 (CLAIMS 1-20)

Contents

I.	ENGAGEMENT	1
II.	PROFESSIONAL BACKGROUND.....	2
III.	MATERIALS REVIEWED	6
IV.	DESCRIPTION OF THE RELEVANT TIMEFRAME, THE RELEVANT FIELD, AND A PERSON OF ORDINARY SKILL IN THE ART.....	7
V.	OVERVIEW OF THE '039 PATENT	8
VI.	CLAIM CONSTRUCTION	15
A.	Terms to be Construed	15
1.	Card Information “Defining / Defines” a Memory Location	15
2.	“unoccupied”	18
B.	Means-Plus-Function Limitations	19
C.	Previously-Construed Terms.....	19
1.	“biometric card pointer system”	20
2.	“biometric card pointer enrollment system”	20
D.	Other Previously-Agreed-On Terms	20
1.	“dependent upon”	20
2.	“biometric signature”	21
VII.	ANTICIPATION	21
VIII.	OBVIOUSNESS.....	21
IX.	OPINIONS REGARDING PATENTABILITY	22
X.	THE CLAIMS OF THE '039 PATENT ARE INVALID.....	25
A.	IPR2022-001093 GROUND #1: Claims 1, 2, 13, 14, 19, and 20 are rendered obvious by Hsu and Sanford	25
1.	Claim 1 is rendered obvious by Hsu and Sanford	25
2.	Claim 2 is rendered obvious by Hsu and Sanford	52
3.	Claim 13 is rendered obvious by Hsu and Sanford	62

4.	Claim 14 is rendered obvious by Hsu and Sanford	70
5.	Claim 19 is rendered obvious by Hsu and Sanford	73
6.	Claim 20 is rendered obvious by Hsu and Sanford	84
B.	IPR2022-001093 GROUND #2: Claims 1, 2, 13, 14, 19, and 20 are rendered obvious by Hsu, Sanford, and Tsukamura	87
1.	Claim 1 is rendered obvious by Hsu, Sanford, and Tsukamura.....	87
2.	Claim 2 is rendered obvious by Hsu, Sanford, and Tsukamura.....	105
3.	Claim 13 is rendered obvious by Hsu, Sanford, and Tsukamura.....	106
4.	Claim 14 is rendered obvious by Hsu, Sanford, and Tsukamura.....	110
5.	Claim 19 is rendered obvious by Hsu, Sanford, and Tsukamura.....	112
6.	Claim 20 is rendered obvious by Hsu, Sanford, and Tsukamura.....	113
C.	IPR2022-001094 GROUND #1: 3, 4, 6-11, 15, 16, and 18 are Rendered Obvious by Sanford and Hsu	114
1.	Claim 3 is rendered obvious by Sanford and Hsu	114
2.	Claim 4 is rendered obvious by Sanford and Hsu	143
3.	Claim 6 is rendered obvious by Sanford and Hsu	144
4.	Claim 7 is rendered obvious by Sanford and Hsu	150
5.	Claim 8 is rendered obvious by Sanford and Hsu	153
6.	Claim 9 is rendered obvious by Sanford and Hsu	155
7.	Claim 10 is rendered obvious by Sanford and Hsu	156
8.	Claim 11 is rendered obvious by Sanford and Hsu	158
9.	Claim 15 is rendered obvious by Sanford and Hsu	159
10.	Claim 16 is rendered obvious by Sanford and Hsu	170
11.	Claim 18 is rendered obvious by Sanford and Hsu	171

D.	IPR2022-001094 GROUND #2: Claims 3, 4, 6-11, 15, 16, and 18 are Rendered Obvious by Sanford, Hsu, and Tsukamura	172
1.	Claim 3 is rendered obvious by Sanford, Hsu, and Tsukamura.....	172
2.	Claims 4 and 6-11 are rendered obvious by Sanford, Hsu, and Tsukamura.....	182
3.	Claim 15 is rendered obvious by Sanford, Hsu, and Tsukamura.....	182
4.	Claim 16 is rendered obvious by Sanford, Hsu, and Tsukamura.....	185
5.	Claim 18 is rendered obvious by Sanford, Hsu, and Tsukamura.....	185
E.	IPR2022-001094 GROUNDS #3 and #4: Claim 5 is rendered obvious	187
F.	IPR2022-001094 GROUNDS #5 and #6: Claim 12 is rendered obvious	195
G.	IPR2022-001094 GROUNDS #7 and #8: Claim 17 is rendered obvious	199
XI.	CONCLUDING STATEMENTS.....	202

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 <i>et al.</i> (“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. 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 <i>et al.</i> (“McCalley”)
Ex. 1012	Claim Construction Order in <i>CPC Patent Technologies Pty Ltd v. Apple Inc.</i> , WDTX-6-21-cv-00165-ADA, Dkt. No. 76 (“Apple CC Order”)
Ex. 1013	Joint Claim Construction Statement in <i>CPC Patent Technologies Pty Ltd v. Apple Inc.</i> , WDTX-6-21-cv-00165-ADA, Dkt. No. 57 (“Apple Joint CC Statement”)
Ex. 1014	Excerpts from Bloomsbury English Dictionary, 2 nd Edition (2004)
Ex. 1015	Excerpts from The Chambers Dictionary, 4 th 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, Stuart J. Lipoff, declare as follows:

I. ENGAGEMENT

1. I reside at 2877 Paradise Road Unit 205, Las Vegas, NV 89109.
2. I have been retained by ASSA ABLOY AB, ASSA ABLOY Inc., ASSA ABLOY Residential Group, Inc., August Home, Inc., HID Global Corporation, and ASSA ABLOY Global Solutions, Inc. (“Petitioners”) in connection with the above-captioned petition for *Inter Partes* Review (“IPR”) of U.S. Patent No. 8,620,039 to Christopher John Burke (“the ’039 Patent,” Ex. 1001). I understand the ’039 Patent is currently assigned to CPC Patent Technologies Pty Ltd. (“Patent Owner”).
3. I have been asked by Petitioners to offer opinions regarding the ’039 Patent, including the unpatentability of claims 1-20 (which I may refer to subsequently as the “challenged claims” or the “’039 Patent claims”) in view of certain prior art. This declaration sets forth the opinions I have reached to date regarding these matters.
4. I am being compensated by Petitioners at my standard hourly consulting rate for my time spent on this matter. My compensation is not contingent on the outcome of the IPR or on the substance of my opinions.
5. I have no financial interest in Petitioners or Patent Owner.

II. **PROFESSIONAL BACKGROUND**

6. As shown in my *curriculum vitae* (“CV”), a true and correct copy of which is attached hereto as Ex. 1007, I am currently the president of IP Action Partners Inc. and have over 50 years of experience in a wide variety of technologies and industries relating to data communications, including data communications over wireless and cable systems networks.

7. I earned a B.S. degree in Electrical Engineering in 1968 from Lehigh University and a second B.S. degree in Engineering Physics in 1969, also from Lehigh University. I also earned a M.S. degree in Electrical Engineering from Northeastern in 1974 and an MBA degree from Suffolk University in 1983.

8. I am currently the president of IP Action Partners Inc., which is a consulting practice serving the telecommunications, information technology, media, electronics, and e-business industries.

9. I hold a Federal Communications Commission (“FCC”) General Radiotelephone License and a Certificate in Data Processing (“CDP”) from the Association for Computing Machinery (“ACM”)-supported Institute for the Certification of Computing Professionals (“ICCP”), and I am a registered professional engineer (by examination) in the State of Nevada and the Commonwealth of Massachusetts.

10. I am a fellow of the IEEE Consumer Electronics, Communications, Computer, Circuits, and Vehicular Technology Groups. I am also a member of the IEEE Consumer Technology Society Board of Governors, and was the Boston Chapter Chairman of the IEEE Vehicular Technology Society. I previously served as 1996-1997 President of the IEEE Consumer Electronics Society, have served as Chairman of the Society's Technical Activities and Standards Committee, as VP of Publications for the Society, and currently as VP of Industry and Standards for the Society. I have also served as an Ibuka Award committee member.

11. I have also presented papers at many IEEE and other meetings. A listing of my publications is included as part of my CV, which is attached as Exhibit 1007. For example, in Fall 2000, I served as general program chair for the IEEE Vehicular Technology Conference on advanced wireless communications technology, and I have organized sessions at The International Conference on Consumer Electronics and was the 1984 program chairman. I also conducted an eight-week IEEE sponsored short course on Fiber Optics System Design. In 1984, I was awarded IEEE's Centennial Medal and in 2000, I was awarded the IEEE's Millennium Medal.

12. As Vice President and Standards Group Chairman of the Association of Computer Users ("ACU"), I served as the ACU representative to the ANSI X3 Standards Group. For the FCC's Citizens advisory committee on Citizen's Band

(“CB”) radio (“PURAC”), I served as Chairman of the task group on user rule compliance. I have been elected to membership in the Society of Cable Television Engineers (“SCTE”), the ACM, and The Society of Motion Picture and Television Engineers (“SMPTE”). I also served as a member of the USA advisory board to the National Science Museum of Israel, presented a short course on international product development strategies as a faculty member of Technion Institute of Management in Israel, and served as a member of the board of directors of The Massachusetts Future Problem Solving Program.

13. I am a named inventor on seven United States patents and have several publications on data communications topics in Electronics Design, Microwaves, EDN, The Proceedings of the Frequency Control Symposium, Optical Spectra, and IEEE publications.

14. For 25 years, I worked for Arthur D. Little, Inc. (“ADL”), where I became Vice President and Director of Communications, Information Technology, and Electronics (“CIE”). Prior to my time at ADL, I served as a Section Manager for Bell & Howell Communications Company for four years, and prior to that, as a Project Engineer for Motorola’s Communications Division for three years.

15. At ADL, I was responsible for the firm’s global CIE practice in laboratory-based contract engineering, product development, and technology based

consulting. At both Bell & Howell and Motorola, I had project design responsibility for wireless communication and paging products.

16. During my 53 years in the practice of engineering research and product development, I have engaged in a number of projects that have provided me with relevant experience and expertise in a number of the foundation technologies and the industries within the scope of the '039 Patent. These projects have included, for example, topics in: motor operated door controllers, wireless communications, wireless remote controls, access control security systems, data communications, and devices incorporating microprocessors.

17. I have worked on a number of security and alarm products. For the Philadelphia Police Department, I designed a wireless address alarm system that was also deployed by The White House Communications Agency. I have also specified and managed aspects of the procurement of complex keypad based access control systems for use in secure areas of electric power utilities and industrial computer rooms.

18. For Symbol Technology, I contributed to the design of the MAC layer protocol of a wireless local area network system (WLAN) that pre-dated the IEEE 802.11 standard. My protocol design was submitted to the IEEE 802.11 standards committee with portions incorporated into the final specification.

19. Working with Cambridge Consultants Ltd (the UK subsidiary of the USA based Arthur D Little Inc), I consulted on several developments of Bluetooth related hardware and software stacks. This development was spun off to Cambridge Silicon Radio (CSR) to which I continued to provide consulting reports.

20. In my capacity as chairman of The IEEE Consumer Electronics Society Standards Committee, I followed the developments of both the IEEE 802.15 Bluetooth and IEEE 802.11 WiFi standards, as well as the IEEE Home Radio Frequency (HomeRF™) Working Group.

21. I have designed products and systems that incorporated microprocessors and microcomputers across multiple products and industry applications, including toys and games, industry controllers, motor controllers, and consumer products.

22. Additional information regarding my background, qualifications, publications, and presentations is provided in my CV, which is included as Ex. 1007.

III. MATERIALS REVIEWED

23. In forming my opinions, I have reviewed the '039 Patent and considered each of the documents listed in the Exhibit List above. In reaching my opinions, I have relied upon my experience in the field and also considered the

viewpoint of a person of ordinary skill in the art at the time of the earliest claimed priority date of the '039 Patent, *i.e.*, 2005. As explained below, I am familiar with the level of a person of ordinary skill in the art regarding the technology at issue as of that time.

IV. DESCRIPTION OF THE RELEVANT TIMEFRAME, THE RELEVANT FIELD, AND A PERSON OF ORDINARY SKILL IN THE ART

24. I understand that the '039 Patent was filed on August 10, 2006, and has an earliest possible priority date of August 12, 2005. I further understand that there is no claim to earlier priority. Thus, for purposes of my analysis, I have treated the time of the invention as August 12, 2005. I reserve the right to update my analysis should Patent Owner assert an earlier priority date.

25. I have received and understand the specification, claims, and file history of the '039 Patent. Based on my review of these materials, I believe that the relevant field for purposes of my analysis is secure access systems.

26. In my opinion, a person of 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. My opinions presented herein are as viewed through the eyes of a person of ordinary skill in the art prior to August 12, 2005.

V. OVERVIEW OF THE '039 PATENT

27. I have reviewed the '039 Patent and understand that Christopher John Burke is named as the inventor on this patent. Mr. Burke's 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.

28. 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). Ex. 1001, 7:50-53. 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.

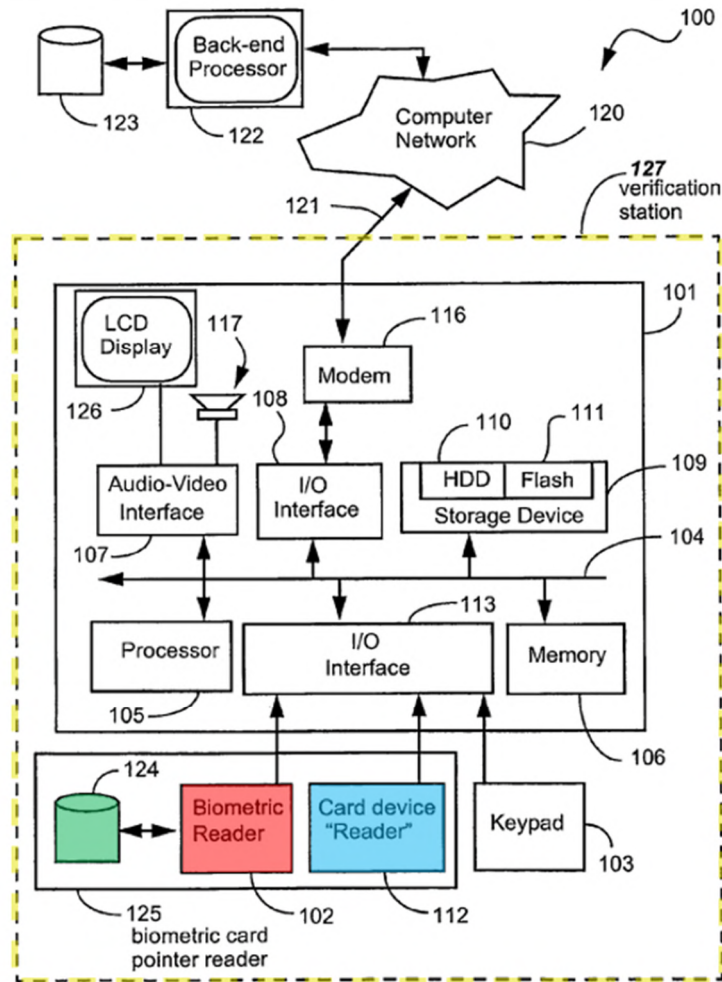


Fig. 3

Ex. 1001, Fig. 3. As a general note, I added emphasis and coloring throughout this declaration unless otherwise noted.

29. 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. Ex. 1001, 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.

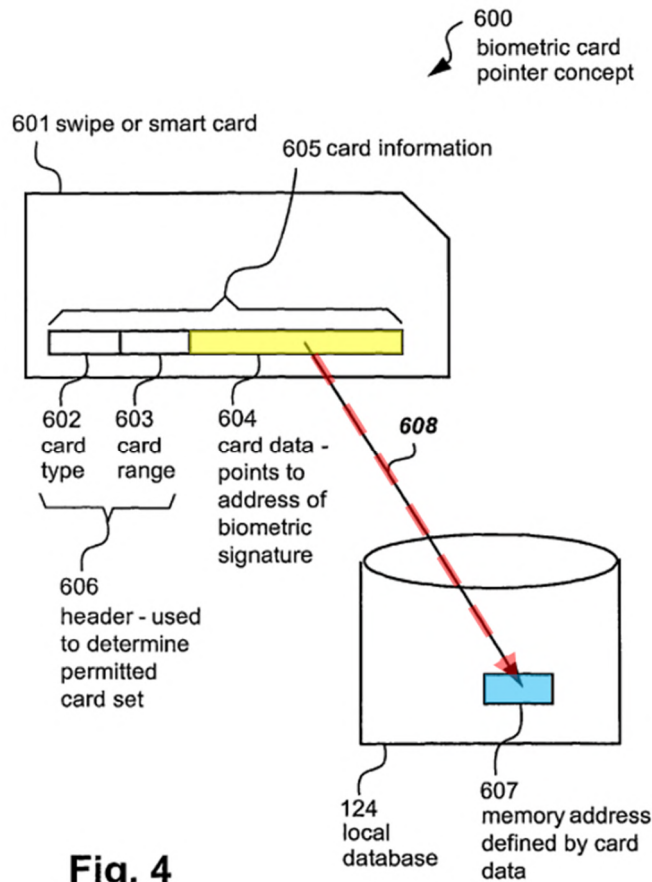


Fig. 4

Ex. 1001 Fig. 4. “Once verification is confirmed, the card information 605 is transferred from the verification station 127 [Fig. 3 above] to the back-end processor 122 [Fig. 3 above] for completion of the transaction.” *Id.*, 7:56-59.

30. The patent discloses many forms of biometric signatures including “fingerprints,” “face, iris, or other unique signature.” Ex. 1001, 7:45-47.

31. 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. In finding claim 3 allowable, 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 during prosecution of any of the prior art references cited herein.

32. In my opinion, there is nothing novel about the system for providing secure access recited in the ’039 Patent claims or anything else that distinguishes it from other earlier systems for providing secure access.

33. For example, Hsu (Ex. 1003) discloses authenticating a user using both the user’s card information and the user’s biometric signature “for controlling access to building doors or to machines, such as automatic teller machines (ATMs).” Ex. 1003, Abstract, ¶0001, ¶0006.

34. Just like the ’039 Patent, Hsu discloses using the card information to efficiently access the user’s stored biometric information. For example, as shown in Fig. 3 below, “[t]he user places his or her card in the reader 62 [blue], which

retrieves an account number or other type of identification unique to the user,” which is then used “to access the fingerprint database 44 [green] and obtain a user reference fingerprint....” Ex. 1003, ¶0024.

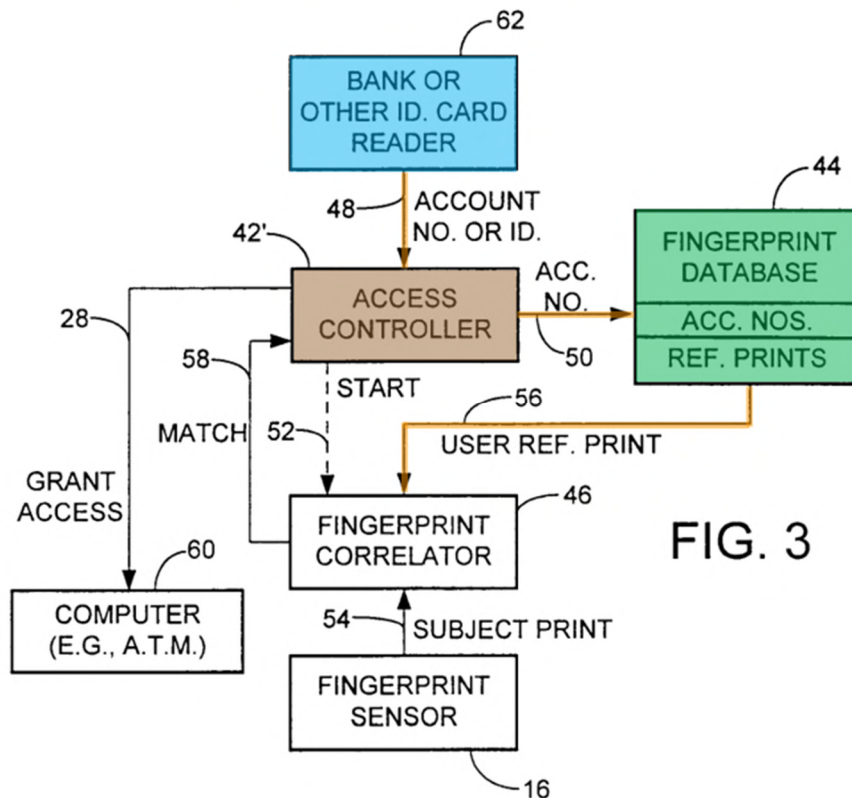


FIG. 3

Ex. 1003, Fig. 3; *see also* Fig. 2. Further, “[t]he **database** [green] is basically a **table that associates each user number with a stored fingerprint image....**” *Id.*, ¶0020. The retrieved “user reference fingerprint” is then compared with a “sensed fingerprint image.” *Id.*, ¶¶0024-25. “A successful match... results in access to the door or machine being granted to the user,” such as for “conduct[ing] banking transactions”. *Id.*, Abstract, ¶0024.

35. Just like the '039 Patent, Hsu recognizes that such an implementation enables the **“fingerprint matching... [to] be achieved rapidly” by not having to “compare a sensed fingerprint image with many possible stored reference images.”** Ex. 1003, ¶0013; ¶0004.

36. As another example, Sanford (Ex. 1004) teaches “a method for **conducting a [] card transaction” using biometric verification**, for example, at “an ATM machine,” just like the '039 Patent and Hsu. Ex. 1004, Abstract, ¶0004, ¶¶0008-09, ¶0016. Sanford also discloses multiple types of biometrics, such as “facial biometrics,” “iris, voice signature, and fingerprint.” *Id.*, ¶0020.

37. Like the '039 Patent, Sanford discloses that “[t]he user may begin the process by inserting or swiping a credit card into the credit card reader.” Ex. 1004, ¶0024. It is then “determine[ed] if the user is enrolled.” *Id.*, ¶0025. If yes, “an image of the user” is taken and compared to “a pre-existing profile [] for the user.” *Id.*, ¶0026, ¶0019. If a match is found, the user may then proceed with the remaining steps of the transaction. *Id.*, ¶0030. If the user is not enrolled, he or she is directed to the enrollment process. *Id.*, ¶0025.

38. As another example, Tsukamura (Ex. 1005) teaches a simplistic way to store and access fingerprint templates for “personal authentication.” Ex. 1005, Abstract. Tsukamura discloses storing fingerprint templates in consecutive, fixed-length memory locations.

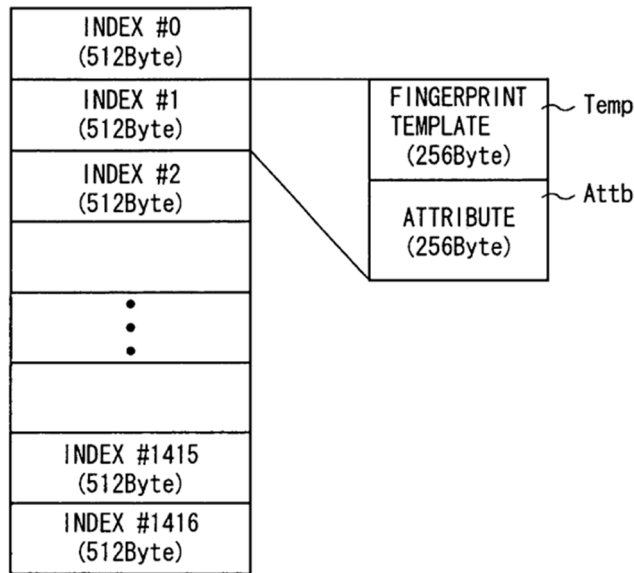


FIG. 3

Ex. 1005, Fig. 3. **Each fingerprint template is stored “at an index (address) specified by the index number N index within the collation flash ROM.”** *Id.*, 3:28-34. This is a well-known way to speed up data access by reading/writing directly to defined locations within a memory.

39. With regard to dependent claim 5, Leu (Ex. 1008 and Ex. 1009) teaches the simple concept of performing certain activity only if a card belongs to a known set of cards.

40. With regard to dependent claim 12, Houvener (Ex. 1010) teaches the well-known concept of outputting and logging information for audit purposes.

41. With regard to dependent claim 17, McCalley (Ex. 1011) teaches packaging a memory in a tamper-proof manner.

VI. CLAIM CONSTRUCTION

42. I understand that claim construction is the process of determining the meaning of a term or phrase in a patent claim. I understand that the proper construction of a term is how a POSITA would have understood the term based on its use in the claims, specification, and file history of the patent. I further understand that the claims are construed before the Board according to the same claim construction standard that applies in district courts. I have followed these principles in my analysis throughout this declaration. I discuss below the meaning of certain claim terms that I have applied in forming my opinions.

A. Terms to be Construed

1. Card Information “Defining / Defines” a Memory Location

43. The claims include the following limitations relating to card information defining a memory location:

Claims	Limitation
Independent claims 1, 13, and 19	“ defining , dependent upon the received card information, a memory location in a local memory external to the card”
Dependent claims 2, 14 and 20	“ memory location...defined by the

	subsequently presented card information”
Independent claims 3, 15 and 18	“ memory location defined by the provided card information”

I believe these limitations are susceptible to two different interpretations regarding what it means for the “**memory location**” to be “**defined**” by the card information.

44. **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.

45. **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.

46. I believe the Second Construction was intended by the patentee. 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.

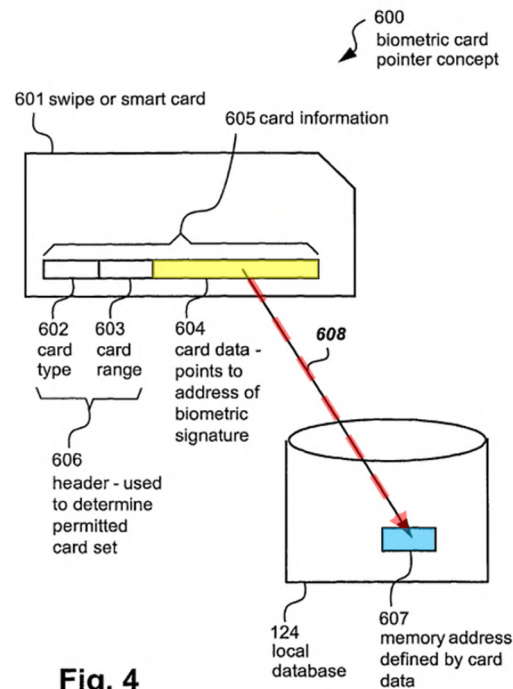


Fig. 4

Ex. 1001 Fig. 4. Moreover, based on my review of the patent specification, I have observed that 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...”).

47. 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) for the user’s biometric signature. I have also noted that Patent Owner appears to be asserting infringement claims under the First Construction. *See Ex. 1016, p. 3.*

48. In my opinion, the ’039 Patent claims are unpatentable under either interpretation. Under the First Construction, the claims are invalid under IPR2202-01093 Ground 1 (Hsu + Sanford) and IPR2202-01094 Grounds 1, 3, 5, 7 (Sanford + Hsu). Under the Second Construction, the claims are invalid under IPR2202-01093 Ground 2 (Hsu + Sanford + Tsukamura) and IPR2202-01094 Grounds 2, 4, 6, and 8 (Sanford + Hsu + Tsukamura).

2. “unoccupied”

49. Independent claims 1, 13, and 19 recite “determining if the defined memory location is **unoccupied**.” The term “occupied” is explicitly defined in the specification:

The term **“occupied”** in this context means that the **memory location** in question **has been used** in the enrolment process for a user, and that the information

stored at the memory location in question has not been deleted by a BCP system administrator.

Ex. 1001, 9:29-33. Therefore, it is clear to me that the opposite term “**unoccupied**” should likewise be construed based on this definition, as follows: a **memory location** that has not been used in the enrollment process for a user, or the information stored at the memory location has been deleted. *Id.*

B. Means-Plus-Function Limitations

50. I understand that Judge Albright (WDTX) construed two means-plus-function limitations from the challenged claims in district court proceedings. I reviewed the constructions, but I do not provide any opinion agreeing or disagreeing with the constructions. Nonetheless, for the purpose of this declaration, I applied the constructions for these terms as identified in my analysis below. It is my understanding that in the context of the '039 Patent claims and the intrinsic evidence, “code for” is an equivalent recitation for “means for.” The '039 Patent’s otherwise identical language for some “code for” and “means for” terms confirms to me that that they should be treated equivalently.

C. Previously-Construed Terms

51. I understand that Judge Albright construed the following terms in district court proceedings. I reviewed the constructions for the following terms, but I do not provide any opinion agreeing or disagreeing with these constructions.

I do not believe that these constructions are material to my opinions regarding unpatentability of the '039 Patent claims

52. Nonetheless, for the purpose of this declaration, I applied the constructions for these terms as listed below.

1. “biometric card pointer system”

53. “Nonlimiting preamble term with no patentable weight.” Ex. 1012, p1.

2. “biometric card pointer enrollment system”

54. “Nonlimiting preamble term with no patentable weight.” Ex. 1012, p1.

D. Other Previously-Agreed-On Terms

55. I understand that Patent Owner and Apple, Inc. agreed to the constructions for the following terms in district court proceedings. I reviewed the constructions for the following terms, but I do not provide any opinion agreeing or disagreeing with these constructions and I do not believe that they are material to my opinions regarding unpatentability of the '039 Patent claims.

1. “dependent upon”

56. “plain and ordinary meaning, defined as ‘contingent on or determined by’.” Ex. 1013, p2.

2. **“biometric signature”**

57. “plain and ordinary meaning.” Ex. 1013, p2.

VII. ANTICIPATION

58. I have been instructed as to the definition of “anticipation” in the context of the patent laws.

59. I understand that anticipation of a claim requires that every element of a claim be disclosed expressly or inherently in a single prior art reference, in combination, as claimed. I understand that a single prior art reference may anticipate claims without expressly disclosing a feature of the claimed invention if that feature is necessarily present, or inherent, in that reference. I understand that a reference is read from the perspective of one of ordinary skill at the time of the invention.

VIII. OBVIOUSNESS

60. I have been instructed as to the definition of “obviousness” in the context of the patent laws.

61. It is my understanding that obviousness is a question of law based on underlying factual issues including the content of the prior art and the level of skill in the art. I understand that for a single reference or a combination of references to render the claimed invention obvious, a person of ordinary skill in the art must

have been able to arrive at the claims by altering or combining the applied references.

62. I also understand that when considering the obviousness of a patent claim, one should consider whether a teaching, suggestion, or motivation to combine the references exists to avoid impermissibly applying hindsight when considering the prior art. I understand this test should not be applied rigidly, but that the test can be important to avoid such hindsight.

IX. OPINIONS REGARDING PATENTABILITY

63. In my opinion, claims 1, 2, 13, 14, 19, and 20 are rendered obvious by the Hsu-Sanford combination or the Hsu-Sanford-Tsukamura combination. Additionally, claims 3, 4, 6-11, 15, 16, and 18 are rendered obvious by the Sanford-Hsu combination or the Sanford-Hsu-Tsukamura combination. Claim 5 is rendered obvious by the Sanford-Hsu combination or the Sanford-Hsu-Tsukamura combination, further in view of Leu. Claim 12 is rendered obvious by the Sanford-Hsu combination or the Sanford-Hsu-Tsukamura combination, further in view of Houvener. Claim 17 is rendered obvious by the Sanford-Hsu combination or the Sanford-Hsu-Tsukamura combination, further in view of McCalley.

64. I have based my opinion on the following references:

- **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**. I understand that Hsu is prior art to the ’039 Patent.

- **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**. I understand that Sanford is prior art to the ’039 Patent.

- **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. I understand that Tsukamura is prior art to the ’039 Patent.

- **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**. I understand that Leu is prior art to the ’039 Patent.

- **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**. I understand Houvener is prior art to the ’039 Patent.

- **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**. I understand McCalley is prior art to the ’039 Patent.

65. In my opinion, claims 1-20 of the ’039 Patent are unpatentable based on the following grounds:

(1) Claims 1, 2, 13, 14, 19, and 20 are rendered obvious by Hsu in view of Sanford;

(2) Claims 1, 2, 13, 14, 19, and 20 are rendered obvious by Hsu in view of Sanford and further in view of Tsukamura;

(3) Claims 3, 4, 6-11, 15, 16, and 18 are rendered obvious by Sanford in view of Hsu;

(4) Claims 3, 4, 6-11, 15, 16, and 18 are rendered obvious by Sanford in view of Hsu and further in view of Tsukamura;

(5) Claim 5 is rendered obvious by Sanford in view of Hsu and further in view of Leu.

(6) Claim 5 is rendered obvious by the Sanford-Hsu-Tsukamura combination further in view of Leu.

(7) Claim 12 is rendered obvious by Sanford in view of Hsu and further in view of Houvener.

(8) Claim 12 is rendered obvious by the Sanford-Hsu-Tsukamura combination further in view of Houvener.

(9) Claim 17 is rendered obvious by Sanford in view of Hsu and further in view of McCalley.

(10) Claim 17 is rendered obvious by the Sanford-Hsu-Tsukamura combination further in view of McCalley.

X. THE CLAIMS OF THE '039 PATENT ARE INVALID

A. IPR2022-001093 GROUND #1: Claims 1, 2, 13, 14, 19, and 20 are rendered obvious by Hsu and Sanford

66. It is my opinion that claims 1, 2, 13, 14, 19, and 20 are rendered obvious by Hsu in view of Sanford because it would have been obvious for one of skill in the art at the time of the invention to modify Hsu in view of Sanford to arrive at the claimed purported invention.

1. Claim 1 is rendered obvious by Hsu and Sanford

67. In my opinion, claim 1 is unpatentable because it is rendered obvious by Hsu and Sanford. Claim 1 of the '039 Patent recites the following. I address each of these in my analysis below.

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

[A] receiving card information;

- [B] receiving the biometric signature;
- [C] defining, dependent upon the received card information, a memory location in a local memory external to the card;
- [D] determining if the defined memory location is unoccupied; and
- [E] storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

68. **Preamble 1[P]**. It is my opinion that Hsu discloses “a method of enrolling in a biometric card pointer system.”

69. *First*, it is my opinion that Hsu discloses a “biometric card pointer system.” As shown in Fig. 1 below, Hsu discloses an access control unit 14 (yellow) that, upon verification, “unlocks the door 12 and allows the user 10 to enter.” Ex. 1003, ¶0018; VI.C.1.

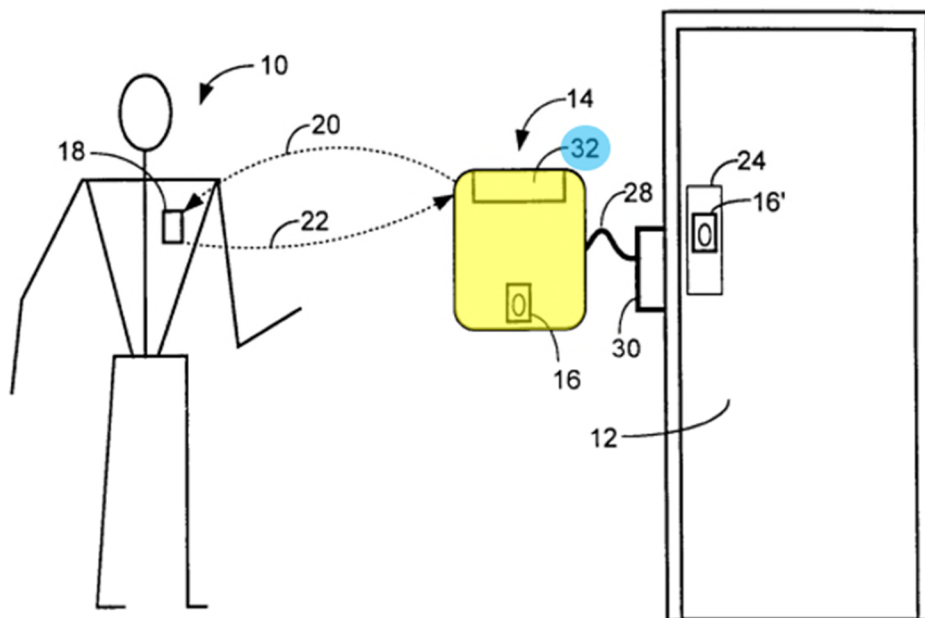
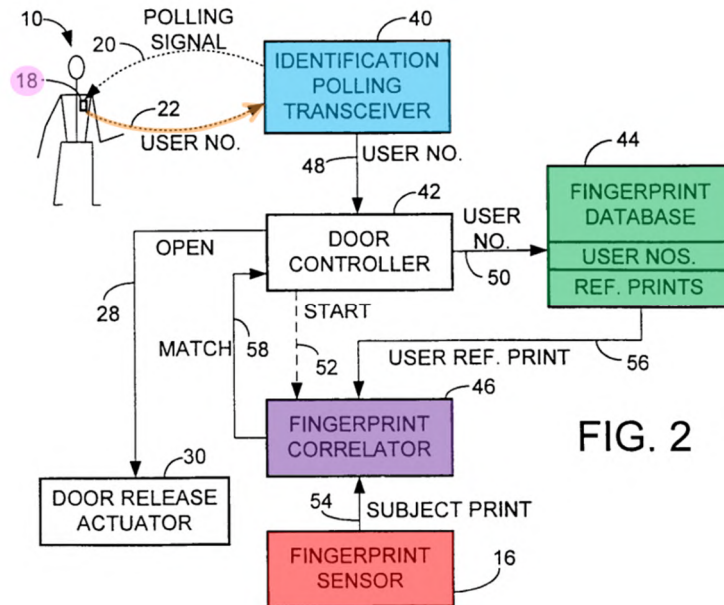


FIG. 1

Id., Fig. 1. Specifically, “FIG. 2 shows the principal components of the access control unit 14.” *Id.*, ¶0020.



Id., Fig. 2. Hsu discloses that the access control unit 14 includes an identification polling transceiver 40 (blue), which transmits polling signals to, and receives reply signals from, the **user’s badge 18** (pink). *Id.*, ¶0020. “[A] reply signal [orange] [] includes the user’s identification number or user number.” *Id.* If a user does not have a badge or the badge is not working, “[t]he access control unit 14 also includes an **integral card reader 32**” (blue) as shown in Fig. 1 above. *Id.*, ¶0018.

70. Hsu also discloses a different configuration of the access control unit, as illustrated in Figure 3:

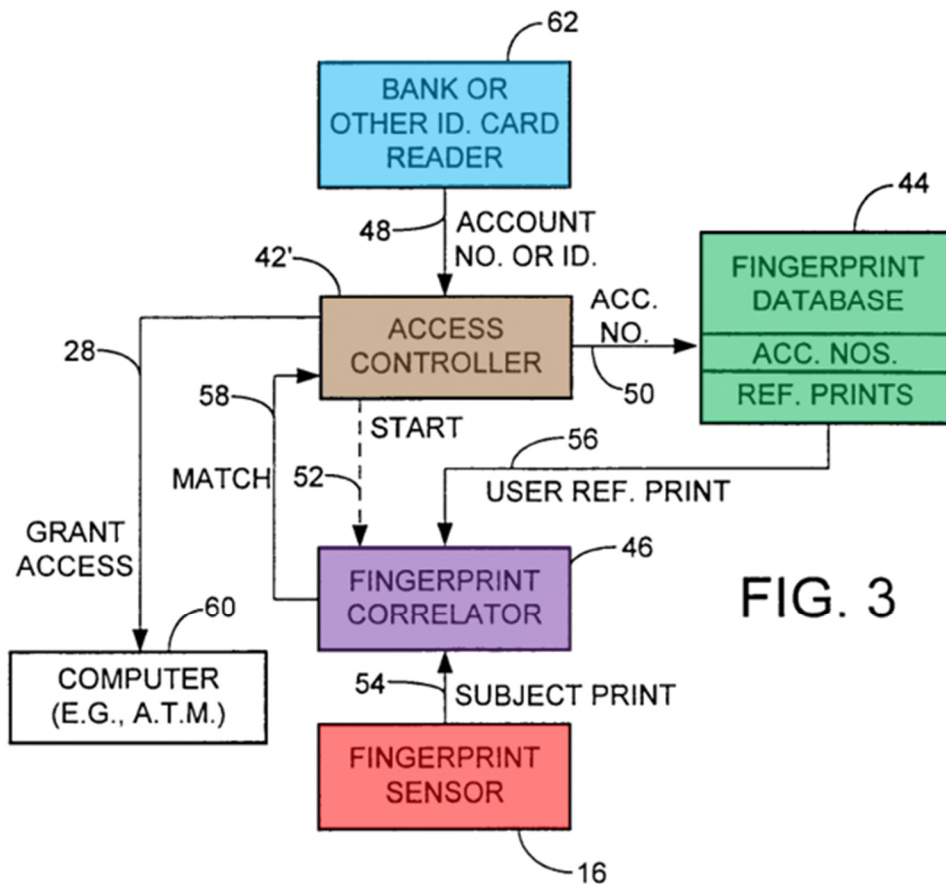


FIG. 3

Ex. 1003, Fig. 3. As shown, “this system has a **bank card reader 62** [blue] or a similar device for reading some type of **identification card.**” *Id.*, ¶0024. When “[t]he user places his or her card in the reader 62 [blue],” “an **account number** or other type of identification unique to the user” is retrieved. *Id.*

71. In both embodiments, the access control unit 14 includes an access controller (42 or 42’) that “uses the account number [or user number] ... to access the **fingerprint database 44** [green] and obtain a **user reference fingerprint.**” *Id.*, ¶0020, ¶0024.

72. As confirmed by the '039 Patent, a fingerprint is a type of **biometric signature**. Ex. 1001, 7:45-47. Therefore, the bank card in Hsu serves as a pointer to biometric information (*i.e.*, reference fingerprint) stored in database 44. Therefore, it is my opinion that Hsu discloses a “biometric card pointer system [e.g., access control unit 14].”

73. *Second*, in my opinion, Hsu also discloses “a method of enrolling” in its biometric card pointer system. Specifically, “FIG. 4 is a block diagram showing a fingerprint **enrollment process** as used in FIG[. 3.” Ex. 1003, ¶0014.

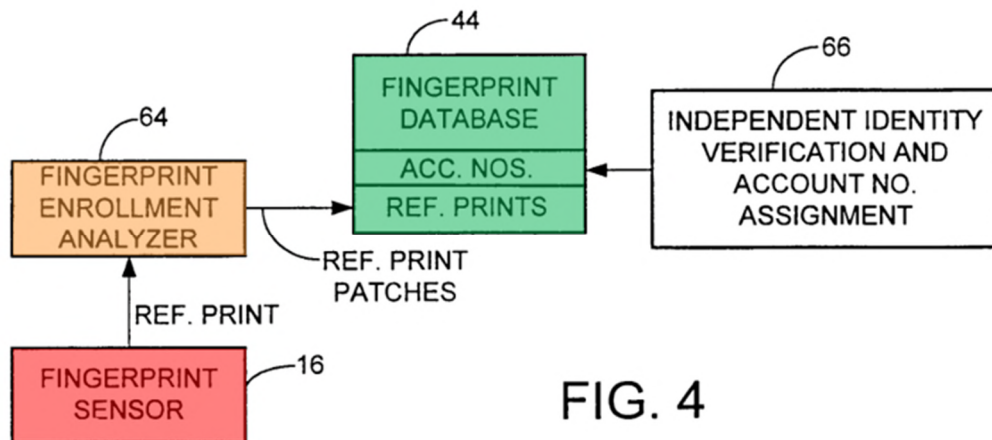


FIG. 4

Ex. 1003, Fig. 4. Hsu’s “enrollment procedure... requires that each user **enroll** by presenting a finger to the fingerprint sensor 16 [red], which generates a fingerprint image for a fingerprint **enrollment analyzer** 64 [orange].” *Id.*, ¶0026. “[T]he user also presents an account number, employee number or similar identity number.” *Id.* As shown, “[t]he account number is stored in the database 44 [green] in

association with the user's fingerprint image data.” *Id.* Once a user is enrolled, he or she may use his or her card to access his or her reference fingerprint for verification purposes, as mentioned above. *Id.*, ¶0024.

74. Therefore, in my opinion, Hsu discloses “**a method of enrolling** [*e.g.*, Hsu's method of enrollment] **in a biometric card pointer system** [*e.g.*, Hsu's access control unit 14].”

75. **Limitation 1[A]**. The claim requires “receiving card information,” which, in my opinion, is disclosed by Hsu in view of Sanford.

76. Hsu teaches two types of **cards**: 1) a card having a transponder, and 2) a “machine-readable card.” Ex. 1003, ¶0011. If a user wears a “badge [] that includes a transponder” and “approaches a door,” the badge “detects the polling signal [green] and **transmits a reply signal** [orange] **that includes the user's identification number or user number**,” as shown in Figure 2 below. *Id.*, Abstract, ¶0020.

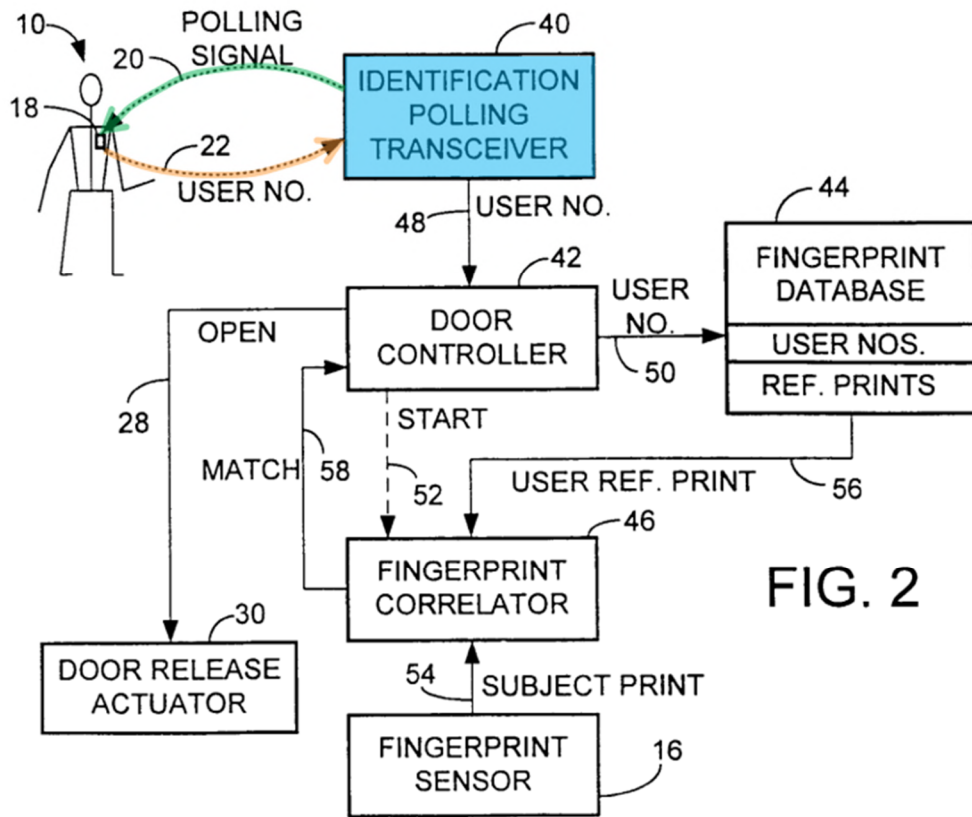


FIG. 2

Ex. 1003, Fig. 2. In other words, the “identification polling transceiver 40 [blue],” which is part of the “the access control unit,” receives the “user’s identification number or user number.” *Id.*, ¶0020, Fig. 1.

77. In my opinion, a POSITA would have understood that a badge is a card or equivalent to a card. In fact, the ’039 Patent discloses that its card can be a “wireless ‘key-fob’ which is a small radio transmitter that emits a radio frequency (RF) signal,” just like Hsu’s badge that uses well-known “[t]ransponder badge technology, sometimes known as RF-ID (radio-frequency identification).” Ex. 1001, 1:50-52; Ex. 1003, ¶0018. Because the “user’s identification number or user

number” is part of the signal (orange above) transmitted by the card (badge), a POSITA would have understood that Hsu’s received “**user’s identification number or user number**” is the claimed “**card information.**”

78. If a user uses a “machine-readable card,” then he or she needs to “place[] his or her card in the **reader 62** [blue], which **retrieves an account number or other type of identification** unique to the user, and **passes** [orange] this data to the access controller 42 [brown],” as shown in Figure 3 of Hsu. Ex. 1003, ¶0024.

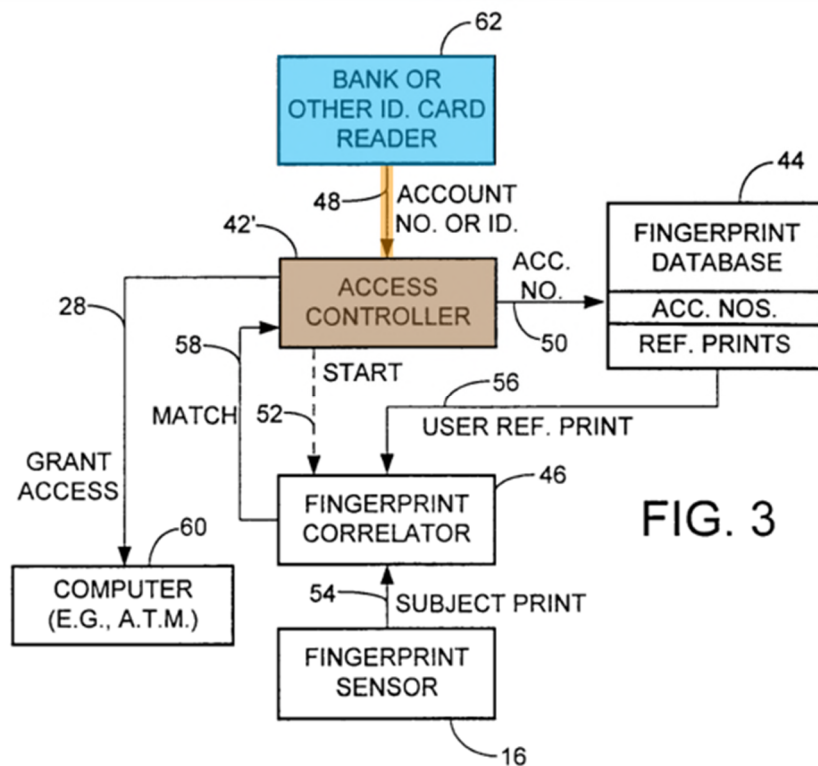


FIG. 3

Id., Fig. 3. A POSITA would have understood that Hsu’s received “**account number**” is the claimed “**card information.**”

79. Hsu's enrollment process also includes "receiving card information." Hsu includes various disclosures of "**reading data from a card reader**," which confirm that the card reader (or its equivalent, a polling transceiver) in the access controller is receiving card information. *See* Ex. 1003, ¶0009 ("reading an identification medium includes a bank **card reader** integral with the ATM"), ¶0011 ("the identification medium carried by each user includes a **machine-readable card**, and the step of **reading data** from an identification medium includes **reading data from a card reader** in which the machine-readable card is placed by the user"), ¶0007 ("machine **readable card**; and the means for **reading the identification medium includes a card reader** capable of **reading the machine readable card to extract preliminary identification data**").

80. Regarding the enrollment context, as I explained for Limitation 1[P], Hsu discloses that the "enrollment procedure requires that each user enroll by presenting a finger to the fingerprint sensor" and "**present[ing] an account number, employee number or similar identity number.**" Ex. 1003, ¶0026. Since Hsu's enrollment procedure in Figure 4 is applicable "for any of the configurations," in my opinion, a POSITA would have understood that regardless of the type of card used, Hsu's enrollment process includes receiving card information (*e.g.*, account number or employee number). *Id.* It should be noted that the claim does not require receiving the card information from the card.

81. Moreover, Sanford (a combination reference used in this Ground) also discloses receiving card information during enrollment. A POSITA would have understood there are at least two ways of presenting Hsu's "account number, employee number or similar identity number" (Ex. 1003, ¶0026)—entering the number, or presenting a card that includes the number. Sanford discloses both. For example, as shown in Figure 2, Sanford discloses a user "swip[ing a] card" or "enter[ing] in [the] card number" in step S200 (blue):

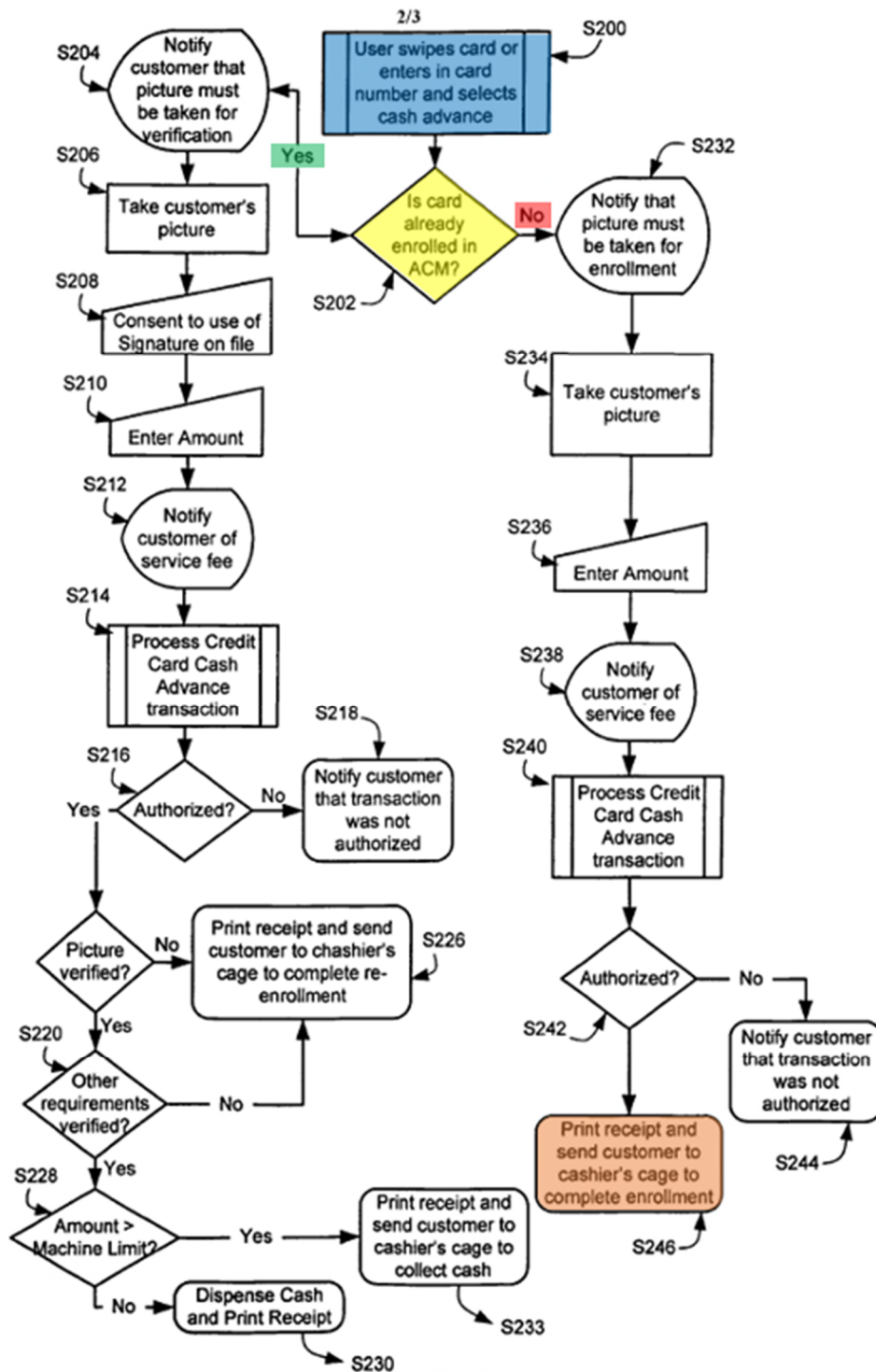


Fig. 2

Ex. 1003, Fig. 2; ¶0024. The card number is then used to determine if the card is enrolled in step S202 (yellow); if not, the user is directed to the enrollment process,

as indicated by step S246 (orange). In my opinion, a POSITA would have been motivated to receive Hsu's number by both methods, but especially by receiving the number from the card because the user would not need to remember her number. A POSITA would also have had a reasonable expectation of success combining Hsu with Sanford because presenting Hsu's "account number, employee number or similar identity number" (Ex. 1003, ¶0026) (as described in Sanford's step S200, *e.g.*, by presenting a card including the number to a card reader) was already contemplated by Hsu and would have resulted in a working system. Indeed, Hsu has numerous disclosures of receiving card information from the card reader. *See*, Ex. 1003 ¶0009, ¶0011, ¶0007. Thus, in my opinion, it would have been obvious for a POSITA to combine Hsu with Sanford. *See full motivation-to-combine at the end of claim 1.*

82. Therefore, in my opinion, Hsu in view of Sanford discloses "receiving card information [*e.g.*, Hsu's account number or employee number; or Sanford's credit card account number]."

83. **Limitation 1[B]**. The claim requires "receiving the [*sic*] biometric signature," which, in my opinion, this is disclosed by Hsu.

84. I note that this term lacks antecedent basis. For the purpose of my analysis, I treat this limitation as reciting "receiving [a] biometric signature."

85. As shown below, the access control unit includes a “fingerprint sensor 16” (red) for “scan[ing] the user’s fingerprint.” Ex. 1003, ¶¶0020-21, ¶¶0024.

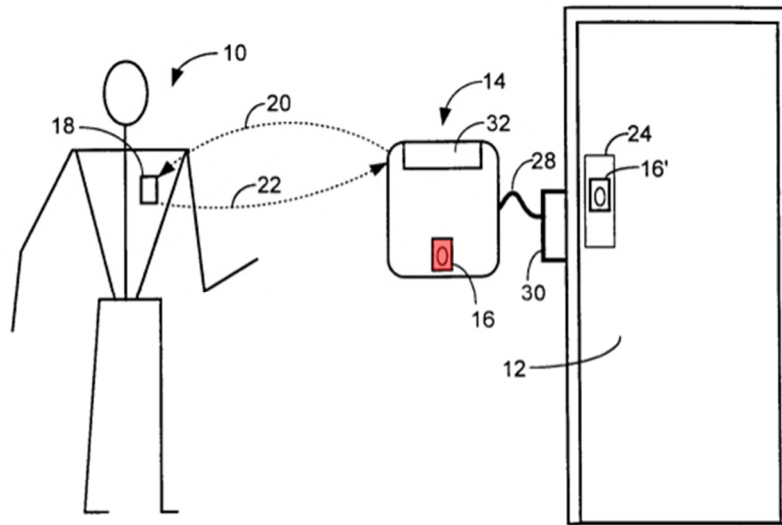


FIG. 1

Ex. 1003, Fig. 1.

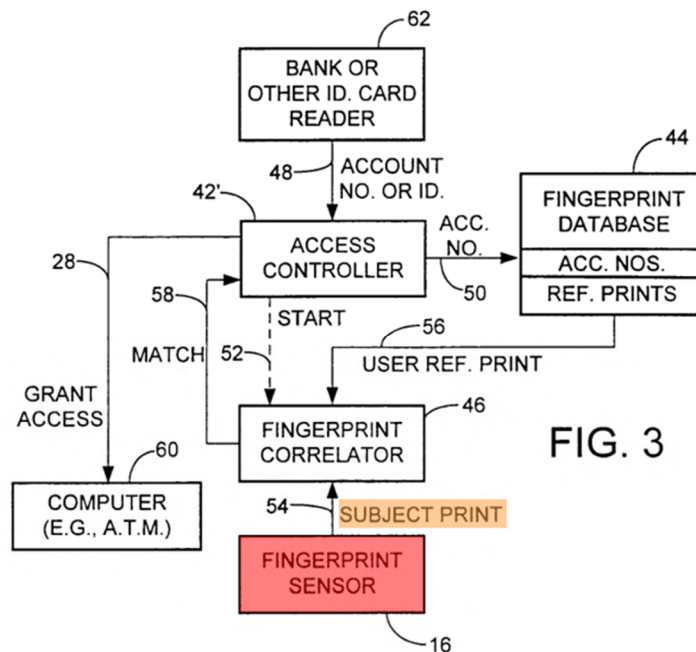


FIG. 3

Ex. 1003, Fig. 3; *see also* Fig. 2. The '039 Patent confirms that a fingerprint is a type of biometric signature. Ex. 1001, 7:45-47 (“input a biometric signature, such as fingerprint”); VI.D.2. Therefore, the “fingerprint sensor 16 [red],” which is part of the “the access control unit” in Hsu, receives the user’s biometric signature (*i.e.*, “subject fingerprint,” orange). Ex. 1003, ¶0020, Figs. 2, 3.

86. It is my opinion that Hsu’s enrollment process also includes “receiving [a] biometric signature” because Hsu’s “enrollment procedure requires that each user enroll by **presenting a finger to the fingerprint sensor,**” as discussed for limitation 1[P]. Ex. 1003, ¶0026.

87. Therefore, in my opinion, Hsu discloses “**receiving the** [*sic*] **biometric signature** [*e.g.*, receiving a fingerprint].”

88. **Limitation 1[C]**. The claim requires “**defining**, dependent upon the received card information, **a memory location in a local memory external to the card,**” which, in my opinion, is disclosed by Hsu.

89. *First*, Hsu discloses “a local memory external to the card.” As shown in Figure 1, the “access control unit 14” (yellow) is external to the “identification badge 18 [card]” (pink):

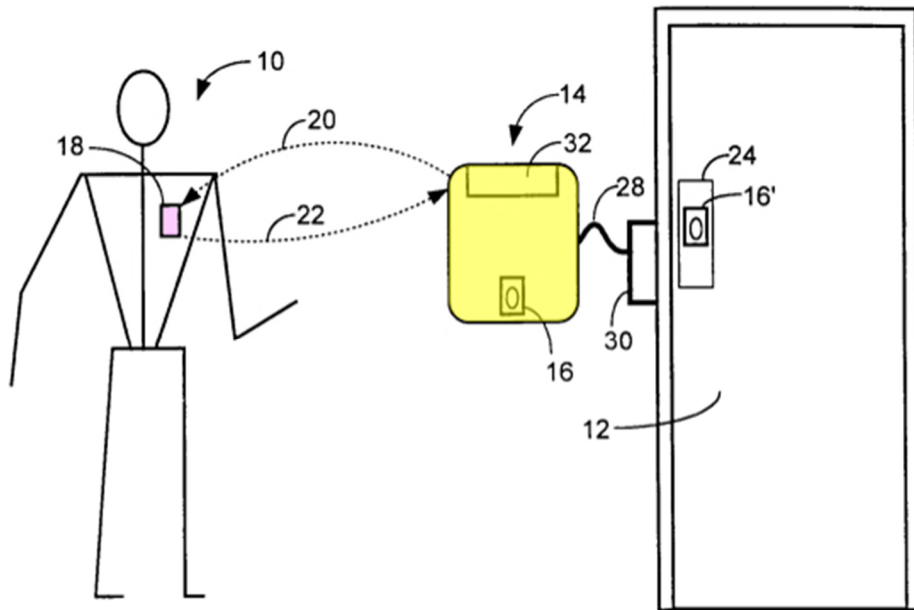


FIG. 1

Ex. 1003, Fig. 1. Since the “fingerprint **database (44)**” (green, Fig. 2 below) is one of “the principal components of the access control unit 14 [yellow, Fig. 1 above],” the “fingerprint database (44)” is therefore **local** to the “access control unit 14” and **external** to the “identification badge 18.” *Id.*, ¶0020.

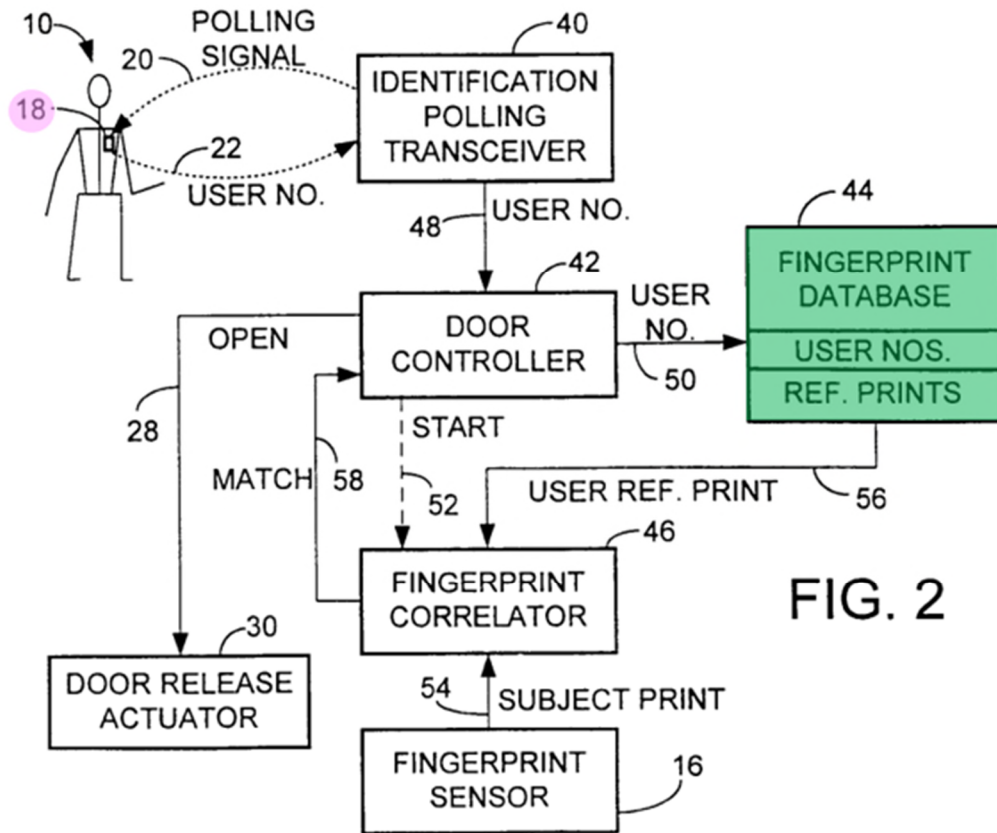
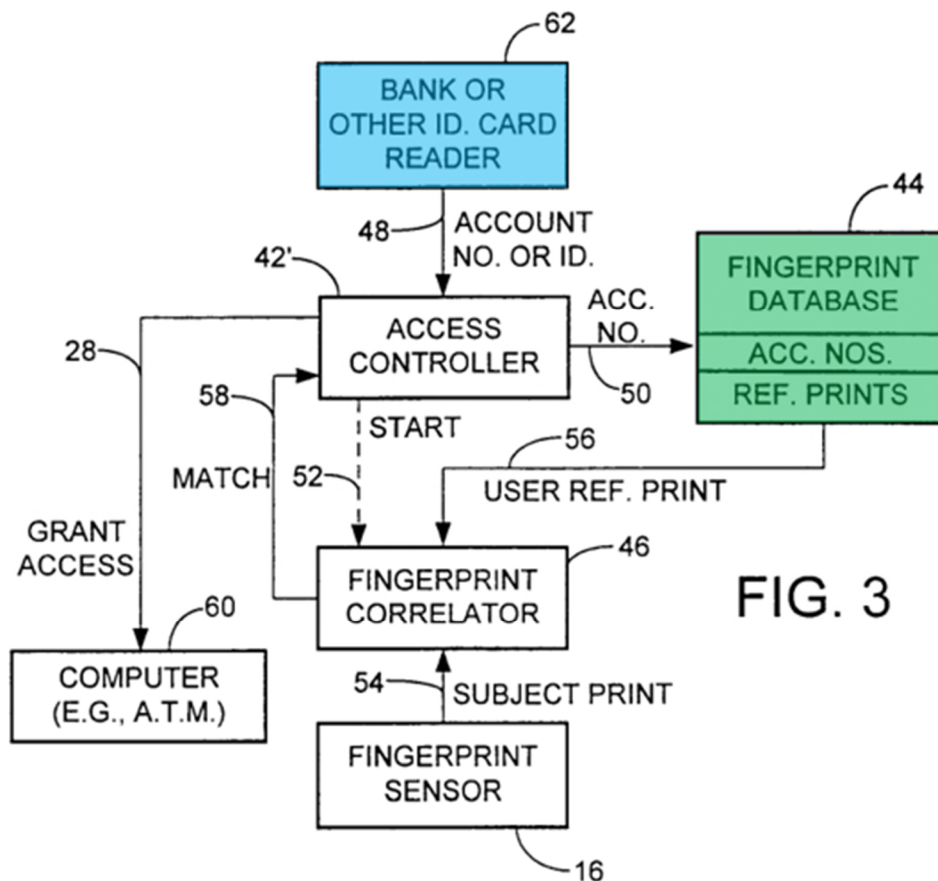


FIG. 2

Ex. 1003, Fig. 2 (“show[ing] the principal components of the access control unit 14”, ¶0020). In other words, the “fingerprint database (44)” is stored in a **local memory external to identification badge 18**.

90. As I discussed for limitation 1[B] and indicated by the '039 Patent, a POSITA would have known that a badge is type of card. A POSITA would also have understood that a database is stored in a memory. Thus, in my opinion, the “fingerprint database (44)” in Figure 2 of Hsu discloses “a local memory external to the card.”

91. Hsu's Fig. 3 is "similar to FIG. 2"—but instead of being used to access a "door release actuator 30," the embodiment illustrated in Figure 3 can be "used to access a computer 60, such as a bank automatic teller machine (ATM)." Ex. 1003, ¶0024. Here, the "access control unit 14" includes a "bank card reader 62 [blue]...for reading some type of identification card." *Id.*



Therefore, similar to Figure 2, since the "fingerprint database (44)" (green) in Figure 3 is local to the "access control unit 14" and external to the "identification card," it discloses "a local memory external to the card."

92. *Second*, in my opinion, Hsu discloses a “memory location” (in its local memory) “defin[ed], dependent upon the received card information,” *i.e.*, the memory location is somehow determined from (or is dependent on) the received card information, under the First Construction discussed in Section VI.A.1.

93. Hsu discloses storing a reference fingerprint to, and retrieving from, the “fingerprint database (44).” Ex. 1003, ¶¶0010, ¶¶0026. Specifically, “[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. As shown in Figure 4 below, “the fingerprint database 44 [green] contains **reference fingerprint image data** for each user, employee, or customer using the system, and that the reference fingerprint data are associated with corresponding **user numbers, or employee or customer account numbers.**” Ex. 1003, ¶¶0026.

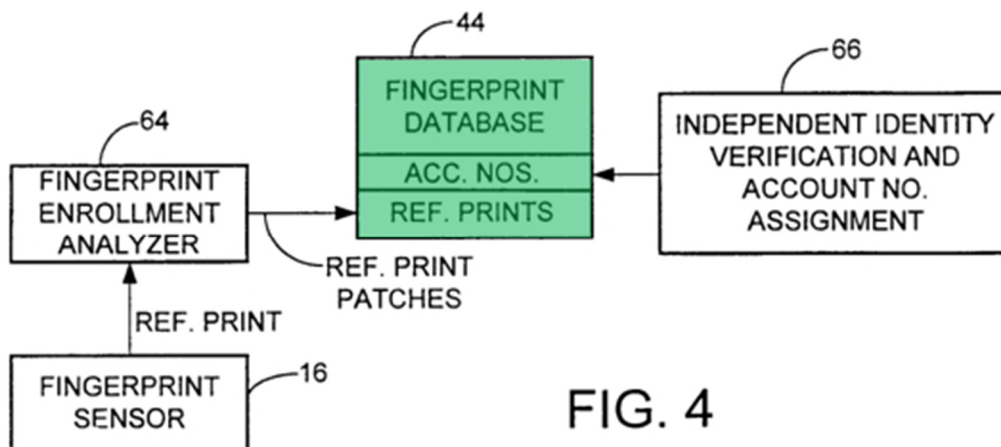


FIG. 4

Id., Fig. 4. The “fingerprint image, or [] selected distinctive attributes or features of the user’s fingerprint image” are not stored at *any* memory location in the database—rather, it is stored at a memory location associated with the specific user/employee number received from a card. *Id.*, ¶0026. In my opinion, a POSITA would have understood that, given a user number, Hsu’s system easily determines from fingerprint database 44 the specific memory location for storing the associated fingerprint.

94. Therefore, in my opinion, Hsu discloses “**defining, dependent upon the received card information** [*e.g.*, Hsu user/account/employee number from card], **a memory location** [*e.g.*, memory location in Hsu’s database] **in a local memory** [*e.g.*, Hsu’s local memory] **external to the card** [*e.g.*, external to Hsu’s card/badge].”

95. **Limitation 1[D]**. The claim requires “**determining if the defined memory location is unoccupied,**” which, in my opinion, is rendered obvious by Hsu and Sanford.

96. As I explained for Limitation 1[C], Hsu discloses the “defined memory location.”

97. Moreover, it is my opinion that Sanford discloses “determining if...[a] memory location is occupied.”

98. According to the construction for “unoccupied” in Section VI.A.2, the ’039 Patent discloses that “determining if...[a] memory location is unoccupied” is determining if the memory location has not been used in an enrollment process for the user. Although this would be obvious to a POSITA, Hsu does not explicitly disclose checking whether a memory location is unoccupied. However, Sanford explicitly checks if a user is enrolled before trying to enroll the user, and for the reasons presented later (*see* full motivation to combine section, *infra*), it is my opinion that it would have been obvious to modify Hsu based on Sanford.

99. As shown in Figure 2 below, Sanford discloses in step S202 (yellow) “determin[ing] if the credit card account number of the user is enrolled to use the PIN-less credit card system.” Ex. 1004, ¶0025.

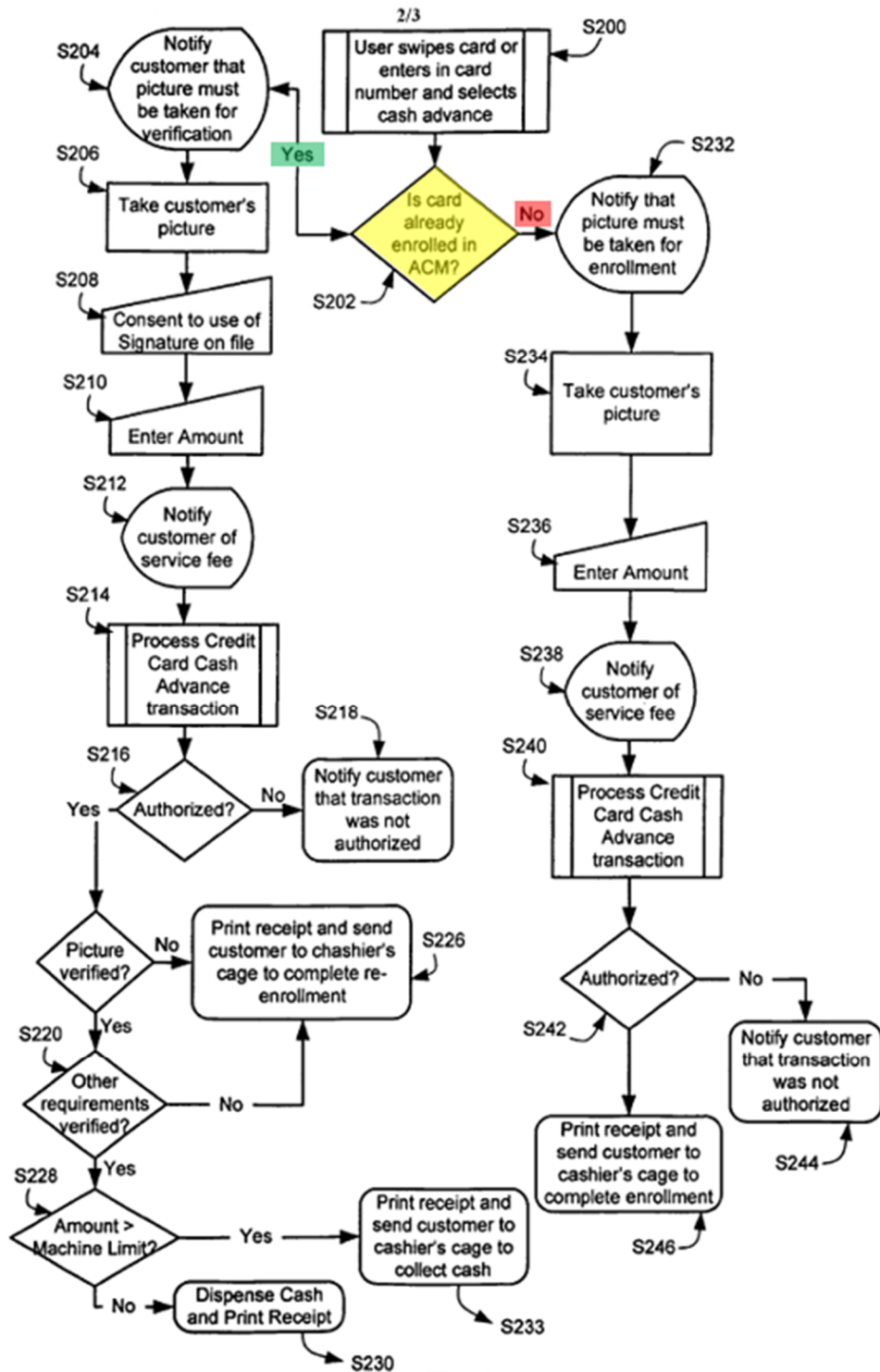


Fig. 2

Ex. 1004, Fig. 2. Such determination involves checking a database. *Id.*, ¶0025

(“ACM 12 may include a database that may be used to determine if the user is

enrolled.”). If the card is already enrolled (“yes,” green), the process proceeds to verification. *Id.*, ¶0026. If the card is not enrolled (“no,” red), the process proceeds to enrollment. *Id.*, ¶0025. Thus, Sanford discloses determining if a user is already enrolled by checking a database. *Id.*

100. I note that a POSITA would have understood that checking whether a card is enrolled is the same as checking whether a user is enrolled (*e.g.*, as each user has a unique card number). Indeed, Sanford uses these two concepts interchangeably. Ex. 1004, ¶0025 (“determines if the **credit card account number** of the user is enrolled”); *cf. id.* (“determining if the **user** is enrolled”).

101. As discussed in more detail below, it would have been obvious to a POSITA to implement Sanford’s determination of whether a user is enrolled in Hsu’s system. In my opinion, since Sanford’s determination involves checking its database, a POSITA would have found it obvious to check Hsu’s database when implementing Sanford’s determination. As discussed above, Hsu describes only a single place where it can be determined if a user is enrolled—its database that includes for each user/employee number, an associated fingerprint. Therefore, for a user whose account or user number already exists in Hsu’s database (*e.g.*, the user’s employer assigned a user number and added the number to the database), the only way to check whether the user has been enrolled is to use his/her account or user number to access the memory location for storing (or reserved for storing) the

associated fingerprint and determine if any fingerprint exists at that memory location (*i.e.*, if the memory location is unoccupied). *See* full motivation-to-combine at the end of claim 1.

102. Therefore, in my opinion, Hsu in view Sanford discloses “**determining if the defined memory location** [*e.g.*, memory location in Hsu’s database] **is unoccupied** [*e.g.*, Sanford’s teaching to check if a user is enrolled requires checking Hsu’s memory location for that user].”

103. **Limitation 1[E]**. The claim requires “storing, if the memory location is unoccupied, the biometric signature at the defined memory location,” which, in my opinion, is disclosed by Hsu and Sanford.

104. As I explained for Limitation 1[D], Hsu in view of Sanford discloses “determining if the defined memory location is unoccupied.”

105. Sanford discloses that if a user is not enrolled (*i.e.*, if Hsu’s memory location is unoccupied), the user is directed to complete enrollment, which involves storing the user’s biometric information (*e.g.*, picture or fingerprint) in the database. Ex. 1004, ¶0037 (“a receipt is printed and the customer is given instructions to proceed to cashier system 14 to complete **enrollment**”); ¶0038 (“an **enrollment** process for **creating a profile in database 24**”); Cls. 33, 34.

Likewise, Hsu also discloses an enrollment process involving storing fingerprints.

Ex. 1003, Fig. 4, ¶0026 (“The account number is **stored in the database** 44 in association with the **user’s fingerprint image data.**”).

106. I note that a POSITA would have understood that storing/comparing fingerprints can use fingerprint images and/or features extracted from the images. Ex. 1003, ¶0026. For the purposes of my opinions regarding the ’039 Patent and the prior art herein, these two concepts are interchangeable.

107. Therefore, in my opinion, Hsu in view of Sanford discloses “**storing, if the memory location is unoccupied** [*e.g.*, checking Hsu’s database to see if a user is not yet enrolled per Sanford, and if so, storing], **the biometric signature** [*e.g.*, user’s fingerprint] **at the defined memory location** [*e.g.*, at the memory address in Hsu’s database assigned to the user].”

108. **Motivation to Combine Hsu and Sanford**. As I explained above, Hsu discloses all limitations of claim 1 except for an explicit disclosure of first checking if the memory location in Hsu’s database assigned to the user is unoccupied (*i.e.*, the user is not yet enrolled), which is disclosed by Hsu in view of Sanford. In my opinion, it would have been obvious to apply Sanford’s check of whether a user is enrolled into Hsu’s system.

109. The ’039 Patent, Hsu, and Sanford 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. Hsu discloses the stored fingerprint data being associated with a user/account number provided by a user's card. Ex. 1003, ¶0026. Sanford discloses a user's picture (or fingerprint) associated with a user's credit card number provided by a user. Ex. 1003, ¶¶0018-21. *I.e.*, 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 a captured fingerprint against multiple stored fingerprints in a one-to-many manner. This concept and the implementation of it were very well-known before the '039 Patent, as I explain below regarding the motivation to combine Sanford-Hsu with Tsukamura.

110. I note that, while Hsu discloses assigning a number to a user as part of an enrollment process, it is merely one of the embodiments described. Ex. 1003, ¶0026 (“**If** the user does not have such a number, one is assigned at this stage.”). In an embodiment where the user already has an account/user/employee number

but has not yet enrolled their fingerprint, Hsu's database includes a memory location used to store the user's fingerprint. *Id.*

111. In this context, it is my opinion that a POSITA would have been **motivated** to implement Sanford's check to determine whether a user (*e.g.*, with a user/account number) is enrolled in Hsu's system.

112. *First*, it is my opinion that, in most instances, a POSITA would not want to enroll a user who already enrolled. This is recognized by Sanford:

“The enrollment process is preferably only done once.

However, exceptions, such as when an ID or credit card has expired, when the identity of the cardholder does not match the card, or when a proper digitized signature was not obtained may require the enrollment process to be repeated.”

Ex. 1004, ¶0038. Re-enrollment is usually unnecessary because fingerprints do not change. Re-enrollment also consumes unnecessary system resources, takes time, and is generally undesirable. Therefore, before enrolling a user, it is my opinion that a POSITA would have been motivated to first check whether the user is already enrolled, as disclosed by Sanford.

113. *Second*, it is my opinion that a POSITA would also have been motivated to check whether a user is enrolled to avoid unintentionally overwriting

existing fingerprints. For example, consistent with the common goal of all biometric authentication systems, checking whether a user is enrolled helps prevent fraud whereby an unauthorized user is able to overwrite the fingerprint of an authorized user by using the authorized user's user number or account number. If it is determined that a user (per their user's account/user number) is already enrolled/authorized, re-enrollment generally will not be allowed.

114. *Third*, it is also my opinion that checking whether a user is enrolled also makes the system more user-friendly. If the user is enrolled, the user can seamlessly proceed with biometric verification.

115. Finally, it is my opinion that a POSITA would also have had a **reasonable expectation of success** in applying Sanford's enrollment check in Hsu's system. In my opinion, a POSITA would have found it obvious to check Hsu's database when implementing Sanford's database/enrollment checking. A POSITA would have understood that the simple and straightforward way to determine whether such user has been enrolled is to check if the user's data is already stored in Hsu's database. A POSITA would have understood that implementing Sanford's checking of whether a user is enrolled in Hsu's system would clearly result in a working system. *Id.*

2. Claim 2 is rendered obvious by Hsu and Sanford

116. In my opinion, claim 2 is unpatentable because it is rendered obvious by Hsu and Sanford. Claim 2 of the '039 Patent recites the following. I address each of these in my analysis below.

[P] A method of obtaining verified access to a process, the method comprising the steps of:
[A] storing a biometric signature according to the enrolment method of claim 1;
[B] subsequently presenting card information and a biometric signature; and
[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.

117. **Preamble 2[P]**. It is my opinion that Hsu (or Hsu in view of Sanford) discloses “a **method of obtaining verified access to a process.**”

118. In the '039 Patent, a user needs to be verified to access a process, *e.g.*, cash withdrawal at an ATM. Ex. 1001, 9:50-59 (“performs **the transaction process** (which may be viewed as a **process of obtaining verified access to a protected resource**) ... may be... **withdrawal of cash from an Automatic Teller Machine (ATM)**”); 3:17-24.

119. Hsu discloses that “[i]n the case of an ATM machine,” a user “may then conduct banking transactions, such as cash withdrawal or deposit

transactions.” *Id.*, ¶0024; Fig. 3. Because a user of Hsu’s system may conduct banking transactions only after her fingerprint is verified, **access to the banking transaction process is a verified access**. This is the same as the example in the ’039 Patent, where a “transaction process” (*e.g.*, “withdrawal of cash from an Automatic Teller Machine (ATM)”) is performed after an “authorisation [*sic*] step [] indicates that the biometric signal received by the biometric reader [] matches the biometric signature previously stored in the local database [] by a previous enrolment [*sic*] process.” Ex. 1001, 9:50-59; 10:3-5; 11:38-43; Figs. 5-6.

120. Sanford similarly 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.*

121. Therefore, in my opinion, Hsu (or Hsu in view of Sanford) discloses “**a method of obtaining verified access to a process** [*e.g.*, Hsu’s banking transaction process].”

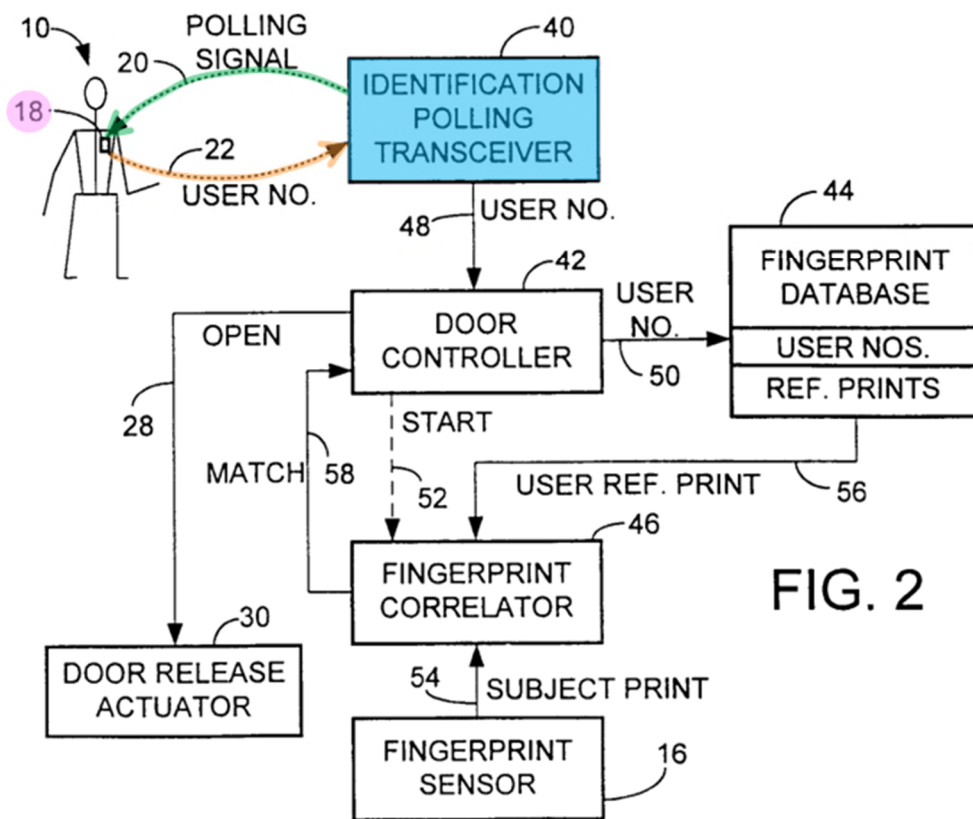
122. **Limitation 2[A]**. The claim requires “**storing a biometric signature according to the enrolment method of claim 1**,” which, in my opinion, is disclosed by Hsu and Sanford, as I explained for Limitation 1[E] above, incorporated here.

123. **Limitation 2[B]**. The claim requires “**subsequently presenting card information and a biometric signature,**” which, in my opinion, is disclosed by Hsu.

124. Hsu discloses both an enrollment process and a verification process. Ex. 1003, ¶0020, ¶0024, ¶0026, Figs. 2-4. For a secure biometric authentication system to work (*e.g.*, be able to grant access to an enrolled user), it is my opinion that enrollment necessarily happens before verification. This is recognized by the ’039 Patent. Ex. 1001, Abstract (“The disclosed Biometric Card Pointer arrangements **store** (207) a card user’s biometric signature in a local memory (124) in a verification station (127) **the first time the card user uses** the verification station (127) in question.”). Hsu discloses the same. Hsu acknowledges that the verification process “assumed... that the fingerprint database 44 contains reference fingerprint image data for each user, employee, or customer using the system.” Ex. 1003, ¶0026. Moreover, “an enrollment procedure [] is required for any of the [verification] configurations described above.” *Id.* Thus, it is my opinion that Hsu discloses performing an enrollment process and “**subsequently**” performing a verification process.

125. Further, it is my opinion that Hsu’s verification process includes “presenting card information and a biometric signature” required by this limitation.

126. First, Hsu’s verification process includes “presenting card information.” See discussion for Limitation 1[A]; Ex. 1003, ¶0011. As shown in Figure 2, if a user “wear[s] an identification badge 18,” “badge 18 [pink] detects the polling signal [green] and transmits a reply signal [orange] that includes the user’s identification number or user number.” *Id.*, ¶0020.



Ex. 1003, Fig. 2. In this way, the card information (the user’s identification number or user number) is presented. If a user uses a “machine-readable card” (e.g., a bank card), as shown in Figure 3 below, Hsu discloses a “a bank card

reader 62 [blue] or a similar device for reading some type of identification card.”

Ex. 1003, ¶0024.

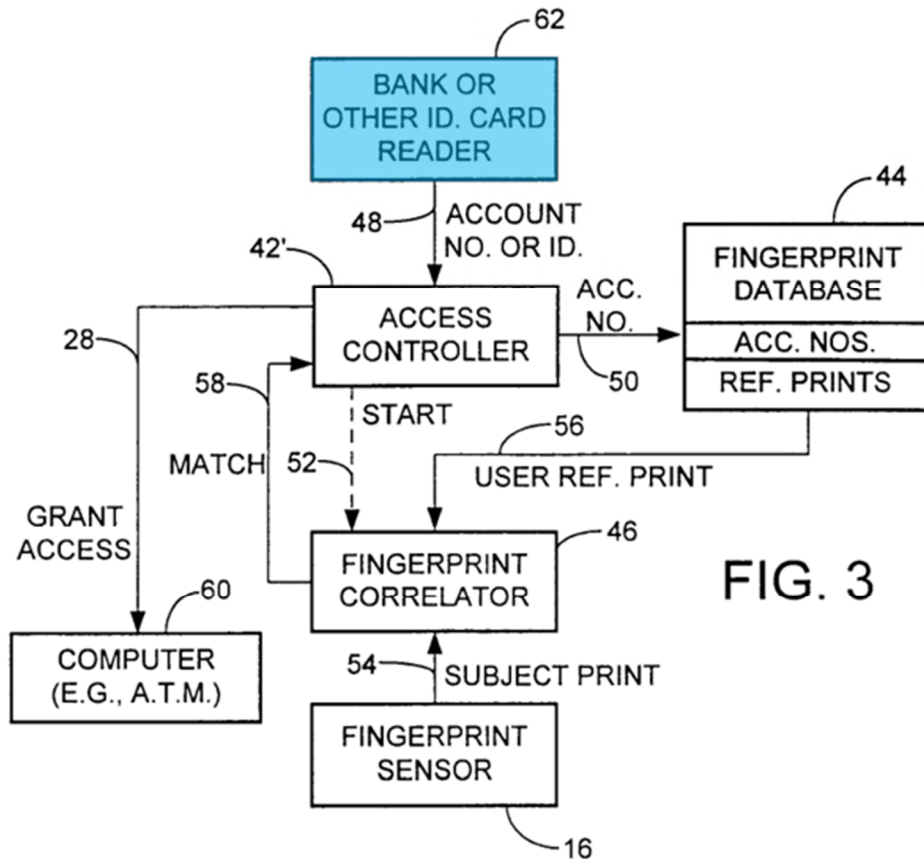


FIG. 3

Ex. 1003, Fig. 3. “The user places his or her card in the reader 62 [blue], which retrieves an account number or other type of identification unique to the user.” *Id.*, ¶0024. Thus, the card information (*i.e.*, the user’s account number or other type of identification unique to the user) is presented. Regardless of the type of card being used, the retrieved card information is passed to a controller (*i.e.*, “door controller 42” in Figure 2, or the “corresponding component” “access controller 42” in Figure

3) to “retrieve[] a reference fingerprint from the database 44” for later comparison.
Id., ¶¶0021, ¶¶0024.

127. *Second*, Hsu’s verification process includes “presenting a biometric signature.” In both Figs. 2 and 3 below, Hsu discloses a “fingerprint sensor 16” (red) for “scan[ing] the user’s fingerprint.” Ex. 1003, ¶¶0021.

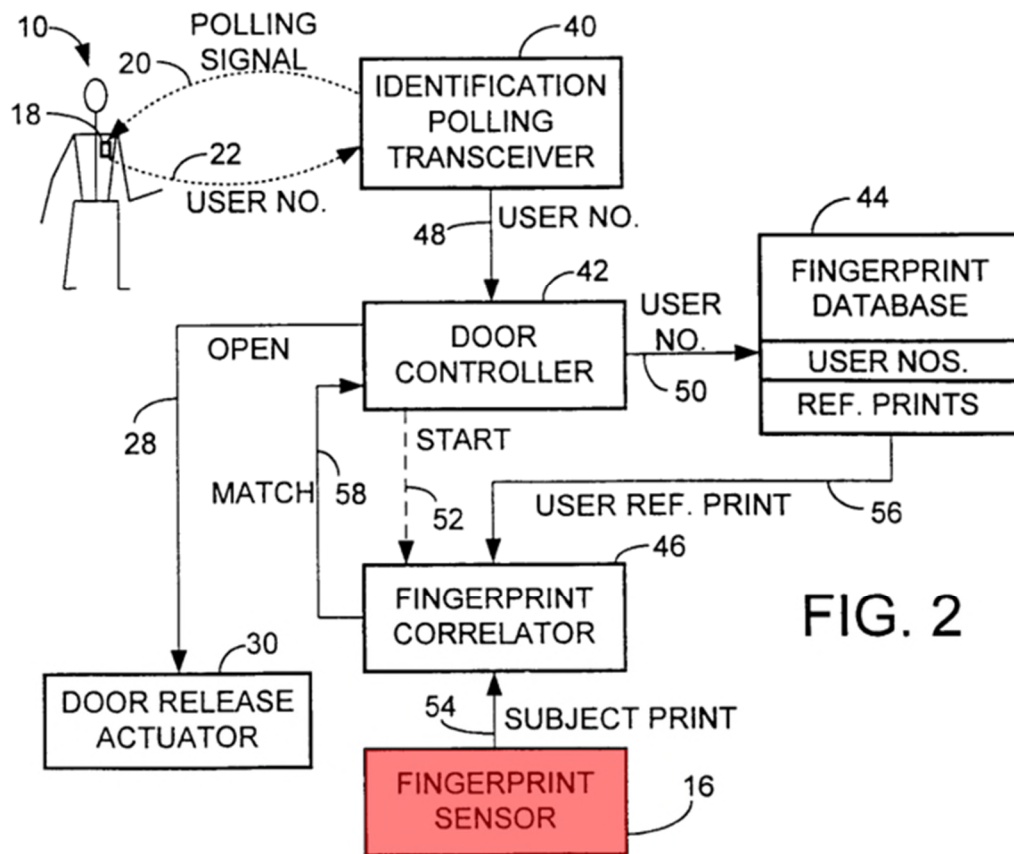


FIG. 2

Ex. 1003, Fig. 2.

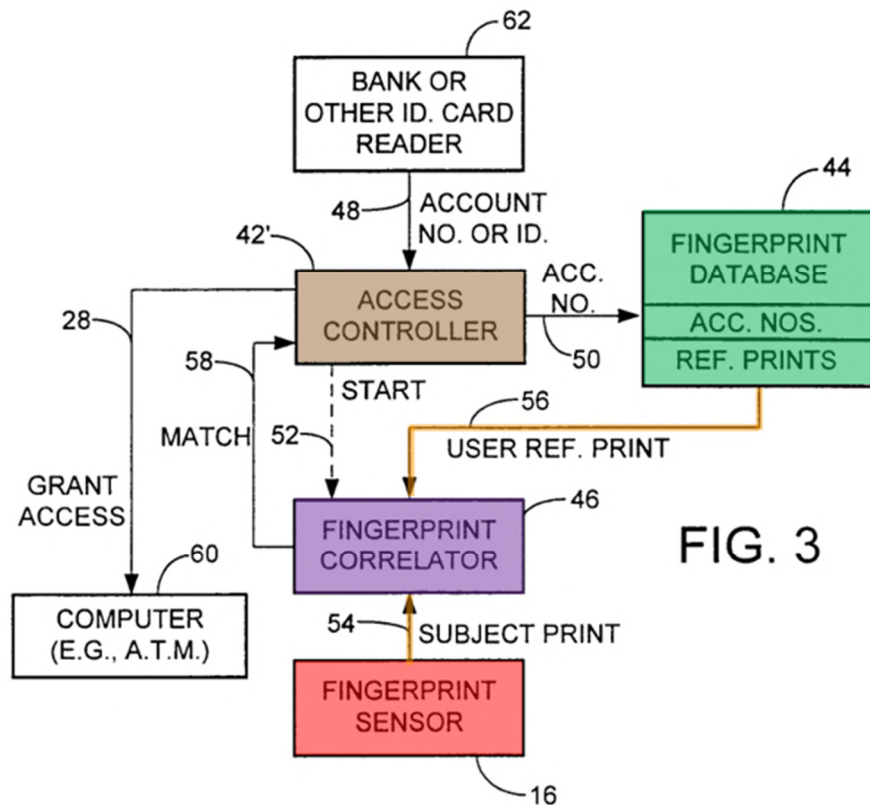


FIG. 3

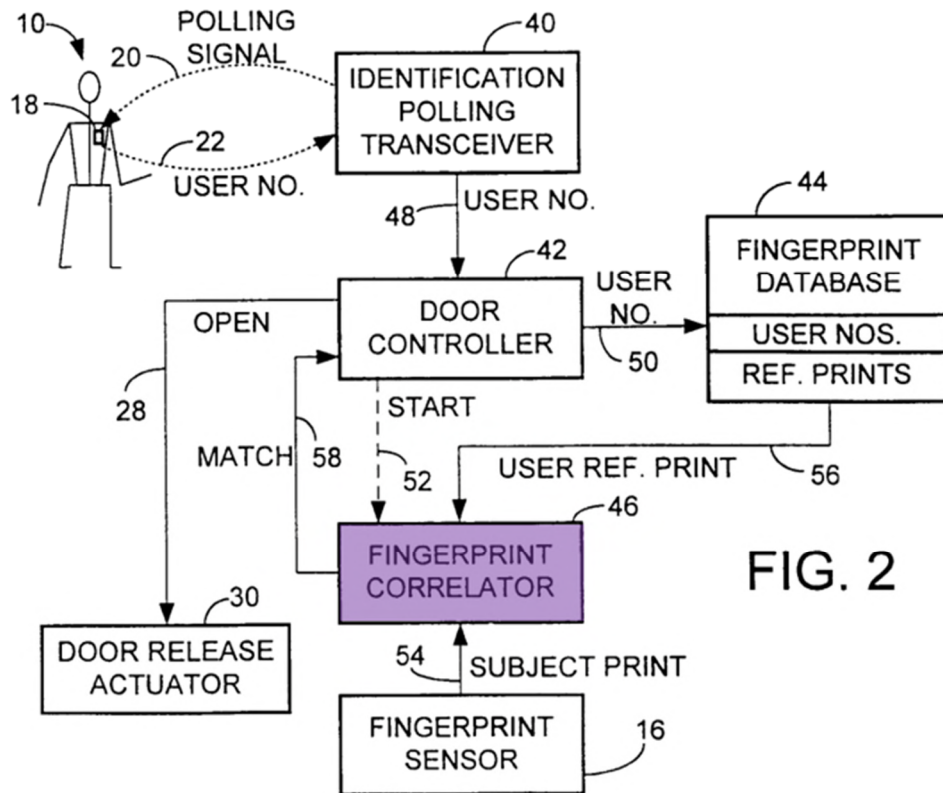
Ex. 1003, Fig. 3. The “fingerprint sensor 16 [red] is activated” by “the controller [brown]... issu[ing] a ‘start’ command to the fingerprint correlator 46 [purple].” *Id.*, ¶0021, ¶0024. “The correlator 46 [purple] then rapidly compares the subject fingerprint from the sensor 16 [red], received over line 54, with the reference fingerprint features received from the database 44 [green] over line 56.” *Id.* The ’039 Patent confirms that a fingerprint is a type of biometric signature. Ex. 1001, 7:45-47. Thus, Hsu discloses presenting a biometric signature (*e.g.*, fingerprint).

128. Therefore, it is my opinion that Hsu discloses “**subsequently** [*e.g.*, any time after Hsu’s enrollment] **presenting card information** [*e.g.*, presenting

Hsu's user/ account/employee number stored on the card/badge] **and a biometric signature** [e.g., Hsu's fingerprint].”

129. **Limitation 2[C]**. The claim requires “**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,” which, in my opinion, is disclosed by Hsu.

130. *First*, regardless which type of card is being used, **Hsu discloses a “fingerprint correlator 46”** (purple) as shown in Figs. 2 and 3 below.



Ex. 1003, Fig. 2.

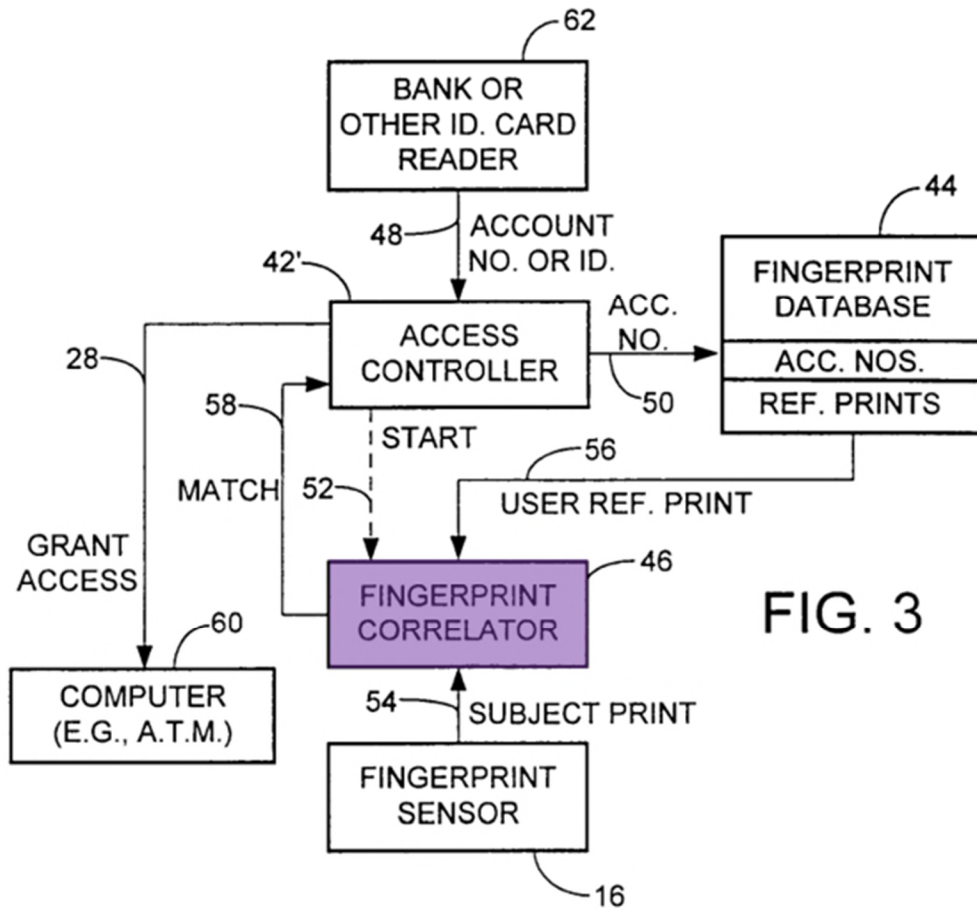


FIG. 3

Ex. 1003, Fig. 3. In both embodiments, the fingerprint correlator 46 (purple) “compares the subject fingerprint from the sensor 16, received over line 54, with the reference fingerprint features received from the database 44 over line 56” to “determine[]... [if] there is a **match**.” *Id.*, ¶0021, ¶0024. Hsu further discloses that “[t]he fingerprint correlator 46 performs the **matching function** very rapidly by using special-purpose hardware in the form of an application-specific integrated circuit (ASIC).” *Id.*, ¶0023. Therefore, Hsu discloses “verifying... if the

subsequently presented biometric signature matches the [stored] biometric signature.”

131. In addition, Hsu’s card information (*e.g.*, user number or account number) is used to retrieve the stored biometric signature (*e.g.*, fingerprint). Ex. 1003, ¶¶0020, ¶¶0024. Therefore, it is my opinion that Hsu discloses “**verifying the subsequently presented presentation of the card information and the biometric signature** if the subsequently presented biometric signature matches the [stored] biometric signature.”

132. *Second*, as I explained for Limitation 1[E], the fingerprint in Hsu’s system is stored “at the memory location defined by the subsequently presented card information.”

133. Therefore, it is my opinion that Hsu discloses “**verifying the subsequently presented presentation of the card information** [*e.g.*, Hsu’s account or user number] **and the biometric signature** [*e.g.*, Hsu’s fingerprint] **if the subsequently presented biometric signature** [*e.g.*, Hsu’s fingerprint] **matches the biometric signature at the memory location** [*e.g.*, a user’s fingerprint stored at Hsu’s memory location associated with the user’s account/user/employee number], **in said local memory** [*e.g.*, Hsu’s local memory], **defined by the subsequently presented card information** [*e.g.*, account/ user/employee number].”

3. Claim 13 is rendered obvious by Hsu and Sanford

134. In my opinion, claim 13 is unpatentable because it is rendered obvious by Hsu and Sanford. Claim 13 of the '039 Patent recites the following. I address each of these in my analysis below.

[P] A biometric card pointer enrolment system comprising:

[A] a card device reader for receiving card information;

[B] a biometric reader for receiving the biometric signature;

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

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

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

135. **Preamble 13[P]**. It is my opinion that Hsu discloses “**a biometric card pointer enrolment [sic] system.**”

136. As I explained for Limitation 1[P], Hsu discloses a “biometric card pointer system [e.g., access control unit 14].” As I also explained for Limitation 1[P], Hsu discloses a method of enrolling in its biometric card pointer system. Thus, Hsu’s biometric card pointer system is also an enrollment system that allows users to be enrolled.

137. **Limitation 13[A]**. The claim requires “**a card device reader for receiving card information,**” which, in my opinion, is disclosed by Hsu in view of Sanford.

138. I noted that according to the '039 Patent, “card device” is synonymous with “card” and “reader device” is synonymous with “reader.” Ex. 1001, 1:21-23.

139. As explained for Limitation 1[A], Hsu teaches two types of cards: 1) a card having a transponder (*e.g.*, a badge), and 2) a “machine-readable card” (*e.g.*, a bank card). Ex. 1003, ¶0011. In situations where a user wears a badge, the access control unit 14 includes an identification polling transceiver 40 (card reader) for sending polling signals to, and receiving card information (*e.g.*, user number) from, the badge. *Id.*, ¶0020, Fig. 2. In situations where a user uses a bank card, the access control unit 14 includes a bank card reader 62 for retrieving card information (*e.g.*, account number). *Id.*, ¶0024, Fig. 3. As also explained for Limitation 1[A], Sanford discloses that the card information can be received from the card during enrollment.

140. Therefore, it is my opinion that Hsu in view of Sanford discloses “**a card device reader** [*e.g.*, identification polling transceiver 40 or bank card reader 62] **for receiving card information** [*e.g.*, user or account number].”

141. **Limitation 13[B]**. The claim requires “a biometric reader for receiving the [*sic*] biometric signature,” which, in my opinion, this is disclosed by Hsu.

142. As I explained for Limitation 1[B], Hsu discloses the access control unit 14 having a fingerprint sensor 16 for receiving a user’s fingerprint. Ex. 1003, ¶¶0020-21, ¶0024, Figs. 2, 3.

143. Therefore, in my opinion, Hsu discloses “**a biometric reader** [*e.g.*, fingerprint sensor 16] **for receiving the** [*sic*] **biometric signature** [*e.g.*, fingerprint].”

144. **Limitation 13[C]**. The claim requires “*means for defining, dependent upon the received card information, a memory location in a local memory external to the card,*” which, in my opinion, is disclosed by Hsu in view of Sanford.

145. I understand that Judge Albright construed this term in district court proceedings as follows:

The **function** of this limitation is “**defining, dependent upon the received card information, a memory location in a local memory external to the card.**”

Structure corresponding to the claimed means is a **computer system** with a **processor** executing an **application that uses any segment of card information**

605 from a card 601 (1) as a memory reference as shown in Fig. 4 or (2) to determine a group of associated memory references or 3) all equivalents of (1) and (2). Structure is found in '039 Patent, col. 6, line 66 – col. 7, line 23; col. 7, lines 31-35, 39-42, 47-48; col. 8, lines 44-46; col. 11, lines 29-37; col. 12, lines 1-9; Fig. 4.

Ex. 1012, pp. 1-2.

146. In my opinion, Hsu in view of Sanford discloses this construed limitation.

147. *First*, as I explained for Limitation 1[C], Hsu discloses the recited **function**.

148. *Second*, Hsu in view of Sanford discloses the same or equivalent **structure**. For example, Hsu discloses that its user/account/employee number (card information) is used as a memory reference and/or to determine a group of associated memory references (under the First Construction). As explained above, Hsu's user or account number is used as a reference to access the memory location that stores the user's fingerprint. Hsu discloses a "door controller 42" (in Figure 2) and a "access controller 42" (in Figure 3), both of which "**use[] the account number [or user number]... to access the fingerprint database 44 and obtain a user reference fingerprint [] from the database.**" Ex. 1003, ¶0024. Therefore,

Hsu's "door controller 42" and "access controller 42" use card information (e.g., user or account number) as a memory reference (e.g., memory location in Hsu's database).

149. In addition, it is my opinion that because Hsu discloses the card information can be used to determine both the fingerprint's memory reference and "other information about the user, such as a history of access to the door" (Ex. 1003, ¶0020), Hsu discloses using card information to determine a group of memory references, which are associated because they correspond to the same user.

150. Moreover, Hsu discloses or renders obvious that fingerprint matching is performed by computer processors executing software/application. Ex. 1003, ¶0004. For example, Hsu discloses using ASIC capable of "parallel processing" for fingerprint verification. *Id.*, ¶0023. A POSITA would have understood that a similar ASIC or process could be used for storing fingerprints (including determining where to store).

151. Sanford also provides such details for a system (like Hsu), including that it "includes a **processor**. The processor may be, for example, a computer, workstation, mainframe, pocket PC, personal digital assistant, etc. The processor also preferably includes or is in communication with a verification process 22 and

database 24. Verification process 22 may be a **software- implemented** process that communicates with database 24.” Ex. 1004, ¶0018.

152. I note that the '039 Patent also acknowledges that the computer system 100 as shown in Figure 3 was well-known in the art, including processor 105, memory 106, storage 109, and I/O Interface 113. Ex. 1001, Fig. 3.

153. Accordingly, it is my opinion that this limitation and construction are disclosed or rendered obvious by Hsu in view of Sanford.

154. **Limitation 13[D]**. The claim requires “*means for determining if the defined memory location is unoccupied,*” which, in my opinion, is disclosed by Hsu and Sanford.

155. I understand that Patent Owner and Apple, Inc. agreed in district court proceedings to the following construction for this term:

Function: determining if the defined memory location is unoccupied

Structure: processor unit 105 running software process(es) 206

Ex. 1013, p. 3.

156. In my opinion, Hsu in view of Sanford discloses this construed limitation.

157. *First*, as I explained for Limitation 1[D], Hsu in view of Sanford discloses the recited **function**.

158. *Second*, it is my opinion that Hsu in view of Sanford discloses the same or equivalent **structure**. For example, the '039 Patent uses a processor unit 105 to determine whether a memory location is unoccupied. Ex. 1001, 6:66-7:1; 8:65-66. The Hsu-Sanford system discloses the same. Sanford discloses a step S202, which determines whether a card (or a user) is already enrolled. Ex. 1004, Fig. 2. As I explained in detail for Limitation 1[D], when checking whether a user is enrolled in Hsu's system, a POSITA would have understood that the straightforward way to do so is to check if the memory location determined by Hsu's user or account number stores a fingerprint—*i.e.*, determining whether that memory location is unoccupied (or empty).

159. Sanford also discloses a processor, which “may be, for example, a computer, workstation, mainframe, pocket PC, personal digital assistant, etc.” Ex. 1004, ¶0018. Sanford also discloses that the processor “preferably includes or is in communication with a verification process 22 and database 24.” *Id.* In my opinion, a POSITA would have understood that Sanford's processor accesses the database 24 in order to determine whether a card (or a user) is enrolled (*i.e.*, step S202). Sanford further discloses that its system “may be a **software-implemented** process that communicates with database 24.” *Id.*

160. Therefore, it is my opinion that a POSITA would have understood that in the Hsu-Sanford system, determining whether a card (or a user) is enrolled is performed by a processor (*e.g.*, Sanford’s processor running its software processes).

161. **Limitation 13[E]**. The claim requires “*means for storing, if the memory location is unoccupied, the biometric signature at the defined memory location,*” which, in my opinion, is disclosed by Hsu and Sanford.

162. I understand that Judge Albright construed this term in district court proceedings as follows:

Function: storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

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.

163. In my opinion, Hsu in view of Sanford discloses this construed limitation.

164. *First*, as I explained for Limitation 1[E], Hsu in view of Sanford discloses the recited **function**.

165. *Second*, Hsu in view of Sanford discloses the same or equivalent **structure**. The construction requires a computer system with a processor to perform the recited storing function. As I explained for Limitation 13[C], a POSITA would have understood that the Hsu-Sanford system is a computer system with a processor, and that Hsu/Sanford discloses a processor and software (which is stored in memory), and these processors/software (*e.g.*, Sanford’s “**software-implemented process**”) are able to access the fingerprint database (storage/memory) and perform fingerprint verification. Ex. 1004, ¶0018. Additionally, as I explained for Limitation 13[D], a POSITA would also have understood that Sanford’s processor that is “in communication with... database 24” reads data from and writes data to the database.

4. Claim 14 is rendered obvious by Hsu and Sanford

166. In my opinion, claim 14 is unpatentable because it is rendered obvious by Hsu and Sanford. Claim 14 of the ’039 Patent recites the following. I address each of these in my analysis below.

[P] A biometric card pointer verified access system comprising:

[A] the biometric card pointer enrolment system of claim 13; and

[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.

167. **Preamble 14[P]**. It is my opinion that Hsu discloses “**a biometric card pointer verified access system.**”

168. As I explained for Limitation 1[P], Hsu discloses a “biometric card pointer system.” As I also explained for Limitation 2[P], Hsu discloses “a method of obtaining verified access to a process [e.g., banking transactions or entering a secured building].”

169. Therefore, it is my opinion that Hsu discloses “**a biometric card pointer verified access system** [e.g., access control unit 14].”

170. **Limitation 14[A]**. The claim requires “the biometric card pointer enrolment system of *claim 13*,” which, in my opinion, is disclosed by Hsu and Sanford, as I explained for claim 13 above, incorporated here.

171. **Limitation 14[B]**. The claim requires “*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,*” which, in my opinion, is disclosed by Hsu in view of Sanford.

172. I understand that Petitioners propose the following construction for this term:

Function: 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.”

Structure: a **computer system** with a **processor** 105 executing an application that compares an inputted biometric signature to a stored biometric signature, a biometric reader 102, a card reader 112, and a database 124; and equivalents thereof.

See Ex. 1001 6:32-38; 6:49-7:8; 7:31-42; 7:50-8:4; 8:5-21; 8:24-43; 9:42-49; Figs. 3, 4.

173. In my opinion, Hsu in view of Sanford discloses this construed limitation.

174. *First*, Hsu discloses the recited **function**, for the same reasons I explained for Limitation 2[C].

175. *Second*, Hsu in view of Sanford discloses the same or equivalent **structure**. For example, Hsu discloses an access control unit having various

components such as a card reader, a fingerprint sensor, a door/access controller, a fingerprint correlator, and a fingerprint database. *See* Ex. 1003, Figs. 2, 3, and 4. Hsu further discloses that “[t]he fingerprint correlator 46 performs the matching function very rapidly by using special-purpose hardware in the form of an application-specific integrated circuit (ASIC), which employs a high degree of **parallel processing**.” Ex. 1003, ¶0023. In my opinion, a POSITA would have understood that ASICs typically include processors and memories and execute programs to perform the desired functions. Therefore, it is my opinion that a POSITA would have understood that the verification process in Hsu (*i.e.*, comparing an inputted fingerprint to a stored fingerprint) would or could obviously be accomplished by at least one processor executing an application.

176. Sanford also provides such details for a system (like Hsu), including that it “includes a **processor**...[t]he processor also preferably includes or is in communication with a verification process...[that] may be a **software-implemented** process [*e.g.*, an application] that communicates with database 24.” Ex. 1004, ¶0018.

5. Claim 19 is rendered obvious by Hsu and Sanford

177. In my opinion, claim 19 is unpatentable because it is rendered obvious by Hsu and Sanford. Claim 19 of the '039 Patent recites the following. I address each of these in my analysis below.

[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:

- [A] code for receiving card information;;
- [B] code for receiving the biometric signature;
- [C] code for defining, dependent upon the received card information, a memory location in a local memory external to the card;
- [D] code for determining if the defined memory location is unoccupied; and
- [E] code for storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

178. **Preamble 19[P]**. It is my opinion that Hsu discloses “[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.”

179. As I explained for Limitation 1[P], Hsu discloses “a method of enrolling in a biometric card pointer system.” Hsu also discloses various components of its biometric card pointer system (*e.g.*, access control unit) in Figs. 2, 3, and 4, such as a card reader, a fingerprint sensor, a door/access controller, a fingerprint correlator, and a fingerprint database. Sanford discloses a similar system (*e.g.*, Sanford’s ACM) including similar components, such as a card reader, a picture-taking device, a verification process, and a database. Sanford’s system “includes a **processor**. The processor may be, for example, a computer,

workstation, mainframe, pocket PC, personal digital assistant, etc. The processor also preferably includes or is in communication with a verification process 22 and **database** 24. Verification process 22 may be a **software-implemented** process that communicates with database 24.” Ex. 1004, ¶0018. A POSITA would have understood that the Hsu-Sanford system includes a processor running computer programs stored on a non-transitory computer readable medium.

180. **Limitation 19[A]**. The claim requires “*code for receiving card information*,” which, in my opinion, is disclosed by Hsu in view of Sanford.

181. I understand that Petitions propose the following construction for this term:

Function: receiving card information

Structure: a card reader 112 capable of communicating with a processor via an I/O interface 11, and equivalents thereof.

See Ex. 1001 Fig. 1, 6:55-56, 8:6-7, 8:11-13, 10:31-33.

182. In my opinion, Hsu in view of Sanford discloses this limitation and construction.

183. For the reasons I discussed for Limitation 13[A], Hsu discloses the **function** of “receiving card information” and the same or equivalent **structure**, *i.e.*, a card reader, for performing such function. Hsu also illustrates in Figures 2

and 3 that the card information is transmitted from the card reader for fingerprint retrieval via Line 48 (orange), which, in my opinion, a POSITA would have understood as disclosing an I/O interface.

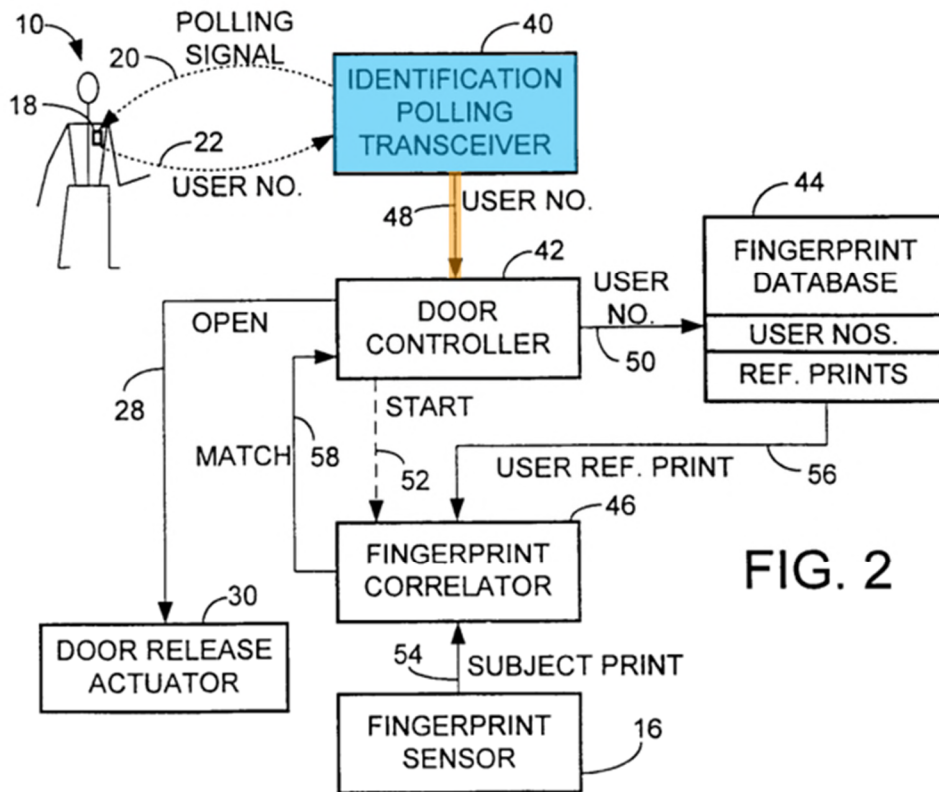
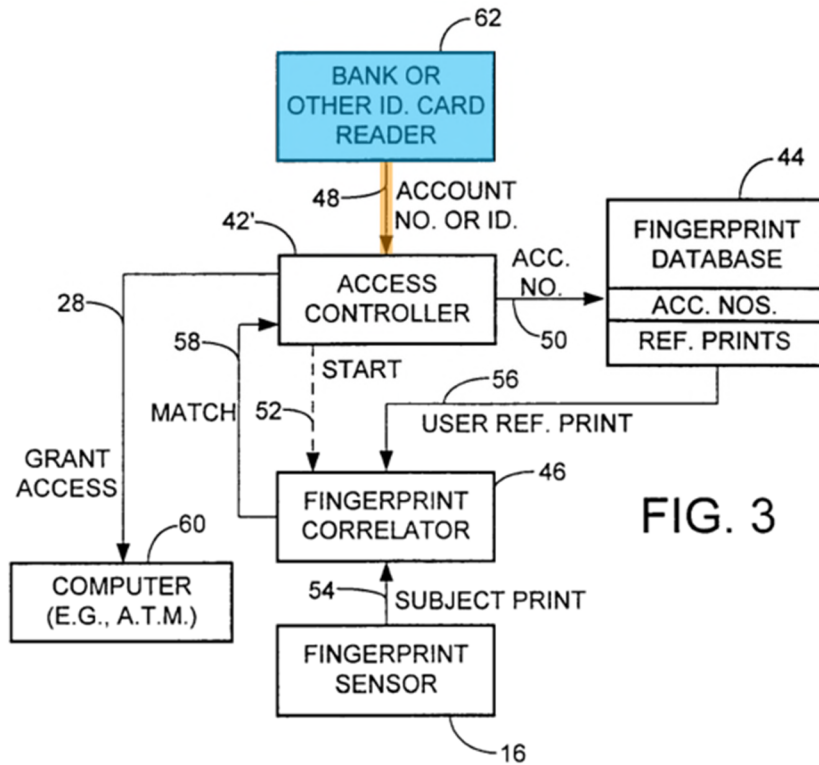


FIG. 2

Ex. 1003, Fig. 2.



Ex. 1003, Fig. 3.

184. Similarly, in Sanford, the card information received at ACM 12 (pink) needs to be transmitted to computer 18 (brown) for fingerprint/picture retrieval.

Ex. 1004, ¶0016, ¶0018.

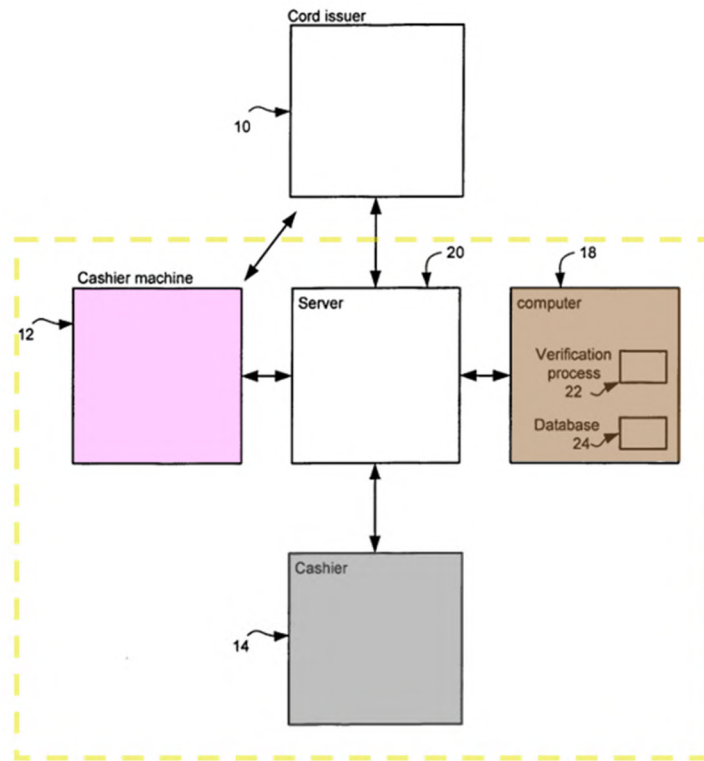


Fig. 1

Ex. 1004, Fig. 1. Sanford’s system “includes a **processor**...[t]he **processor** also preferably includes or is in communication with a verification process...[that] may be a **software-implemented** process [e.g., an application] that communicates with database 24.” Ex. 1004, ¶0018.

185. Accordingly, Hsu in view of Sanford discloses the recited **function** and the same or equivalent **structure** (including code) required by this construed limitation.

186. **Limitation 19[B]**. The claim requires “*code for receiving the biometric signature*,” which, in my opinion, this is disclosed by Hsu and Sanford.

187. I understand that Petitions propose the following construction for this term:

Function: receiving [a] biometric signature

Structure: a biometric reader 102 capable of communicating with a processor via an I/O interface 11; and equivalents thereof.

See Ex. 1001 Fig. 1, 6:55-56, 8:27:31.

188. In my opinion, Hsu in view of Sanford discloses this construed limitation.

189. As I discussed for Limitation 13[B], Hsu discloses the recited **function** and the same or equivalent **structure**. Hsu also illustrates in Figures 2 and 3 that the fingerprint is transmitted from the card reader for verification via Line 54 (orange), which a POSITA would have understood as disclosing an I/O interface.

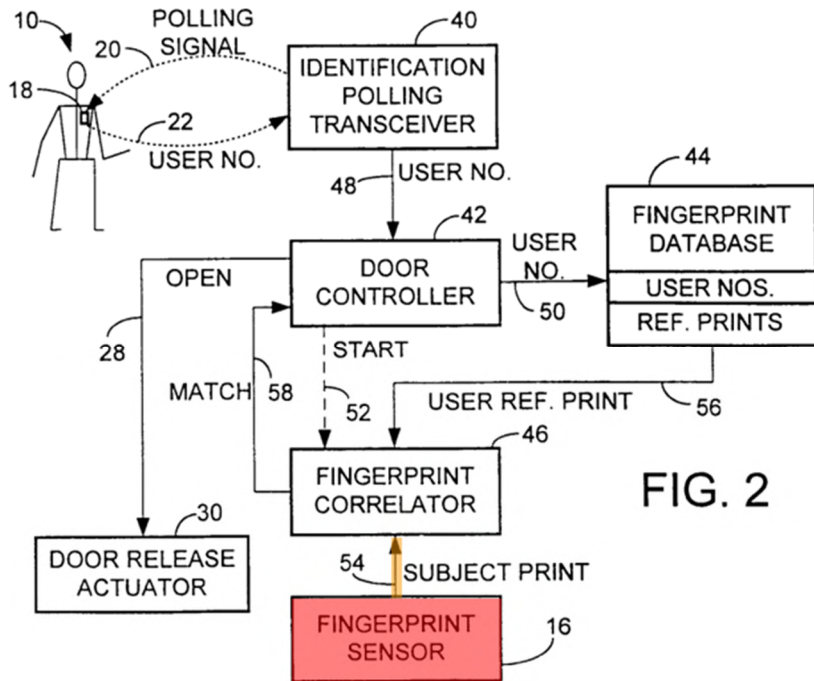


FIG. 2

Ex. 1003, Fig. 2.

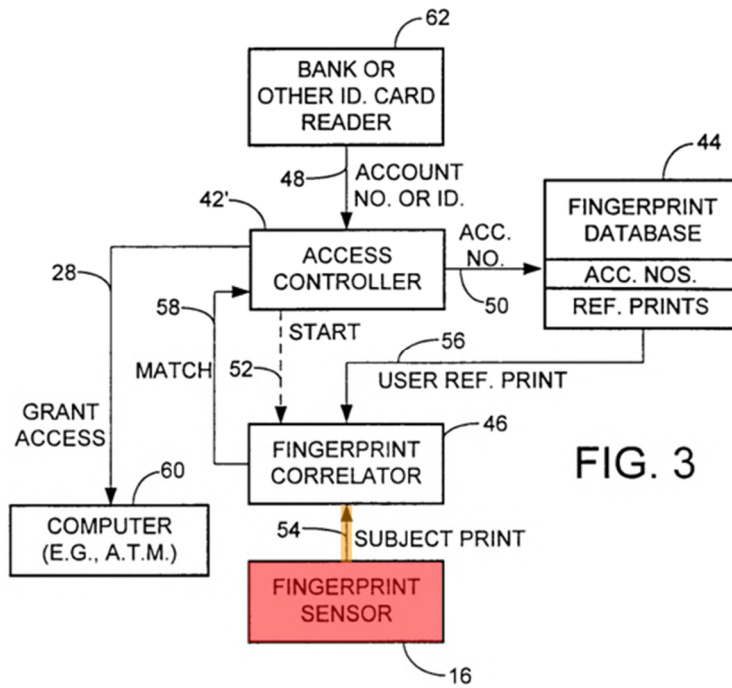


FIG. 3

Ex. 1003, Fig. 3.

190. Similarly, in Sanford, the picture/fingerprint captured by a picture-taking device/fingerprint sensor at ACM 12 (pink) needs to be transmitted to computer 18 (brown) for verification. Ex. 1004, ¶0016, ¶0018.

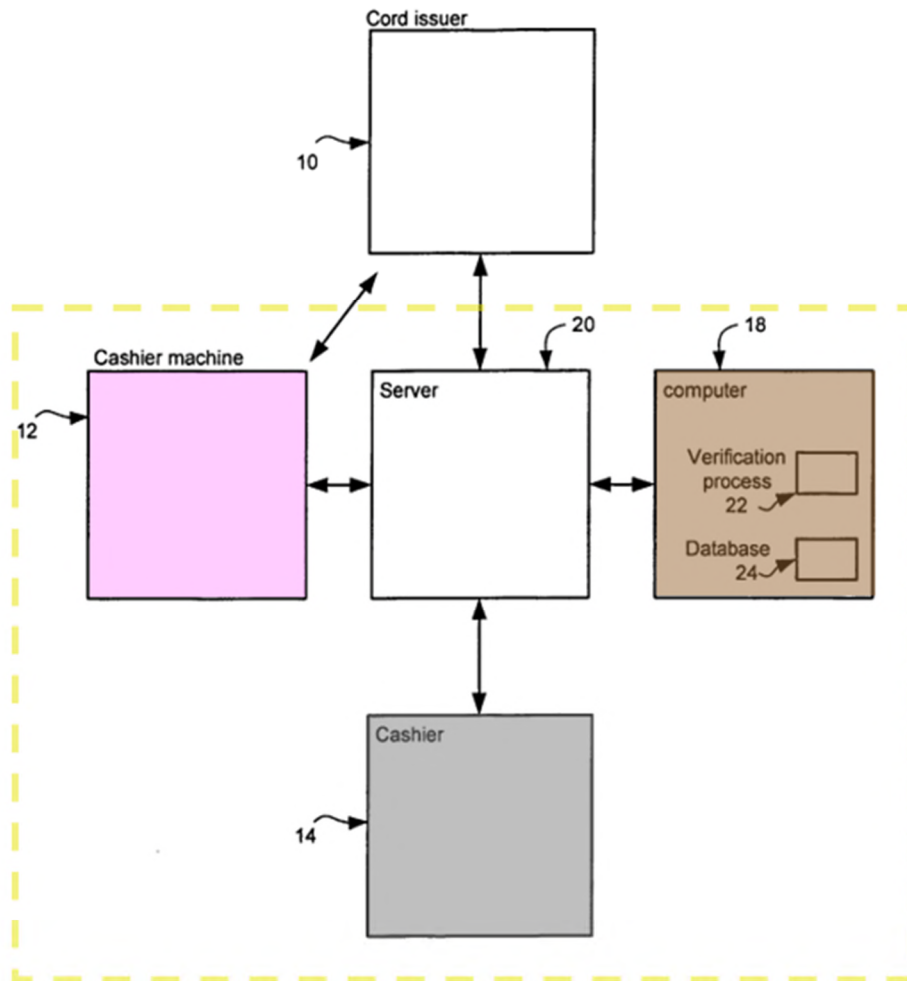


Fig. 1

Ex. 1004, Fig. 1. Sanford's system also "includes a **processor...**[t]he **processor** also preferably includes or is in communication with a verification process...[that]

may be a software-implemented process.” Ex. 1004, ¶0018. In my opinion, a POSITA would have understood that the processor is in communication with the biometric reader.

191. Accordingly, Hsu in view of Sanford discloses the recited **function** and the same or equivalent **structure** (including code) required by this construed limitation.

192. **Limitation 19[C]**. The claim requires “*code for defining, dependent upon the received card information, a memory location in a local memory external to the card,*” which, in my opinion, is disclosed by Hsu and Sanford.

193. I note that this limitation is the same as Limitation 13[C] except that “means for” in Limitation 13[C] is substituted with “code for.” I understand that Petitioners propose this term be construed the same as the corresponding “means for” term in Limitation 13[C]. Therefore, for the same reasons that I set forth for Limitation 13[C], it is my opinion that Hsu in view of Sanford discloses the recited **function** and the same or equivalent **structure** (including code) required by this construed limitation.

194. **Limitation 19[D]**. The claim requires “*code for determining if the defined memory location is unoccupied,*” which, in my opinion, is rendered obvious by Hsu and Sanford.

195. I note that this limitation is the same as Limitation 13[D] except that “means for” in Limitation 13[D] is substituted with “code for.” I understand that Petitioners propose this term be construed the same as the corresponding “means for” term in Limitation 13[D]. Therefore, for the same reasons explained for Limitation 13[D], it is my opinion that Hsu in view of Sanford discloses the recited **function** and the same or equivalent **structure** (including code) required by this construed limitation.

196. **Limitation 19[E]**. The claim requires “*code for storing, if the memory location is unoccupied, the biometric signature at the defined memory location,*” which, in my opinion, is disclosed by Hsu and Sanford.

197. I note that this limitation is the same as Limitation 13[E] except that “means for” in Limitation 13[E] is substituted with “code for.” I understand that Petitioners propose this term be construed the same as the corresponding “means for” term in Limitation 13[E]. Therefore, for the same reasons I explained for Limitation 13[E], it is my opinion that Hsu in view of Sanford discloses the recited **function** and the same or equivalent **structure** (including code) required by this construed limitation.

6. Claim 20 is rendered obvious by Hsu and Sanford

198. In my opinion, claim 20 is unpatentable because it is rendered obvious by Hsu and Sanford. Claim 20 of the '039 Patent recites the following. I address each of these in my analysis below.

[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:

- [A] code for storing a biometric signature according to the enrolment method of claim 19;
- [B] code for subsequently presenting card information and a biometric signature; and
- [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.

199. **Preamble 20[P]**. It is my opinion that Hsu in view of Sanford discloses “[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.”

200. As I explained for Limitation 2[P], Hsu discloses “a method of obtaining verified access to a process.” Hsu also discloses an access control unit having various components such as a card reader, a fingerprint sensor, a door/access controller, a fingerprint correlator, and a fingerprint database, for

performing the method of obtaining verified access to a process. *See* Ex. 1003, Figs. 2, 3, and 4. For reasons I explained for Preamble 19[P], it is my opinion that a POSITA would have understood that the Hsu-Sanford system includes a processor running computer programs stored on a non-transitory computer readable medium.

201. **Limitation 20[A]**. The claim requires “*code for storing a biometric signature according to the enrolment method of claim 19*,” which, in my opinion, is disclosed by Hsu and Sanford.

202. I understand that Petitioners propose this term be treated as a “means for” term. For the same reasons I explained for Limitation 19[E], it is my opinion that Hsu in view of Sanford discloses the recited **function** and the same or equivalent **structure** (including code) required by this limitation.

203. **Limitation 20[B]**. The claim requires “*code for subsequently presenting card information and a biometric signature*,” which, in my opinion, is disclosed by Hsu and Sanford.

204. I understand that Petitions propose the following construction for this term:

Function: presenting card information and a biometric signature

Structure: a card reader 112 capable of communicating with a processor via an I/O interface 11 (Ex. 1001 Fig.1, 6:55-56, 8:6-7, 8:11-13, 10:31-33) and a biometric reader 102 capable of communicating with a processor via an I/O interface 11 (Ex. 1001 Fig. 1, 6:55-56, 8:27:31); and equivalents thereof.

205. In my opinion, Hsu in view of Sanford discloses this construed limitation.

206. *First*, as I explained for Limitation 2[B], Hsu discloses the recited **function**.

207. *Second*, Hsu in view of Sanford discloses the same or equivalent **structure**. As I discussed for Limitations 19[A] and 19[B], both Hsu and Sanford disclose presenting and transmitting the card information received from a card reader and biometric signature captured by a biometric reader to a verification component/process, and the relevant I/O interfaces. Sanford also discloses that its system “includes a **processor**...[t]he **processor** also preferably includes or is in communication with a verification process...[that] may be a software-implemented process.” Ex. 1004, ¶0018. In my opinion, a POSITA would have understood that the processor(s) is in communication with the card reader and biometric reader.

208. Accordingly, Hsu in view of Sanford discloses the recited **function** and the same or equivalent **structure** (including code).

209. **Limitation 20[C]**. The claim requires “*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,*” which, in my opinion, is disclosed by Hsu.

210. I note that this limitation is the almost same as Limitation 13[C] except that “means for” in Limitation 13[C] is substituted with “code for.” I understand that Petitioners propose this term be construed the same as the corresponding “means for” term in Limitation 14[B]. Therefore, for the same reasons I explained for Limitation 14[B], it is my opinion that Hsu discloses the recited **function** and the same or equivalent **structure** (including code) required by this construed limitation.

B. IPR2022-001093 GROUND #2: Claims 1, 2, 13, 14, 19, and 20 are rendered obvious by Hsu, Sanford, and Tsukamura

1. Claim 1 is rendered obvious by Hsu, Sanford, and Tsukamura

211. As I explained in Ground 1, incorporated herein, Hsu in view of Sanford discloses claim 1 under the First Construction of “**defining, dependent upon the received card information, a memory location...**” as I discussed in Section VI.A.1 and found in Limitation 1[C].

212. To the extent the term means “**a memory location is specified by the card information**” (Second Construction), it is my opinion that Hsu in view of Sanford and further in view of Tsukamura discloses claim 1.

213. **Limitation 1[C]**. The claim requires “**defining, dependent upon the received card information, a memory location in a local memory external to the card,**” which, in my opinion, is disclosed by Hsu in view of Tsukamura.

214. In my opinion, a POSITA would also understand that there are many different ways to implement Hsu’s “table that associates each user number with a stored fingerprint image.” Ex. 1003, ¶0020. To the extent that Hsu’s user or account number is deemed to **not specify the physical memory address** where the user’s fingerprint is stored, Tsukamura does, and it would have been obvious to modify Hsu in view of Tsukamura for the reasons provided below (*see full motivation to combine section, infra*).

215. Tsukamura discloses a simple and efficient structure for “stored...fingerprint data” in Figure 3. Ex. 1005, 2:9-10.

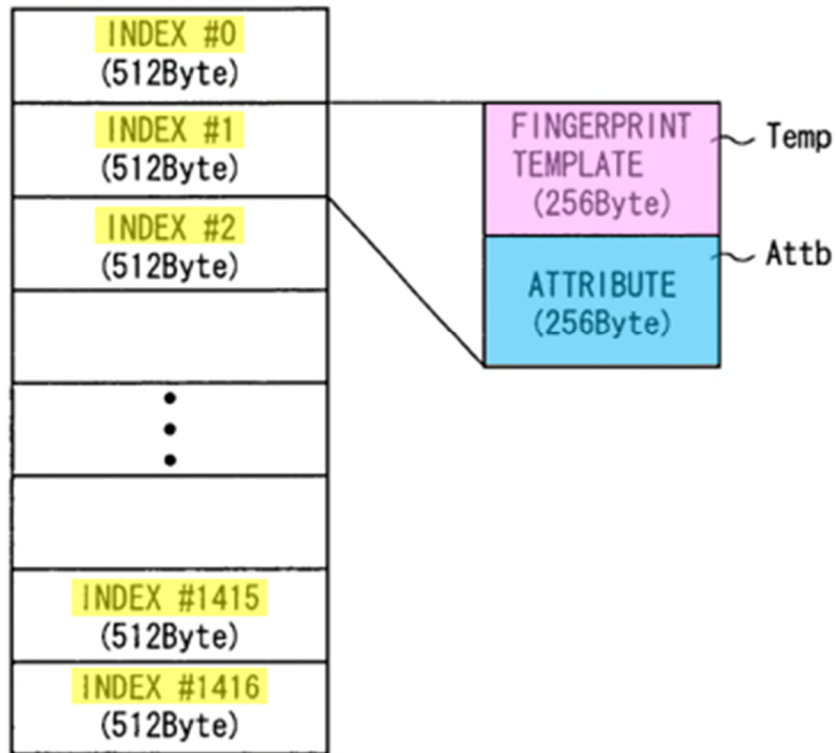


FIG. 3

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, a POSITA would know that **Tsukamura’s index number specifies the physical memory address** 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.*, “a memory location is specified by the card information” under the Second Construction in Section VI.A.1.

216. At the end of claim 1 is a detailed discussion of why it would have been obvious to combine Hsu with Tsukamura.

217. Therefore, it is my opinion that Hsu in view of Tsukamura discloses “**defining, dependent upon the received card information** [*e.g.*, Sanford’s index number used as Hsu’s user/account/employee number from card], **a memory location** [*e.g.*, Tsukamura’s indexed locations in memory] **in a local memory** [*e.g.*, Tsukamura’s local memory] **external to the card** [*e.g.*, external to Hsu’s badge/card or machine-readable card].”

218. **Limitation 1[D]**. The claim requires “determining if the defined memory location is unoccupied,” which, in my opinion, is disclosed by Hsu in view of Sanford and Tsukamura.

219. In my opinion, the way to check whether a user has been enrolled in the Hsu-Sanford-Tsukamura system is to check whether Tsukamura’s memory

location for storing the user's fingerprint is occupied. As shown in Figure 3 below, the index numbers (yellow) are used to specify physical memory addresses for storing fingerprint templates (pink) for different users.

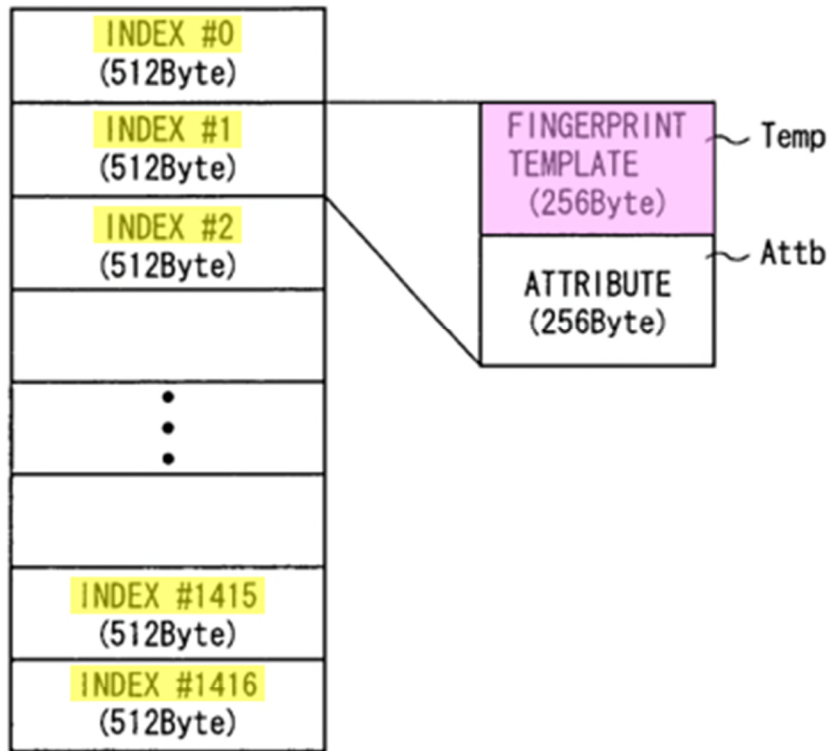


FIG. 3

Ex. 1005, Fig. 3. Tsukamura does not disclose any other memory structure for storing fingerprints, such as storing a list of enrolled users or storing the index numbers themselves in memory. Nor does Sanford disclose any specific way of checking whether a user is enrolled other than by searching its database. Ex. 1004,

¶0025. Therefore, in my opinion, a POSITA would have understood that to determine whether a user is enrolled in the Hsu-Sanford-Tsukamura system is to check whether the memory location specified by the Hsu-Tsukamura account/index number is occupied (*i.e.*, stores a fingerprint). If the memory location is occupied by an existing fingerprint, then the user associated with the account/index number is already enrolled. Otherwise, the user is not enrolled.

220. Therefore, it is my opinion that the Hsu-Sanford-Tsukamura combination discloses “**determining if the defined memory location** [*e.g.*, Tsukamura’s memory location defined by Hsu’s user/account/employee number as modified by Tsukamura’s index number] **is unoccupied** [*e.g.*, Sanford’s teaching to check if a user is enrolled by checking Tsukamura’s memory location for that user (*e.g.*, Hsu’s user)].”

221. **Limitation 1[E]**. The claim requires “storing, if the memory location is unoccupied, the biometric signature at the defined memory location,” which, in my opinion, is disclosed by Hsu in view of Sanford and Tsukamura.

222. Just like Hsu and Sanford, Tsukamura also discloses an enrollment process involving storing fingerprints. Ex. 1003, Fig. 4, ¶0026 (“The account number is stored in the database 44 in association with the user’s fingerprint image data.”); Ex. 1005, 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”). Thus, the references all disclose storing a user’s fingerprint at the appropriate memory location, which here is the Tsukamura’s physical memory location defined by the Hsu-Tsukamura user account/index number.

223. Therefore, it is my opinion that the Hsu-Sanford-Tsukamura combination discloses “**storing, if the memory location is unoccupied** [*e.g.*, checking Tsukamura’s memory location to see if a user is enrolled per Sanford, and if not, storing], **the biometric signature** [*e.g.*, Hsu’s fingerprint signature] **at the defined memory location** [*e.g.*, Tsukamura memory location defined by the Hsu-Tsukamura account/index number].”

224. **Motivation to Combine Hsu-Sanford and Tsukamura.** The ’039 Patent, Hsu, Sanford, and Tsukamura are all in **the same field of endeavor**, *i.e.*, access control using biometric authentication. All references (and the ’039 Patent) are directed to ways of 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. Hsu discloses the stored fingerprint data being associated with a user/account/employee number from a user’s card. Ex. 1003,

¶0026. Sanford discloses using a user's picture (or fingerprint) associated with a user's credit card number. Ex. 1003, ¶¶0018-21. 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 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.

225. I note that comparing fingerprints in a one-to-one manner is also known as “one-to-one match” and was well known in the art for its benefits over “one-to-many match” before the '039 Patent. As its name suggests, a “one-to-one match” happens when you compare a captured fingerprint to a single reference fingerprint and determine if the captured fingerprint matches this particular reference fingerprint. In other words, a “*one-to-one match*” requires you to *perform only one comparison*. In contrast, a “one-to-many match” happens when you compare a captured fingerprint to each of many reference fingerprints to determine if the captured fingerprint matches *any* of the many reference fingerprints—*i.e.*, using the captured fingerprint to search the entire reference fingerprints to find a match. In other words, a “*one-to-many match*” requires you to *compare N times*, where N equals to the number of reference fingerprints in the database. Obviously, a “one-to-one match” is far more efficient than a “one-to-

many match” due to the difference in the number of comparisons needed. This is significant because biometric comparison is generally complex and takes considerable time and computer processing resources. This is explicitly recognized in Hsu: “Even with the availability of high-speed computer processors, a fingerprint matching system that must compare a sensed fingerprint image with many possible stored reference images will not operate fast enough to provide rapid access to a building.” Ex. 1003, ¶0004; *see also id.*, ¶0013.

226. As another example, Black also mentions that “the matching is **preferably one-to-one** as opposed to one-to-many.” Ex. 1017, p. 16. This is because “one-to-one matches” provide many benefits compared to “one-to-many matches,” such as, “considerably faster” “[p]rocessing speed” (*id.*), better suitability for “open environment situations where the size of the community is continually expanding through registration without limitation” (*id.*), and “far less complex” “biometric sensing” (*e.g.*, stringent sensor quality and fewer sensors) (*id.*, pp. 21, 16]). *See also* Ex. 1018, 33:34-35:4 (“The above method of looking up the user ID and then checking the authenticity of the owner by his fingerprint enables a so-called ‘one-to-one’ match. Thereby the number of users does not dilute the security of the system. The system will thereby provide maximum security, even for large user groups *e.g.* within a hospital.”).

227. When implementing a “one-to-one match,” a POSITA would have understood that the single reference biometric being compared against must be *somehow* identified among many. Indeed, there are different ways to do so. One method is to use something as a *pointer* to the stored reference biometric, just like the '039 Patent. A POSITA would have understood that other forms of identifiers could also be used, such as a PIN, a passport, a date of birth, a license plate, and etc, as long as it “uniquely identifies the user.” *See* Ex. 1004, ¶0019. Another way to do so is to store the reference biometric directly on the card. When performing verification, the reference biometric can be retrieved directly from the card. This is described at length in Tsukamura. Ex. 1005, 4:31-5:2 (“(302) Fingerprint Collation Process with Fingerprint Template within IC Card...”); *see also* Ex. 1017, p.7 (“... one-to-one biometric matching is used. This embodiment requires each user to carry on his/her user a device that includes an encrypted reference biometric for reference purposes to gain access into the system. The encryption device can be the stylus, a card, a stylus insert, or a device carried on a key-chain”). Again, these were all very well-known techniques used in biometric verification systems before the '039 Patent.

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

“FIG. 4 illustrates an enrollment procedure that is required for any of the configurations described above. It has been assumed in the foregoing description that the fingerprint database 44 contains reference fingerprint image data for each user, employee, or customer using the system, and that the reference fingerprint data are associated with corresponding user numbers, or employee or customer account numbers.”

Ex. 1003, ¶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.

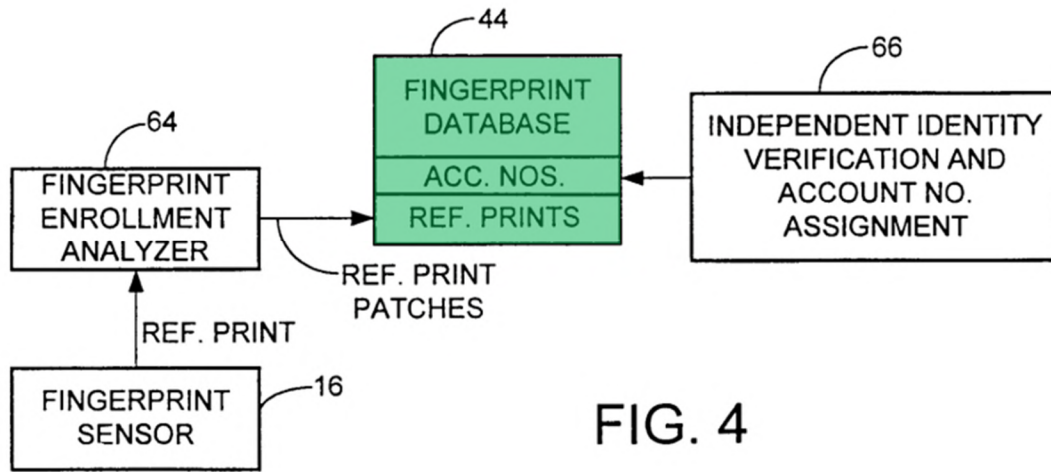


FIG. 4

Ex. 1003, Fig. 4.

229. In my opinion, it was common knowledge to a POSITA that there are multiple ways of generating and storing a table that associates each user number with a stored fingerprint.

230. As I mentioned in above in Section VI.A.1, there are different interpretations as to whether the language “defining, dependent upon the received card information, a memory location” requires the card information itself to specify the physical memory address where the user’s fingerprint is stored. However, a POSITA would have known that there existed a number of simple and well-known ways to store a list of fingerprints such that each fingerprint accessible at a specified physical memory address. For example, Wirth (textbook published in 1976), describes a “linear mapping function” which calculates “[t]he address... *i*

of the j th array” based on “the address of the first component $[i_0]$ and... the number of words $[s]$ that a component ‘occupies’”:

$$i = i_0 + j * s$$

Ex. 1019, p. 30. This is essentially the same memory configuration as described in Tsukamura (*i.e.*, continuous layout), where j becomes Tsukamura’s index number and s equals 512 bytes. *See* Ex. 1005, Fig. 4; *see also* Ex. 1020 (textbook published in 1973), p. 240 (“The simplest and most natural way to keep a linear list inside a computer is to put the list items in sequential locations, one node after the other.... This technique for representing a linear list is so obvious and well-known that there seems to be no need to dwell on it at any length.”).

231. Hashing is another well-known example. As described in Knuth (textbook published in 1973), hashing refers to a process where, given an argument or key K , “the location of K ” is calculated by using a “hash function $h(K)$.” Ex. 1021, pp. 506-508; *see also* Ex. 1019 pp. 264-265 (“4.6. KEY TRANSFORMATIONS (HASHING)... finding an appropriate mapping H of keys (K) into addresses (A).”). Since each user’s fingerprint must be stored at a unique memory address, such requirement can easily be satisfied by “[c]ollision handling” in hashing. Ex. 1019, p. 266 (“4.6.2. Collision Handling”); *see also* Ex. 1022 (paper published in 1977), p. 841 (“it is common practice to use an identifier-to-address function h to store elements of I in a *hash table* and then to use the same

function h to retrieve ω in the table.... if h transforms the identifies in I into unique addresses, a single probe is sufficient. Such a transformation will be called a *perfect hashing function.*”).

232. Thus, various techniques of defining a specific physical memory address to store and retrieve a user’s fingerprint were well-known as early as the 1970s, and there is nothing innovative about “defining, dependent upon the received card information, a memory location” (or any variation of this language) as recited by the challenged claims.

233. Again, Tsukamura teaches one of the simplest and most efficient ways of generating and storing a table that associates each user number with a stored fingerprint by **storing** fingerprints consecutively in memory at indexed locations, as shown in Figure 3 below.

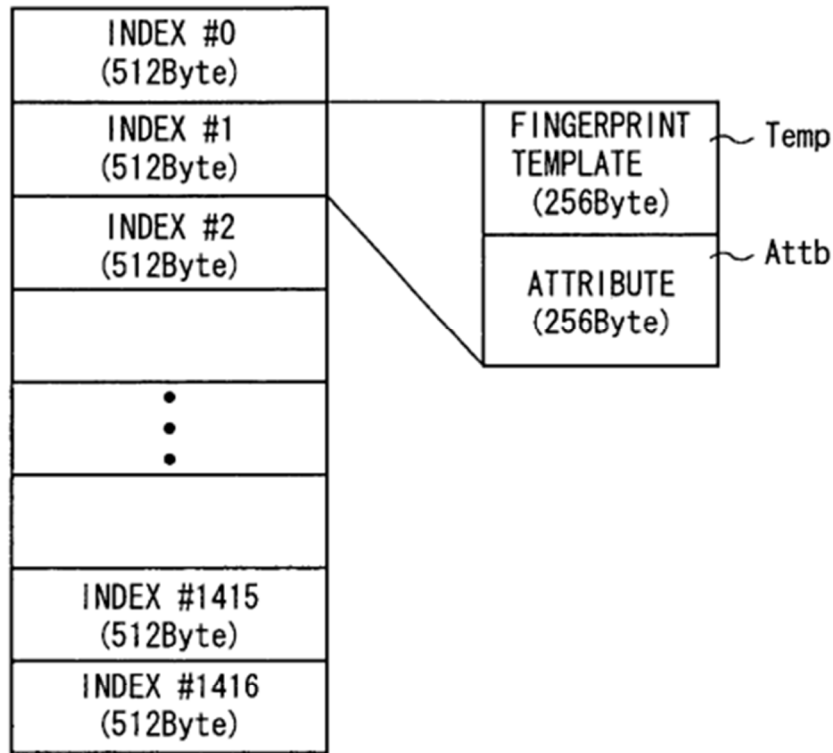


FIG. 3

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 byte), the memory location for any user’s fingerprint is defined based on the index number. *Id.*

234. 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.”).

235. I note that a POSITA would have understood that “collate” here means “compare” or “verify,” for multiple reasons. First, Tsukamura discloses a “fingerprint **collation** process” (Ex. 1005, 3:36) as a different process from a “fingerprint **registration** process” (*id.* 2:39), and therefore “collation” does not mean “registration” (or storing”). Second, Tsukamura uses “collate” as synonymous with “compare.” *See, e.g.*, Ex. 1005 4:7-11 (“**collates** the fingerprint image data D37 **with** the read fingerprint template Temp.”); *see also* Abstract (“**collating** the read fingerprint information with the registered fingerprint information to **effect personal authentication and output a result of authentication** when the read history information is stored in the read history storage.”). Finally, dictionary definitions also confirm that “collate” means “compare” in this context. *See, e.g.*, Ex. 1014, p. 373 (“COMPARE INFORMATION”); Ex. 1015, p. 299 (“to bring together for comparison; to examine and compare”).

236. 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. In my opinion, 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.

237. Hsu values speed of matching: “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. It is my opinion that a POSITA implementing the Hsu-Sanford system would have been motivated to use Tsukamura’s memory structure to improve the speed and efficiency of Hsu’s system. It is also my opinion that a POSITA would further understand 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 corresponding index numbers. Ex. 1005, Fig. 4.

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

239. In my opinion, a POSITA likewise would have had a **reasonable expectation of success** in using Tsukamura's memory structure in Hsu-Sanford's database. As mentioned above, both Tsukamura and Hsu-Sanford store and allow access to a user's fingerprint based on a number (*e.g.*, user/account/employee or index number) provided by a user. A POSITA would have understood that implementing Tsukamura's memory structure and index numbers in Hsu's

database would result in a working system having improved speed and efficiency. Therefore, it is my opinion that a POSITA would have had a reasonable expectation of success in using Tsukamura's memory structure for Hsu's database to efficiently store and retrieve fingerprints.

2. Claim 2 is rendered obvious by Hsu, Sanford, and Tsukamura

240. While Hsu-Sanford (Ground 1) discloses claim 2, incorporated here, it is my opinion that Hsu in view of Sanford and further in view of Tsukamura discloses certain limitations of claim 2 for the following additional reasons specific to this Ground.

241. **Limitation 2[A]**. The claim requires “**storing a biometric signature according to the enrolment method of claim 1,**” which, in my opinion, is disclosed by Hsu, Sanford, and Tsukamura, as explained for Limitation 1[E] (Ground 2), incorporated here.

242. **Limitation 2[C]**. The fingerprint in the Hsu-Sanford-Tsukamura system is stored “**at the memory location [e.g., Tsukamura's memory location], in said local memory [e.g., Hsu-Tsukamura's local memory], defined by the subsequently presented card information [e.g., Hsu-Tsukamura account/index number],**” as I explained for Limitation 1[E] (Ground 2), incorporated here. Therefore, it is my opinion that the Hsu-Sanford-Tsukamura combination discloses

“**verifying the subsequently presented presentation of the card information** [e.g., Hsu-Tsukamura account/index number] **and the biometric signature** [e.g., Hsu’s fingerprint image] **if the subsequently presented biometric signature** [e.g., Hsu’s fingerprint image] **matches the biometric signature at the memory location** [e.g., fingerprint image at Tsukamura’s memory location], **in said local memory** [e.g., Hsu-Tsukamura’s local memory], **defined by the subsequently presented card information** [e.g., Hsu-Tsukamura account/index number from card].”

3. Claim 13 is rendered obvious by Hsu, Sanford, and Tsukamura

243. While Hsu-Sanford (Ground 1) discloses claim 13, incorporated here, it is my opinion that Hsu in view of Sanford and further in view of Tsukamura discloses certain limitations of claim 13 for the following additional reasons specific to this Ground.

244. **Limitation 13[C]**. The claim requires “*means for defining, dependent upon the received card information, a memory location in a local memory external to the card,*” which, in my opinion, is disclosed by Hsu, Sanford, and Tsukamura.

245. *First*, as explained for Limitation 1[C] (Ground 2), Hsu, Sanford, and Tsukamura disclose the recited **function**.

246. *Second*, in my opinion, the Hsu-Sanford-Tsukamura system discloses the same or equivalent **structure**. In addition to reasons explained for Limitation 13[C] (Ground 1), incorporated here, it is my opinion that Tsukamura's Figure 3 (and accompanying description) discloses that the memory location for each fingerprint template is determined by an index number:

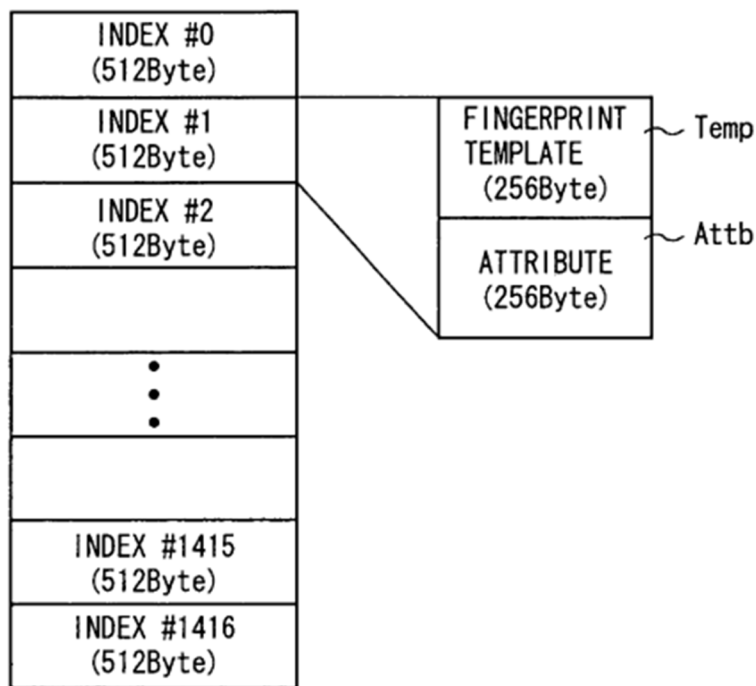
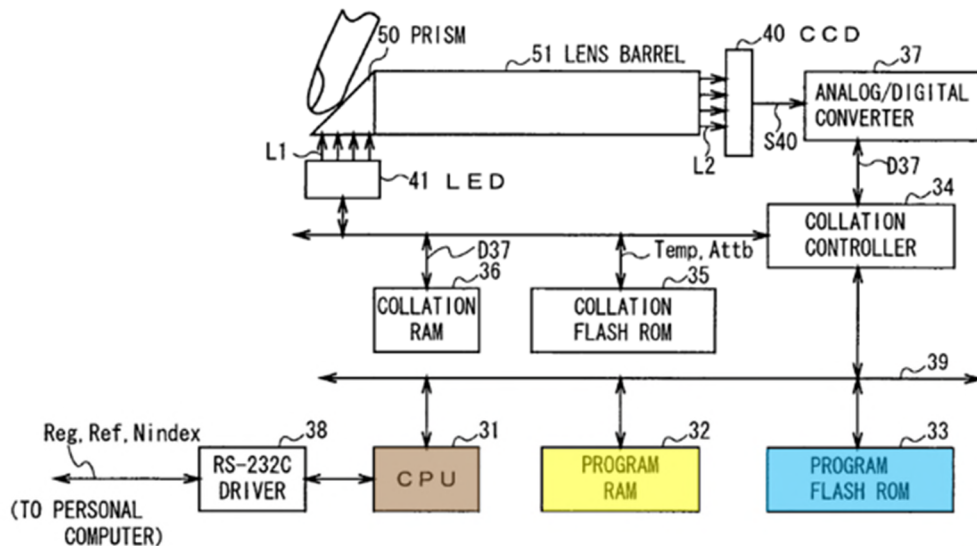


FIG. 3

Ex. 1005, Fig. 3. In addition, within each 512-byte long memory block, the first 256 bytes are for storing a fingerprint template, and the second 256 bytes are for storing an attribute. Therefore, in the Hsu-Sanford-Tsukamura system, each index

number of Tsukamura's is assigned as Hsu-Sanford's user/account number, and defines (specifies) the physical memory address at which that user's biometric signature will be stored. This memory location is of course in a local memory external to the card. *Id.*, 2:18-38, 3:25-34, Figs. 1, 2.

247. Moreover, it is my opinion that Hsu-Sanford-Tsukamura discloses or renders obvious that a fingerprint matching system has computer processors. In addition to reasons I explained for Limitation 13[C] (Ground 1) and incorporated here, Tsukamura also discloses its fingerprint collating unit as a computer system that includes a CPU (*i.e.*, a processor):



30

FIG. 2

Id., Fig. 2; Ex. 1005, 2:7-8. As shown, “[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. *I.e.*, a POSITA would also have understood Tsukamura discloses a processor (*e.g.*, CPU 31) running software (*e.g.*, a control program) that is stored in memory or a computer readable medium (*e.g.*, RAM 32).

248. **Limitation 13[D]**. The claim requires “*means for determining if the defined memory location is unoccupied,*” which, in my opinion, is disclosed by Hsu, Sanford, and Tsukamura.

249. *First*, as I explained for Limitation 1[D] (Ground 2), Hsu in view of Tsukamura and Sanford discloses the recited **function**.

250. *Second*, it is my opinion that Hsu-Sanford-Tsukamura discloses the same or equivalent **structure**. In addition to the reasons I explained for Limitation 13[D] (Ground 1) and incorporated here, Tsukamura also discloses the same or equivalent **structure**. As I discussed for Limitation 13[C], Tsukamura discloses a processor (*i.e.*, CPU 31) running software (*e.g.*, a control program) that is stored in memory or a computer readable medium (*e.g.*, RAM 32). Ex. 1005, 2:50-56. Since Tsukamura’s fingerprint collating unit 30 “accepts a user’s fingerprint [] and collates the fingerprint” (*id.*, 2:26-27), it is my opinion that a POSITA would have understood that the same CPU running a control program (code) performs the recited determining function, which occurs before comparing and storing the fingerprint.

251. **Limitation 13[E]**. The claim requires “*means for storing, if the memory location is unoccupied, the biometric signature at the defined memory location,*” which, in my opinion, is disclosed by Hsu, Sanford, and Tsukamura.

252. *First*, as I explained for Limitation 1[E] (Ground 2), Hsu-Sanford-Tsukamura discloses the recited **function**.

253. *Second*, it is my opinion that Hsu-Sanford-Tsukamura discloses the same or equivalent **structure**. In addition to reasons explained for Limitation 13[D] (Ground 1) and incorporated here, Tsukamura also discloses the same or equivalent **structure** because 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.” A POSITA would have understood that RAM stands for Random Access Memory and is a type of memory.

4. Claim 14 is rendered obvious by Hsu, Sanford, and Tsukamura

254. While Hsu-Sanford (Ground 1) discloses claim 14, incorporated here, it is my opinion that Hsu in view of Sanford and further in view of Tsukamura discloses certain limitations of claim 14 for the following additional reasons specific to this Ground.

255. **Limitation 14[A]**. The claim requires “the biometric card pointer enrolment system of claim 13,” which, in my opinion, is disclosed by Hsu, Sanford, and Tsukamura, as I explained for Limitation claim 13 (Ground 2), incorporated here.

256. **Limitation 14[B]**. The claim requires “*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,*” which, in my opinion, is disclosed by Hsu, Sanford, and Tsukamura.

257. *First*, as I explained for Limitation 1[C] (Ground 2), Hsu-Sanford-Tsukamura discloses the recited **function**.

258. *Second*, it is my opinion that Hsu-Sanford-Tsukamura discloses the same or equivalent **structure**. In addition to reasons explained for Limitation 14[B] (Ground 1) and incorporated here, Tsukamura also discloses the same or equivalent **structure** because Tsukamura’s CPU 31 “control[s] the whole of the fingerprint collating unit 30” (Ex. 1005, 2:50-53). As such, it is my opinion that a POSITA would have found it obvious to use the same CPU 31 to control the entire

Hsu-Tsukamura system, including comparing an inputted fingerprint with a stored fingerprint.

5. Claim 19 is rendered obvious by Hsu, Sanford, and Tsukamura

259. While Hsu-Sanford (Ground 1) discloses claim 19, incorporated here, it is my opinion that Hsu in view of Sanford and further in view of Tsukamura discloses certain limitations of claim 19 for the following additional reasons specific to this Ground.

260. **Limitations 19[C-E]**. I understand that Petitioners propose these terms be treated the same as “means for” terms. Therefore, for the same reasons set forth for Limitations 13[C]-[E] (Ground 2), Hsu-Sanford-Tsukamura discloses the recited function and the same or equivalent structure required by these limitations.

261. To the extent that the term “**code for**” requires disclosure of computer program or code that performs the recited function, it is my opinion that a POSITA would have understood that the Hsu-Sanford-Tsukamura system includes a processor (*i.e.*, Tsukamura’s CPU 31) running software (*e.g.*, Tsukamura’s control program) that is stored in memory or a computer readable medium (*e.g.*, Tsukamura’s RAM 32), to effectuate the recited functions in these limitations.

262. Accordingly, Hsu in view of Sanford and Tsukamura discloses the recited **function** and the same or equivalent **structure** (including code).

6. Claim 20 is rendered obvious by Hsu, Sanford, and Tsukamura

263. While Hsu-Sanford (Ground 1) discloses claim 20, incorporated here, it is my opinion that Hsu in view of Sanford and further in view of Tsukamura discloses certain limitations of claim 20 for the following additional reasons specific to this Ground.

264. **Limitations 20[A] and 20[C]**. I understand that Petitioners propose these terms be treated the same as “means for” terms. Therefore, for the same reasons I explained for claim 19 (Ground 2) and Limitation 14[B] (Ground 2), Hsu-Sanford-Tsukamura discloses the recited function and the same or equivalent structure required by these limitations.

265. To the extent that the term “code for” requires disclosure of computer program or code that performs the recited function, it is my opinion that a POSITA would have understood that the combined Hsu-Sanford-Tsukamura system includes a processor (*i.e.*, Tsukamura’s CPU 31) running software (*e.g.*, Tsukamura’s control program) that is stored in memory or a computer readable medium (*e.g.*, Tsukamura’s RAM 32), to effectuate the recited functions.

266. Accordingly, Hsu in view of Sanford and Tsukamura discloses the recited **function** and the same or equivalent **structure** (including code).

C. IPR2022-001094 GROUND #1: 3, 4, 6-11, 15, 16, and 18 are Rendered Obvious by Sanford and Hsu

1. Claim 3 is rendered obvious by Sanford and Hsu

267. In my opinion, claim 3 is unpatentable because it is rendered obvious by Sanford and Hsu. Claim 3 of the '039 Patent recites the following. I address each of these in my analysis below.

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

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

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

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

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

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

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

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

[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;
[E(2)] (eb) if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and
[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.

268. **Preamble 3[P]**: In my opinion, Sanford discloses “[a] method of securing a process at a verification station.”

269. 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.*

270. Sanford illustrates an exemplary system in Figure 1:

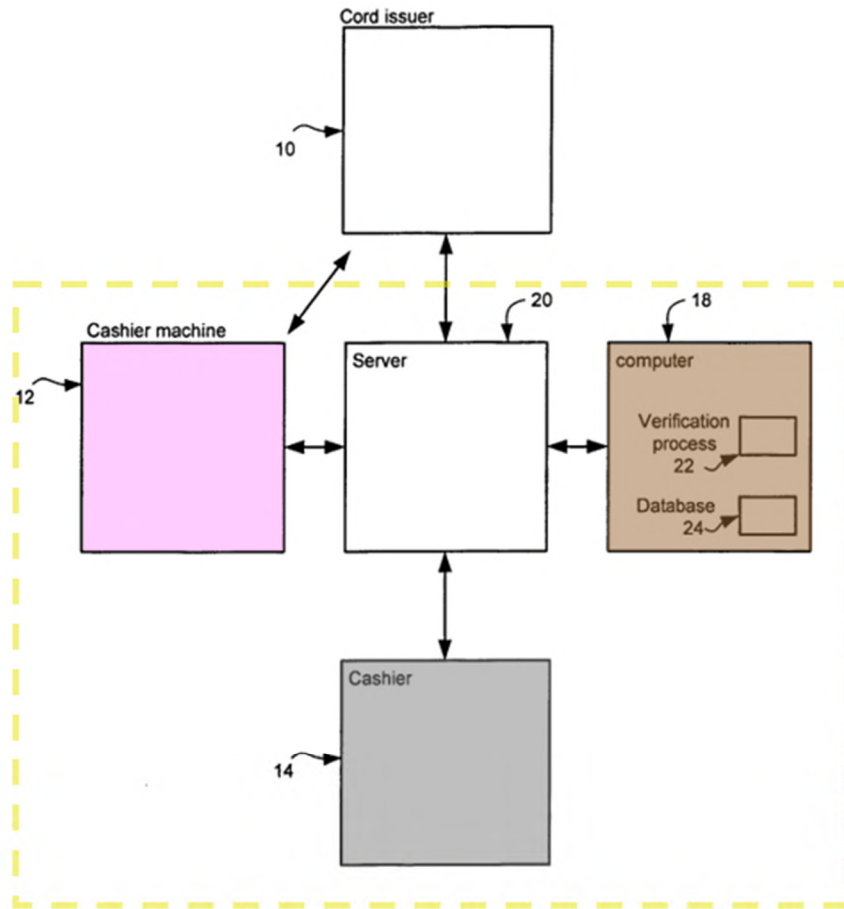


Fig. 1

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.*, ¶10014. 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].” *Id.*, ¶0015. I noted that A POSITA would have understood that these components of Sanford’s system may be present at the same physical facility.

271. Unless otherwise specified, I refer to the ACM indicated by the yellow box (as shown in Fig. 1 above) 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. Figure 2 shows “a method for conducting a PIN-less credit card transaction” performed by Sanford’s ACM. *Id.*, ¶0024.

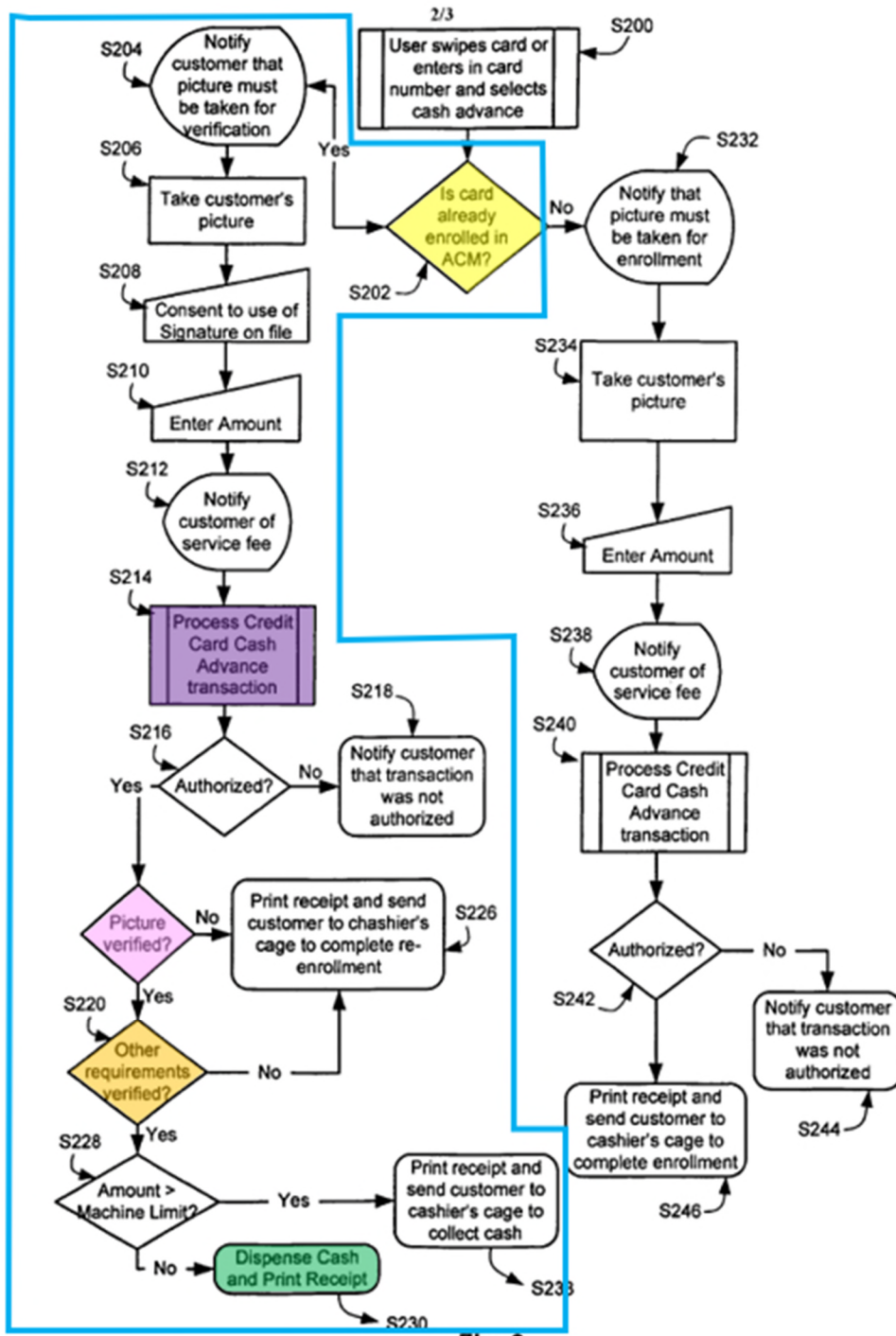


Fig. 2

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.*, ¶10025, ¶10028, ¶10031.

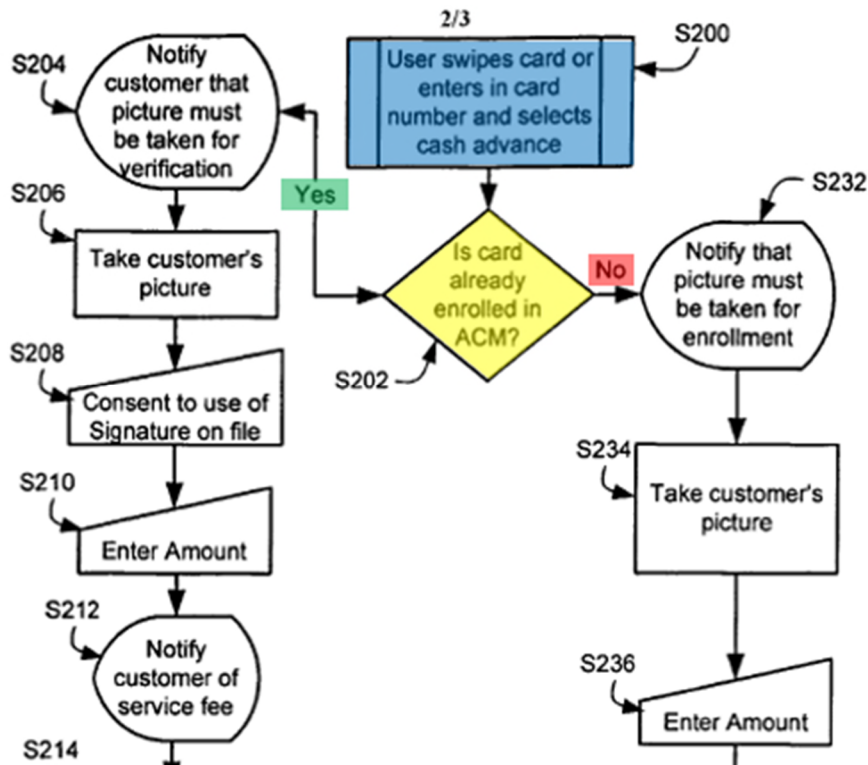
272. Therefore, it is my opinion that Sanford discloses “**a method of securing a process** [*e.g.*, Automated Cash Machine (ACM) cash withdrawal or a PIN-less credit card transaction] **at a verification station** [*e.g.*, Sanford’s ACM].”

273. **Limitation 3[A]**: In my opinion, Sanford discloses “(a) providing card information from a card device to a card reader in the verification station.”

274. 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.

275. 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 I mentioned for Limitation 3[P] above, Sanford’s ACM includes ACM 12 and its card reader is capable of reading credit cards.

276. 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.*, ¶10024. 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.*, ¶10025. Thus, in my opinion, a POSITA would have understood that the credit card account number is provided to the card reader by “inserting or swiping” the card.

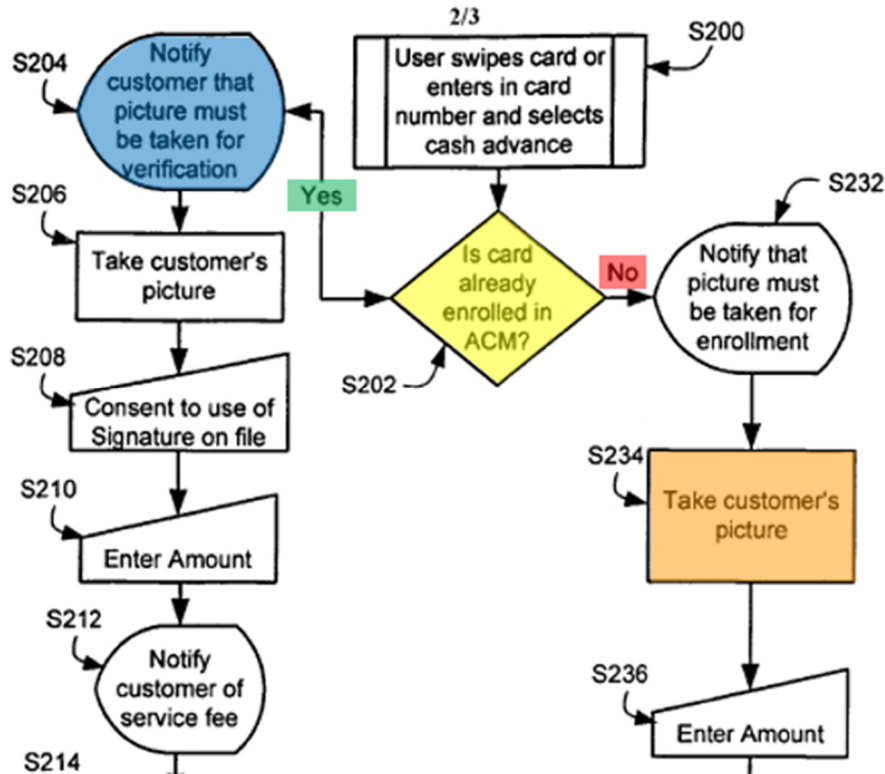
277. Therefore, it is my opinion that Sanford discloses “(a) **providing card information** [e.g., credit card account number] **from a card device** [e.g., credit

card] to a card reader [e.g., card reader] in the verification station [e.g., Sanford's ACM].”

278. **Limitation 3[B]**: In my opinion, Sanford discloses “(b) inputting a biometric signature of a user of the card device to a biometric reader in the verification station.”

279. 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. In my opinion, 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.

280. 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.

281. Therefore, it is my opinion that 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].**”

282. **Limitation 3[C]**: In my opinion, Sanford discloses “(c) determining if the provided card information has been previously provided to the verification station.”

283. 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, it is my opinion that 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.

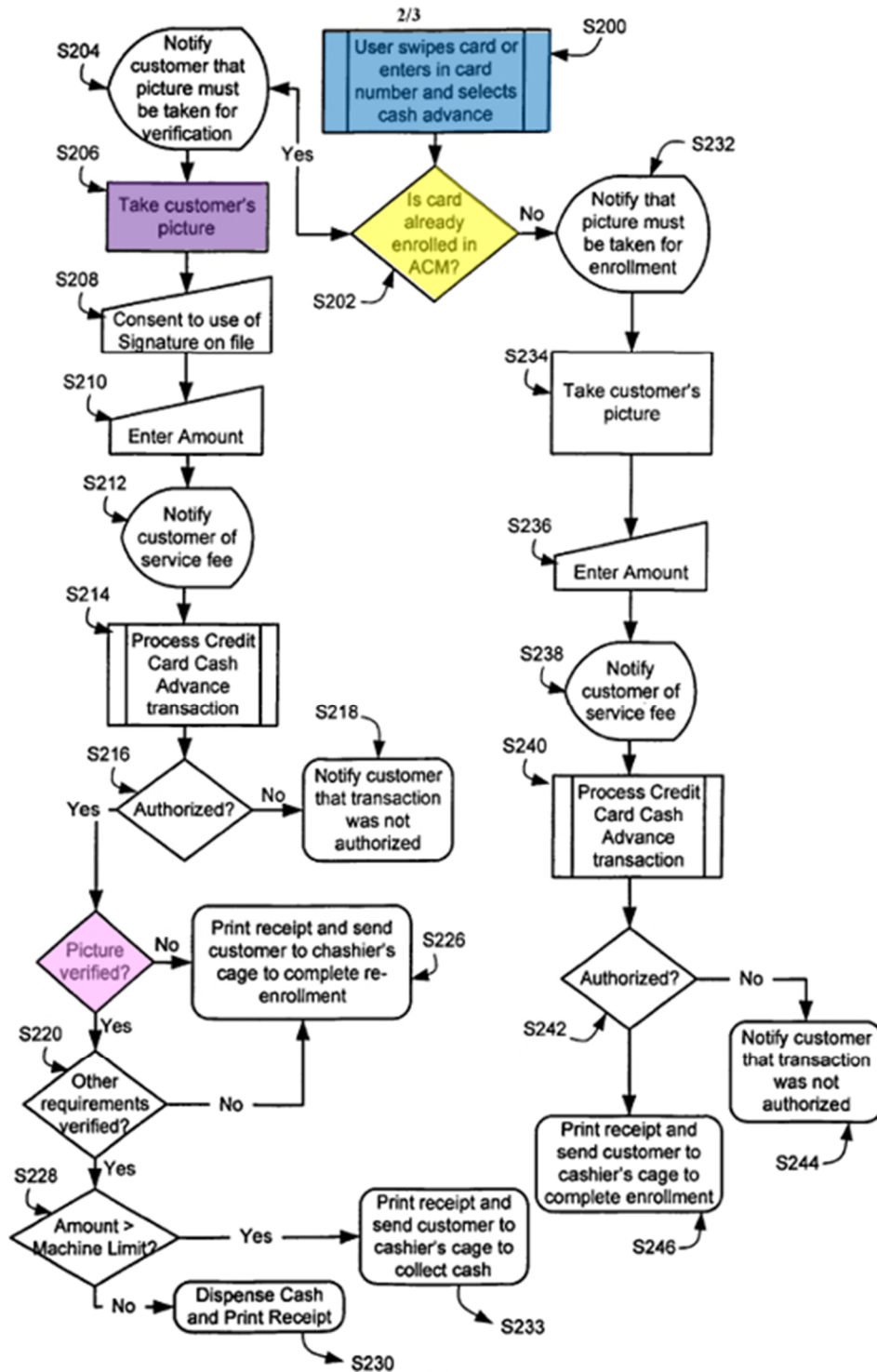


Fig. 2

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). *Id.*, ¶0026, ¶0030.

284. I note that, 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, it is my opinion that a POSITA would have understood that the step colored in pink is step S219.

285. Therefore, it is my opinion that 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].**”

286. **Limitation 3[D(P)+D(1)]**: In my opinion, Sanford in view of Hsu discloses “(d) if the provided card information has not been previously provided to the verification station; (da) storing the inputted biometric signature in a memory at a memory location defined by the provided card information.”

287. 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* Limitation 3[B].

288. 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.

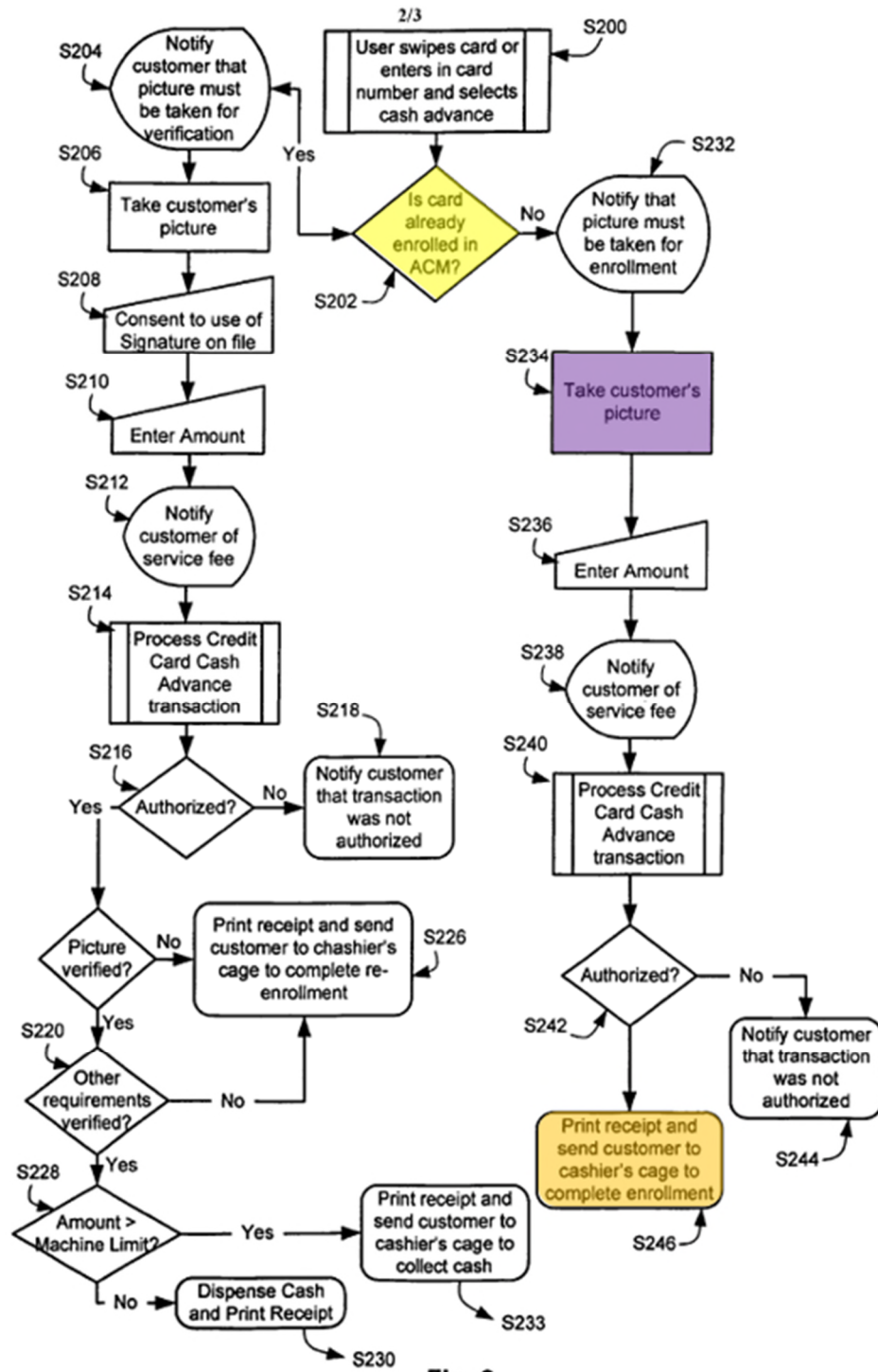


Fig. 2

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):

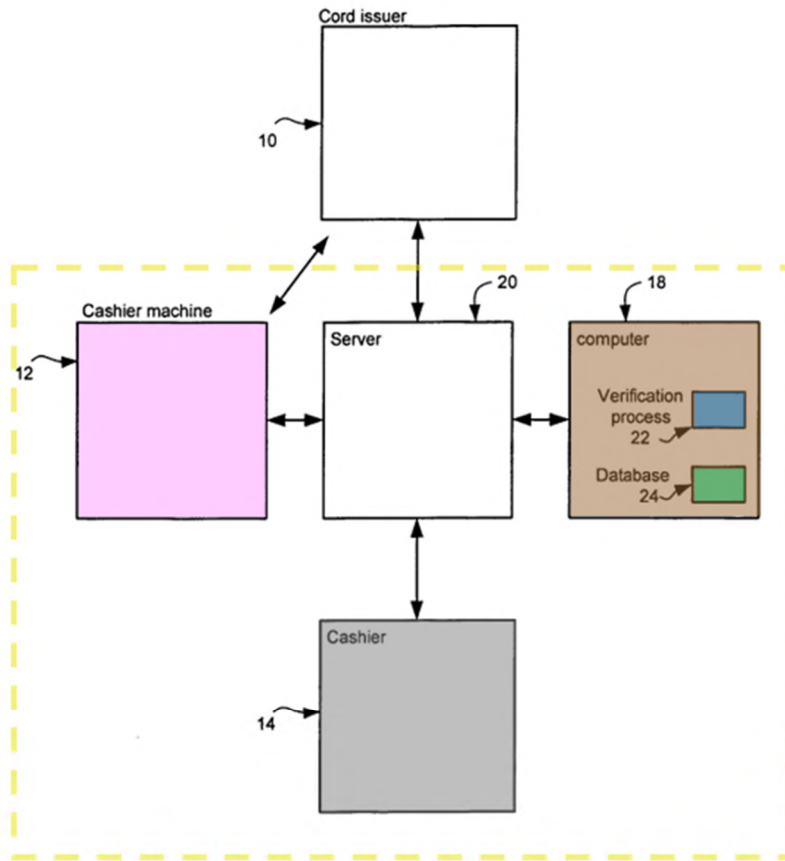


Fig. 1

Ex. 1004, Fig. 1. Therefore, in my opinion, 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.

289. 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. In my opinion, 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.

290. 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.**”).

291. 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.

292. Therefore, it is my opinion that 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.

293. It is also my opinion that 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.”

294. Therefore, it is my opinion that 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].”

295. **Limitation 3[D(P)+D(2)]**: In my opinion, Sanford discloses “(d) if the provided card information has not been previously provided to the verification station;... (db) performing the process dependent upon the received card information.”

296. 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.

297. 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.

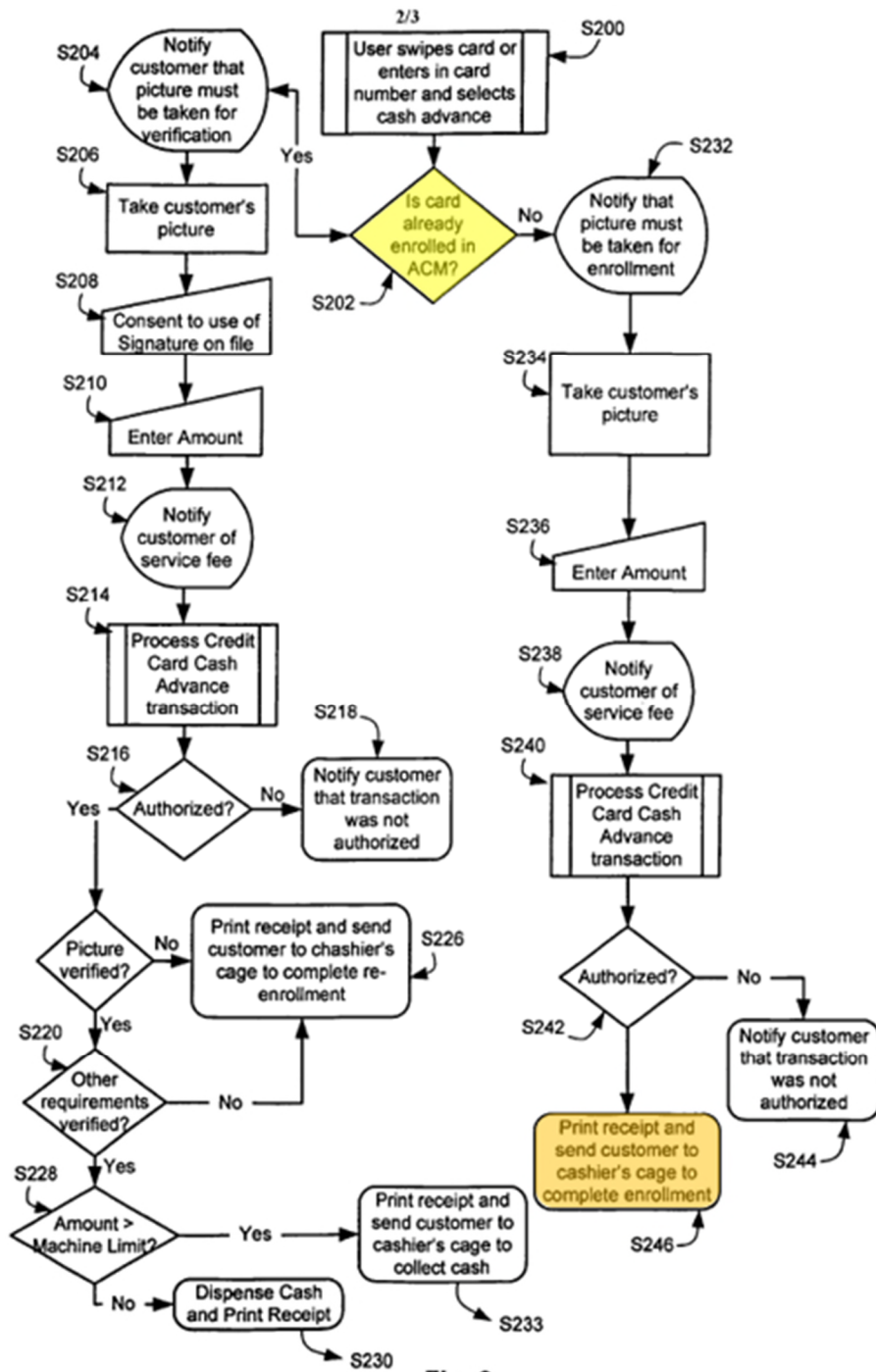


Fig. 2

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.

298. 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 in my opinion, 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.

299. Therefore, it is my opinion that 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].”

300. **Limitation 3[E(P)+E(1)]**: In my opinion, Sanford in view of Hsu discloses “(e) if the provided card information has been previously provided to the verification station; (ea) comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information.”

301. 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.

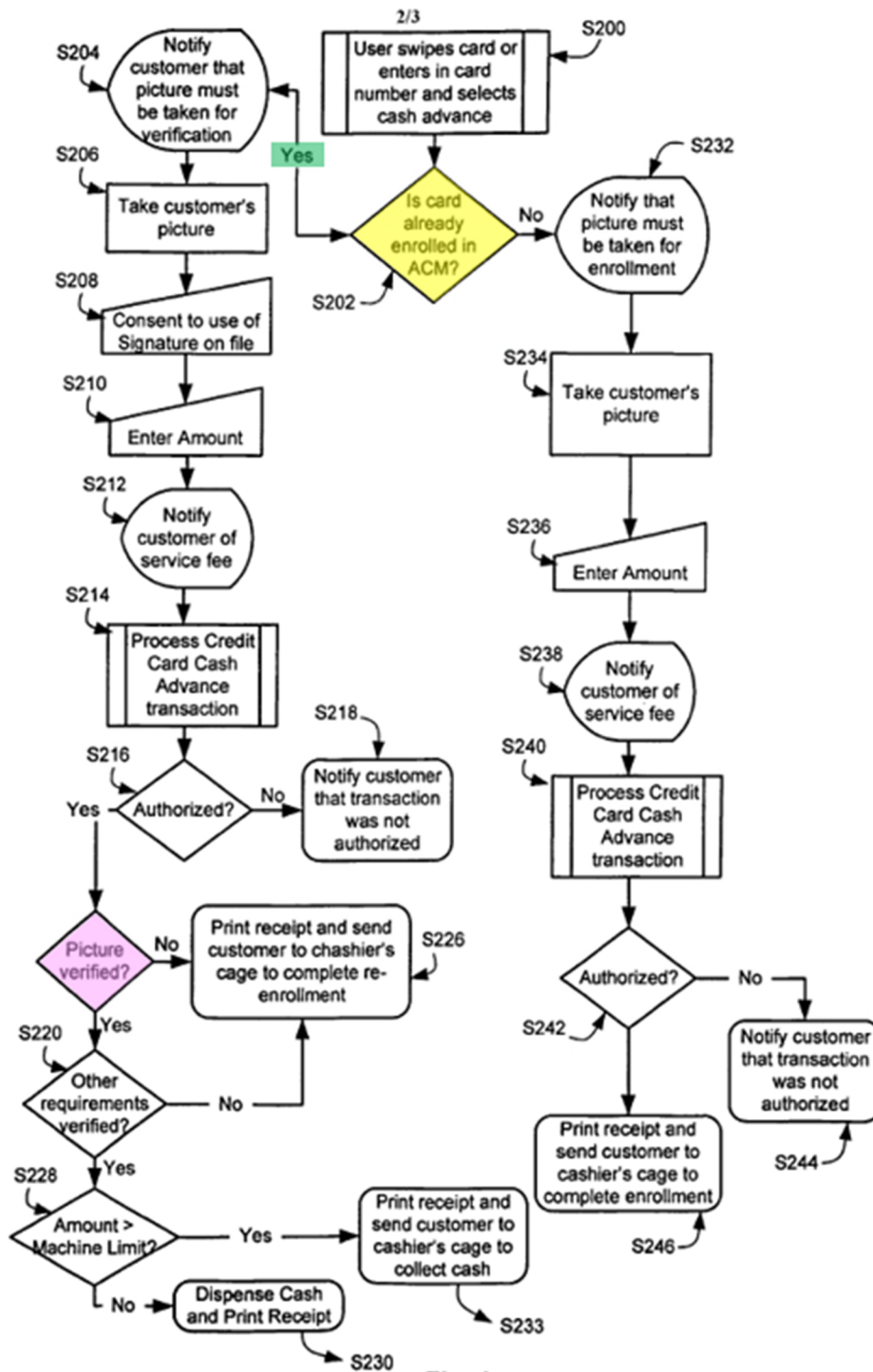


Fig. 2

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 I explained 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.

302. Therefore, it is my opinion that 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].”**

303. **Limitation 3[E(2)]**: In my opinion, Sanford discloses “(eb) if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information.”

304. 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.

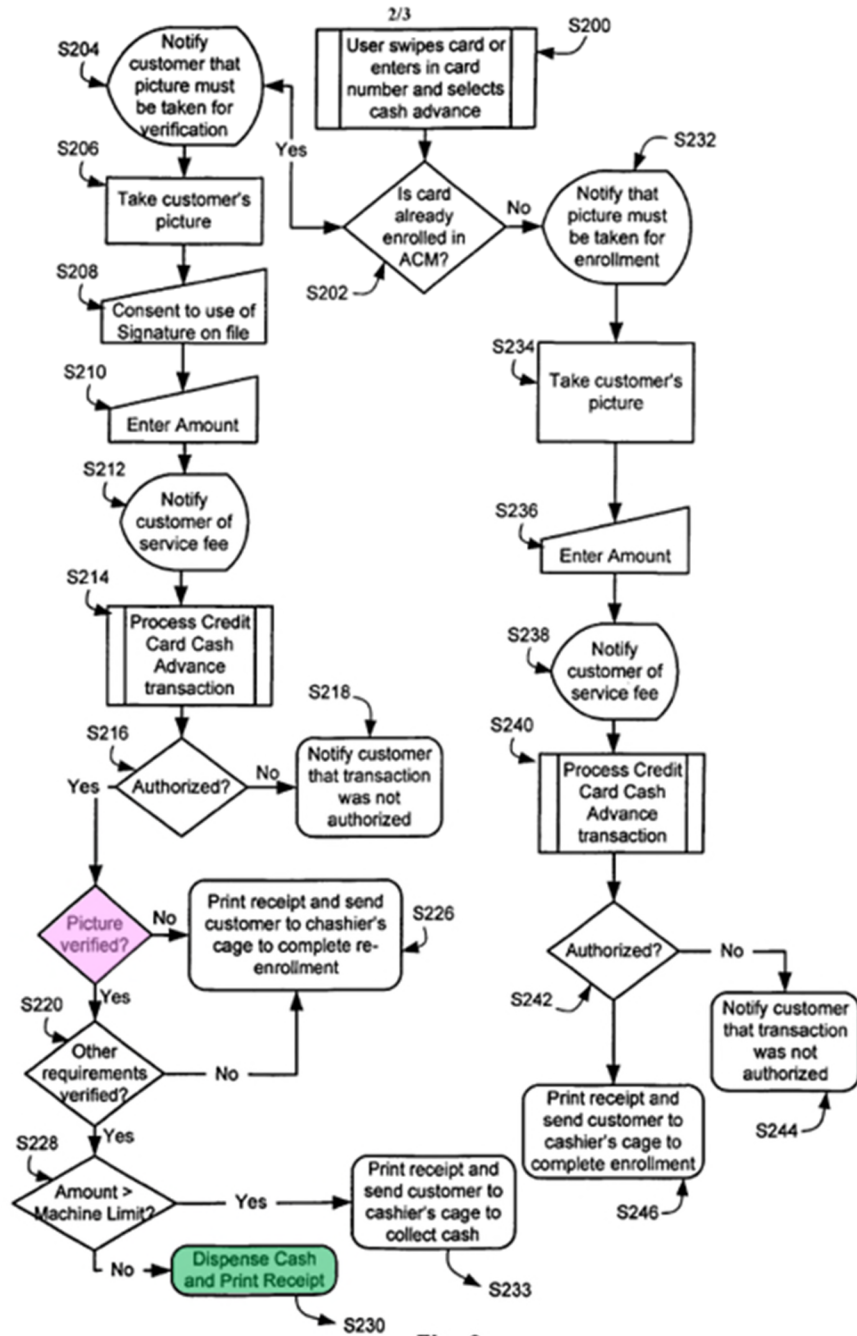


Fig. 2

Ex. 1004, Fig. 2. As I explained for Limitation 3[D(P)+D(2)], cash dispensing is a process dependent upon the received card information.

305. Therefore, it is my opinion that 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].”

306. **Limitation 3[E(3)]**: In my opinion, Sanford discloses “(ec) if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.”

307. 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.

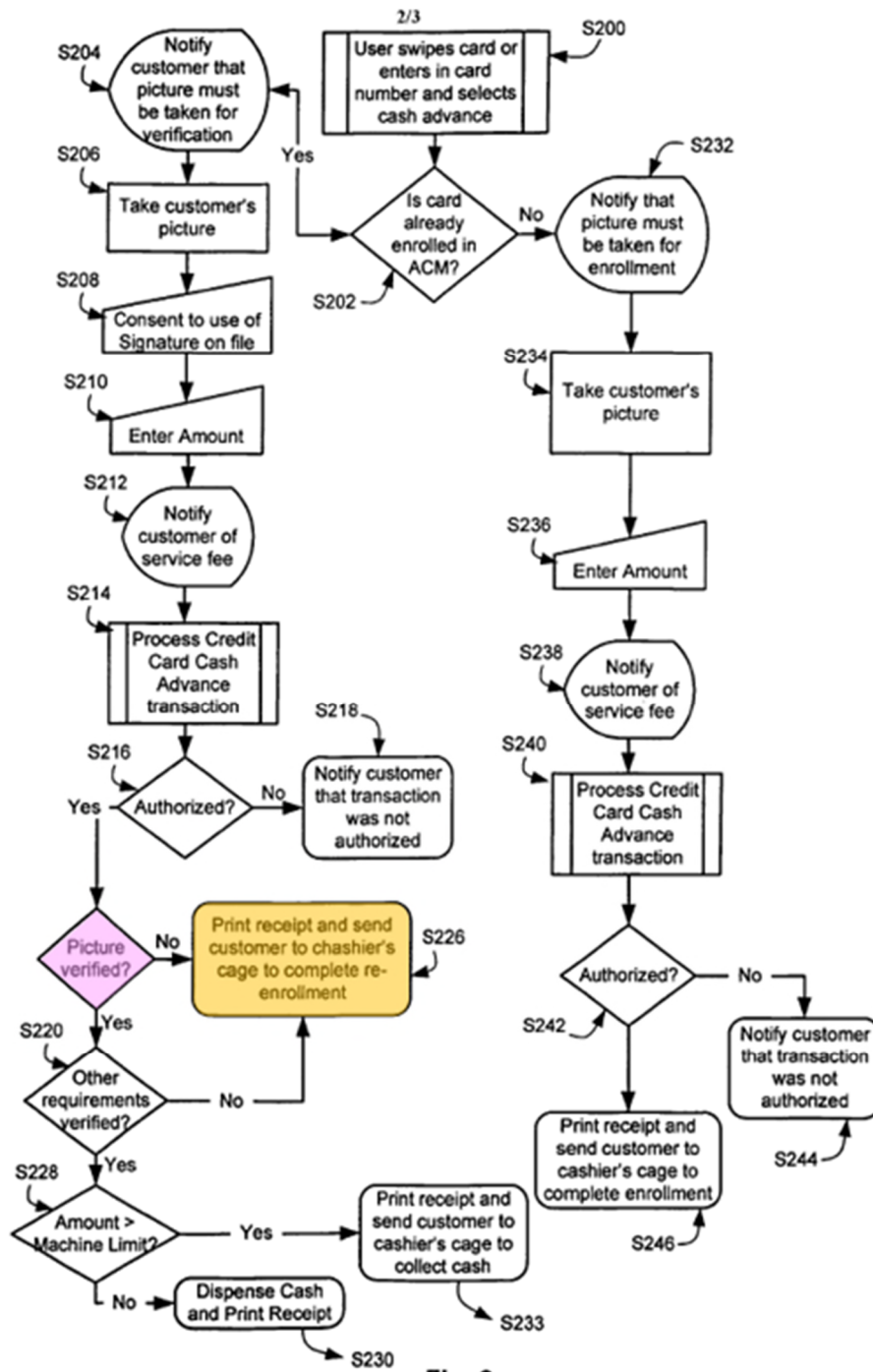


Fig. 2

Ex. 1004, Fig. 2. No cash dispensing process is executed. See Preamble 3[P]. As I explained for Limitation 3[D(2)], cash dispensing is a process dependent upon the received card information.

308. Therefore, it is my opinion that 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].**”

309. **Motivation to Combine Sanford and Hsu:** I noted that as explained above, 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 is my opinion that it would have been obvious to modify Sanford’s generic database to use Hsu’s database and memory structure.

310. In my opinion, 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.

311. In my opinion, 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.

312. In my opinion, a POSITA would have had a **reasonable expectation of success** in implementing Sanford's database according to Hsu's teachings. As I explained in motivation to combine for IPR2202-01093 Ground 2, 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.

313. Therefore, in my opinion, 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.

2. Claim 4 is rendered obvious by Sanford and Hsu

314. Claim 4 requires “[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.” In my opinion, this is rendered obvious by Sanford and Hsu.

315. I understand that since the preamble recites “one of,” only one of the portions [i] to [iv] needs to be disclosed.

316. In my opinion, Sanford discloses card information “encoded in a magnetic strip.” As I explained 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.

317. I noted that although not necessary to satisfy the claim, Hsu discloses each of [i], [ii], [iii] and [iv] of the claim. *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).

3. Claim 6 is rendered obvious by Sanford and Hsu

318. 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**.” In my opinion, this is disclosed by Sanford and Hsu.

319. 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, it is my opinion that Sanford discloses this claim.

320. *First*, it is my opinion that Sanford discloses that “the performance of the process in step[] (**db**)... comprises outputting at least part of the inputted card information from the verification station.”

321. As I explained 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].”

322. 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:

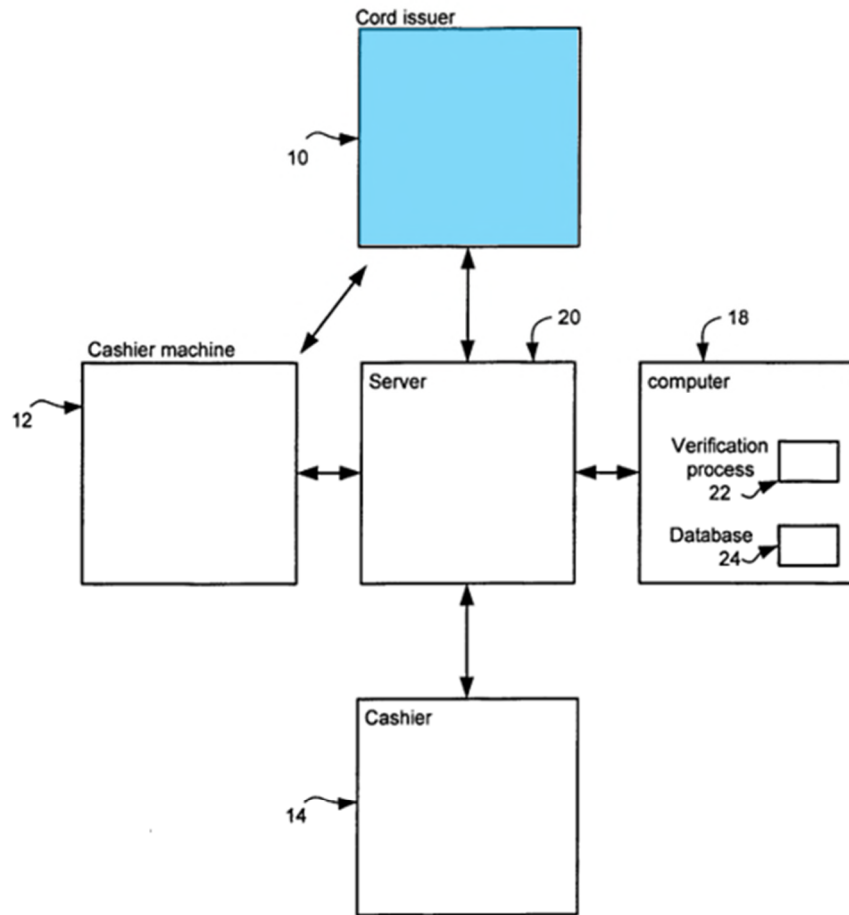


Fig. 1

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.” *Id.*, ¶0023; *see also* ¶0024 (“The PIN-less credit card transaction may be used to **withdraw cash** ... credit **from an institution** ... from ACM 12.”). I noted that “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.”).

323. In addition, Sanford discloses in Figure 2 that if it is determined at step S202 (yellow) that a card is **not** enrolled, “[i]n step S240 [purple], **the transaction is sent** for pre-authorization **to the financial institution...**, which may use an Address Verification System (AVS) to help validate the users address.” Ex. 1004, ¶0034.

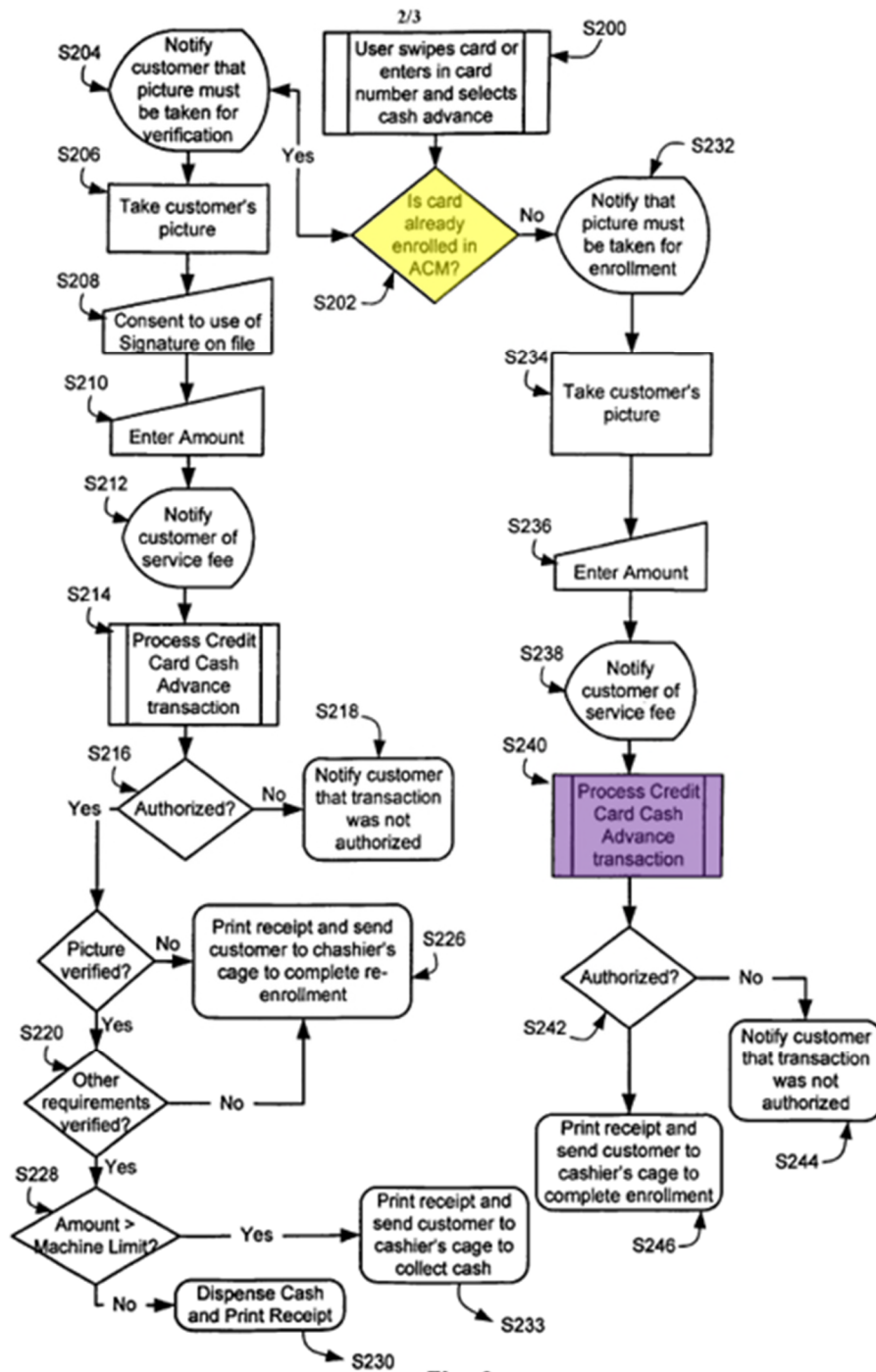


Fig. 2

Ex. 1004, Fig. 2. It is my opinion that a POSITA would have expected that the “transaction” that is sent to the “financial institution” would include the credit card account number.

324. Therefore, in my opinion, 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). 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.

325. Therefore, it is my opinion that 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]."

326. *Second*, it is my opinion that Sanford discloses "the performance of the process in the step[]... **(eb)** comprises outputting at least part of the inputted card information from the verification station."

327. As I explained 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]."

328. As explained above, 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.

329. Therefore, it is my opinion that 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].”

4. Claim 7 is rendered obvious by Sanford and Hsu

330. 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.” In my opinion, this is disclosed by Sanford and Hsu.

331. My understanding is that 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].” In my opinion, Sanford discloses that step (db) comprises both steps [i] and [ii].

332. 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.

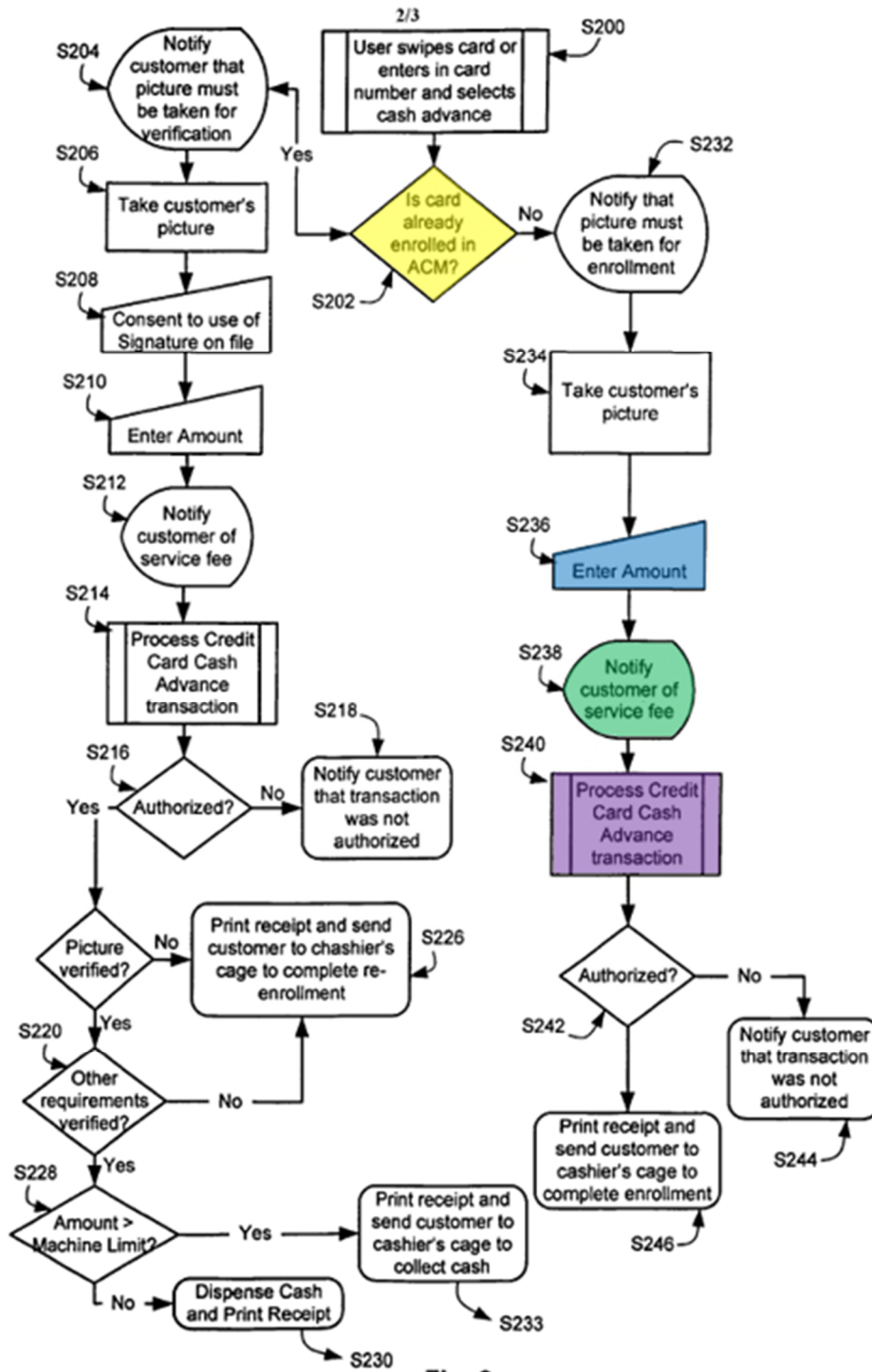


Fig. 2

Ex. 1004, Fig. 2. In my opinion, a POSITA would have understood that the “withdrawal amount” is entered by using Sanford’s input device (*e.g.*, keypad).

333. 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. In my opinion, 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, in my opinion, 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.

334. Therefore, it is my opinion that 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.

5. Claim 8 is rendered obvious by Sanford and Hsu

335. 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.” In my opinion, this is disclosed by Sanford and Hsu.

336. The claim recites “one of,” and therefore only portion [i] or portion [ii] need be disclosed. In my opinion, Sanford discloses both.

337. 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, it is my opinion that Sanford discloses that the “withdrawal amount” (outputted information) is sent to the financial institution for pre-authorization. In my opinion, 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.

338. Therefore, it is my opinion that Sanford discloses that “the information outputted [*e.g.*, withdrawal amount] is communicated to... [i] a service provider [*e.g.*, financial institution 16] for providing a service [*e.g.*, credit or cash withdrawal] dependent upon receipt of the outputted information [*e.g.*, withdrawal amount].”

339. 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. In my opinion, 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 also have understood that the cashier system 14 is an apparatus for providing access to cash dependent upon the withdrawal amount provided by the user.

340. Therefore, it is also my opinion that 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].”

6. Claim 9 is rendered obvious by Sanford and Hsu

341. 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.” In my opinion, this is disclosed by Sanford and Hsu.

342. I noted that 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, it is my opinion that Sanford discloses claim 9.

343. 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.

344. As discussed for claim 6, when it is determined that the user’s card is not enrolled, the user’s “credit card account number” is sent to financial institution 16 for pre-authorization. Ex. 1004, ¶0034; Fig. 2. The user’s “credit card account

number” is also sent to financial institution 16 for cash dispensing. Thus, in my opinion, a POSITA would have understood that financial institution 16 is a service provider for providing pre-authorization and cash dispensing services dependent upon the received credit card account information. Therefore, when claim 9 depends from claim 6, Sanford discloses “the information outputted is communicated to... [i] a service provider [financial institution 16] for providing a service [credit or cash withdrawal] dependent upon receipt of the outputted information [card account number].” *See* claim 6 discussion.

7. Claim 10 is rendered obvious by Sanford and Hsu

345. 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 authorized [*sic*] authorized.” In my opinion, this is disclosed by Sanford and Hsu.

346. As I 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].”

347. It is my opinion that 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.

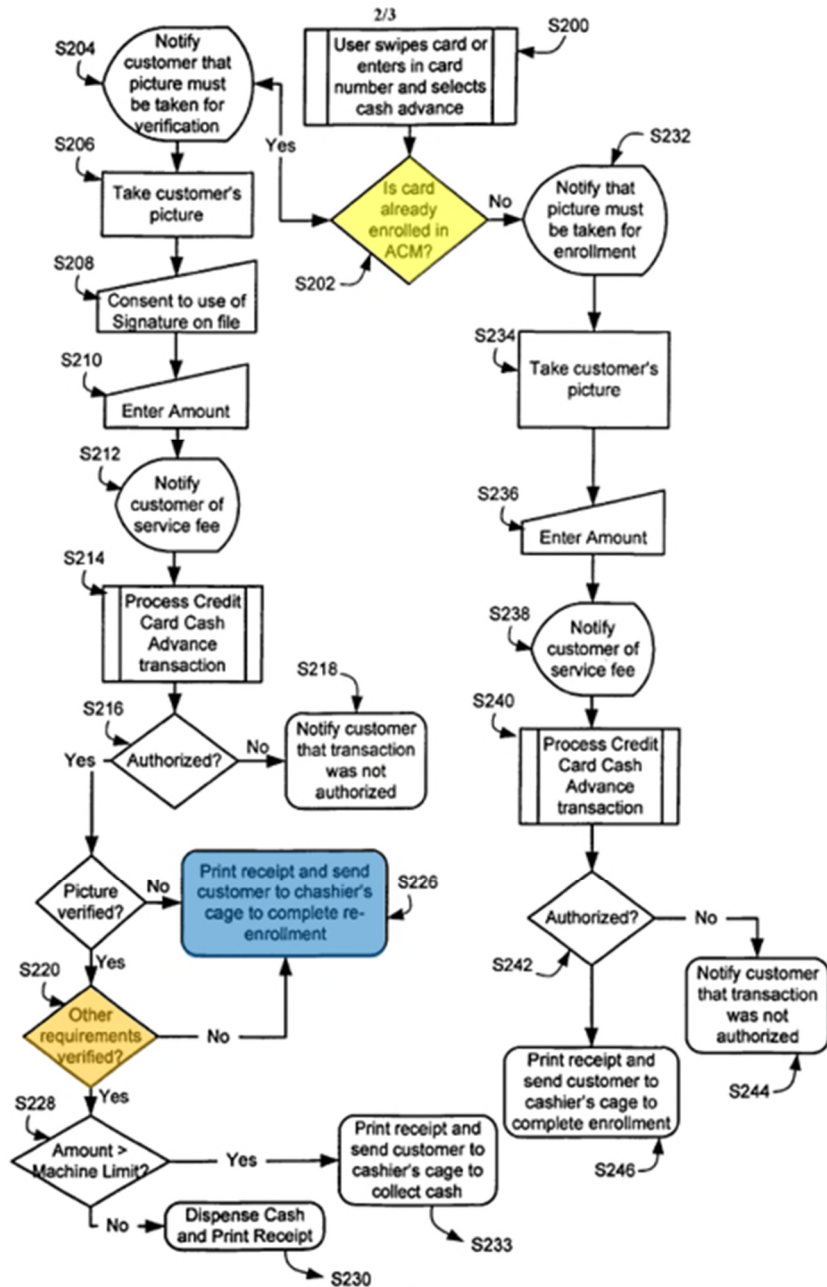


Fig. 2

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.

8. Claim 11 is rendered obvious by Sanford and Hsu

348. Claim 11 requires “[a] method according to claim 10, 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.” In my opinion, this is disclosed by Sanford and Hsu.

349. The preamble recites “one of,” and therefore only the first portion [i] or the second portion [ii] need be disclosed. It is my opinion that Sanford discloses both.

350. As I explained 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, in my opinion, 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.

351. Therefore, Sanford in view of Hsu discloses or renders obvious that “[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.”

9. Claim 15 is rendered obvious by Sanford and Hsu

352. In my opinion, claim 15 is unpatentable because it is rendered obvious by Sanford and Hsu. Claim 15 of the ’039 Patent recites the following. I address each of these in my analysis below.

[P] A verification station for securing a process, the verification station comprising:

[A] a card device reader for receiving card information from a card device coupled to the verification station;

[B] a biometric signature reader for receiving a biometric signature provided to the verification station;

[C] means for determining if the provided card information has been previously provided to the verification station;

[D(P)] means, if the provided card information has not been previously provided to the verification station, for:

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

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

[E(P)] means, if the provided card information has been previously provided to the verification station, for:

[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;

[E(2)] if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

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

353. **Preamble 15[P]**: As I explained for Limitation 3[P], it is my opinion that Sanford discloses “[a] **verification station for securing a process**, [Stanford’s verification station comprising] **the verification station comprising.**” *See* Limitation 3[P].

354. **Limitation 15[A]**: As I explained for Limitation 3[A], it is my opinion that Sanford discloses “**a card device reader for receiving card information from a card device coupled to the verification station.**” *See* Limitation 3[A].

355. 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). I also noted that because the card reader is part of its ACM, when Sanford’s card is **coupled to** the card reader, it is also **coupled to** the ACM.

356. **Limitation 15[B]**: In my opinion, Sanford discloses “**a biometric signature reader for receiving a biometric signature provided to the verification station.**”

357. As I 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].” Therefore,

Sanford discloses that a biometric signature is **provided to** a biometric signature reader. Because the biometric signature reader is **part of** Sanford's ACM (Ex. 1004, ¶0016), when the biometric signature is **provided to** the biometric signature reader, it is also **provided to** Sanford's ACM.

358. **Limitation 15[C]**: In my opinion, Sanford discloses “*means for determining if the provided card information has been previously provided to the verification station.*”

359. I understand that 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.

360. In my opinion, Sanford discloses this construed limitation.

361. *First*, as I explained for Limitation 3[C], Sanford discloses the recited **function**.

362. *Second*, it is my opinion that 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.

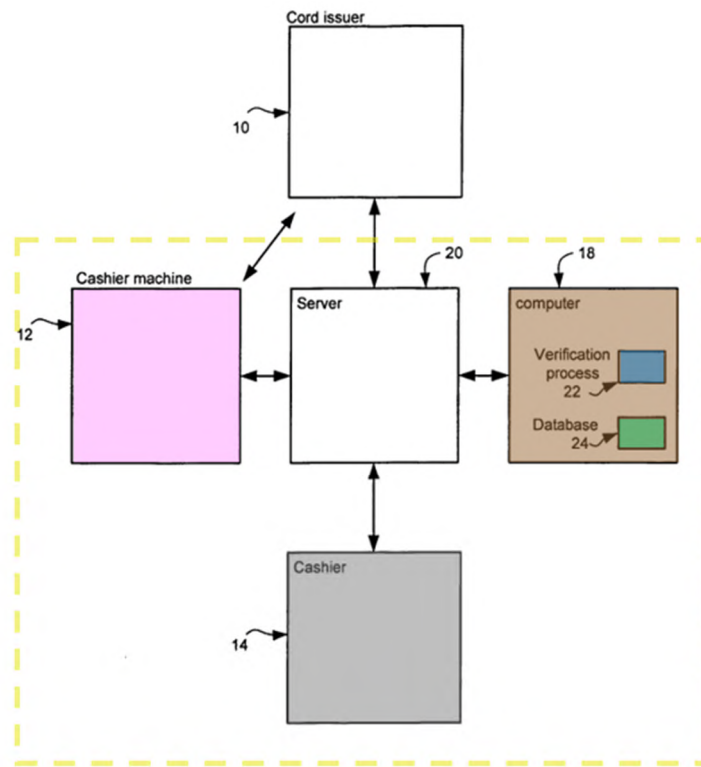


Fig. 1

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.

363. **Limitation 15[D(P)+D(1)]**: In my opinion, Sanford in view of Hsu discloses “*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.*”

364. I understand that 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.

365. In my opinion, Sanford discloses this construed limitation.

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

367. *Second*, it is my opinion that 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. In my opinion, 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.

368. **Limitation 15[D(P)+D(2)]**: In my opinion, Sanford discloses "*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.*"

369. I understand that 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.

370. In my opinion, Sanford discloses this construed limitation.

371. *First*, for the same reasons I explained for Limitations 3[D(P)+D(2)], Sanford discloses the recited **function**.

372. *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 I 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.

373. **Limitation 15[E(P)+E(1)]**: In my opinion, Sanford in view of Hsu discloses “*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.*”

374. I understand that 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.

375. In my opinion, Sanford discloses this construed limitation.

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

377. *Second*, it is my opinion that 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. In my opinion, 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.

378. 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. *Id.* I note that 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.

379. **Limitation 15[E(2)]**: In my opinion, Sanford discloses “[*means... for:*] if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information.”

380. I understand that 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.

381. As I explained for Limitation 3[E(2)], Sanford discloses the **function**. As I explained for Limitation 15[D(2)], Sanford also discloses the same or equivalent **structure**.

382. **Limitation 15[E(3)]**: In my opinion, Sanford discloses “[*means... for:*] if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.”

383. I understand that 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.

384. As I explained for Limitation 3[E(3)], Sanford discloses the **function**. As I explained for Limitation 15[D(2)], Sanford also discloses the same or equivalent **structure**. Such structure performs the recited function because it does not dispense money if the user verification process fails, as I explained for Limitation 3[E(3)].

10. Claim 16 is rendered obvious by Sanford and Hsu

385. 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 fob** adapted to provide the card information by transmitting a wireless signal to the verification station.” In my opinion, this is rendered obvious by Sanford and Hsu.

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

387. 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. I noted that although not necessary to disclose the claim, Hsu discloses and renders obvious each of [i] through [iv]. *See* discussion at claim 4, incorporated here.

11. Claim 18 is rendered obvious by Sanford and Hsu

388. I noted that 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 VI.B). Thus, for the same reasons that I discussed for claim 15, Sanford and Hsu disclose or render obvious claim 18, as summarized below:

Claim 18 Limitation	Description	Claim 15 Limitation
18[P]	“a method for securing a process”	15[P]
18[A]	“code for determining”	15[C]
18[B(P)]	“if the provided card information	15[D(P)]

	has not been previously provided”	
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)]

389. I note that claim 18 also recites “non-transitory computer readable medium” in its preamble. In order for the various components of Sanford and Hsu to perform their functions, a POSITA would have understood and found it obvious that both Sanford and Hsu (and the combined system) include one or more processors running computer programs stored on a non-transitory computer readable medium.

D. IPR2022-001094 GROUND #2: Claims 3, 4, 6-11, 15, 16, and 18 are Rendered Obvious by Sanford, Hsu, and Tsukamura

1. Claim 3 is rendered obvious by Sanford, Hsu, and Tsukamura

390. As I explained in IPR2022-001094 Ground 1, incorporated here, Sanford in view of Hsu discloses claim 1 under the First Construction. *See* Section VI.A.1 and discussion for Limitations 3[D(1)] and 3[E(1)].

391. If this limitation means “a memory location is specified by the card information” (Second Construction), it is my opinion that Sanford in view of Hsu and Tsukamura renders obvious claim 3.

392. **Limitation 3[D(P)+D(1)]**: In my opinion, Sanford in view of Hsu and Tsukamura discloses “(d) if the provided card information has not been previously provided to the verification station; (da) storing the inputted biometric signature in a memory at a memory location defined by the provided card information.”

393. It is my opinion that 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.

394. Tsukamura discloses a simple and efficient structure for “stored...fingerprint data” in Figure 3. Ex. 1005, 2:9-10.

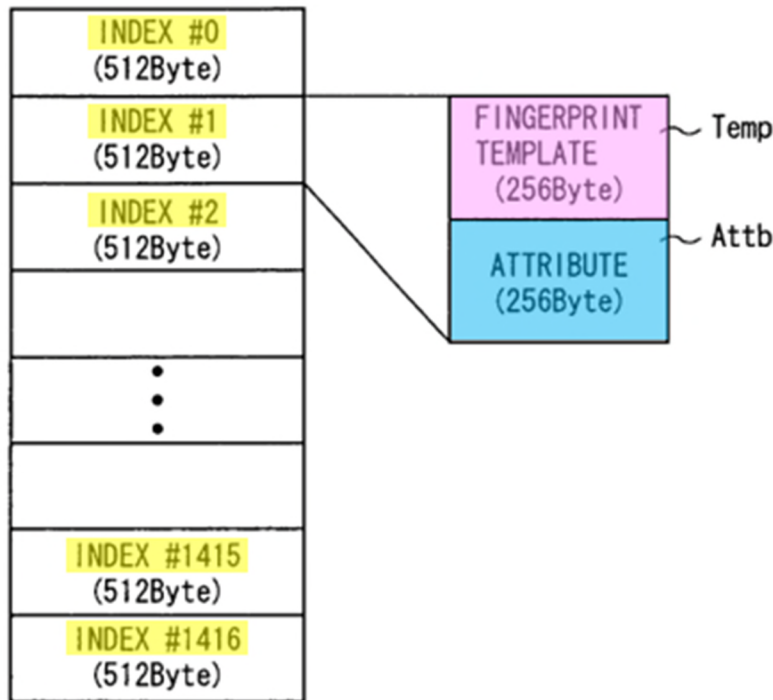


FIG. 3

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. In my opinion, if the Tsukamura implementation were used for Sanford-Hsu database, each user/account number would specify a different entry (index number) in the database.

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

396. Therefore, it is my opinion that 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]."

397. **Limitation 3[E(P)+E(1)]**: In my opinion, 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 I explained for Limitation 3[D(P)+D(1)] (Ground 1) and the additional reasons I explained for Limitation 3[D(P)+D(1)] (Ground 2).

398. **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. As I explained for motivation to combine Hsu, Sanford, and Tsukamura at the end of Section X.B.1, this was well-known before the '039 Patent.

399. 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.

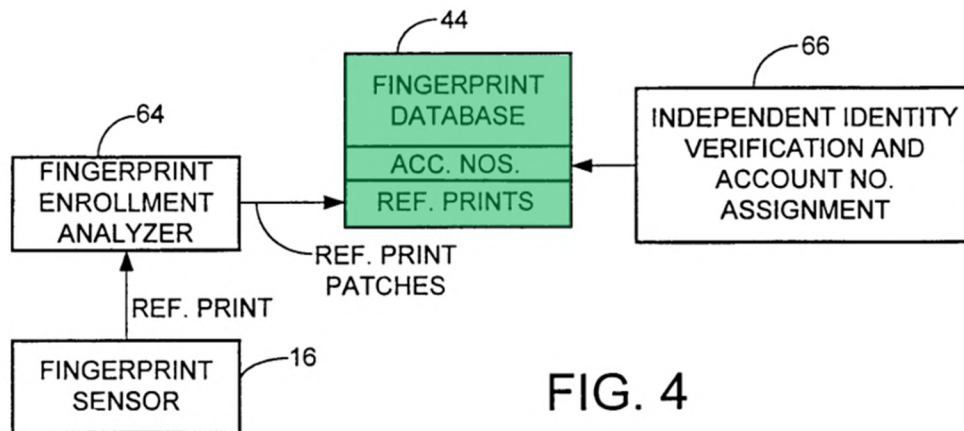


FIG. 4

Ex. 1003, Fig. 4. As I explained for motivation to combine Hsu, Sanford, and Tsukamura at the end of Section X.B.1, 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. 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.

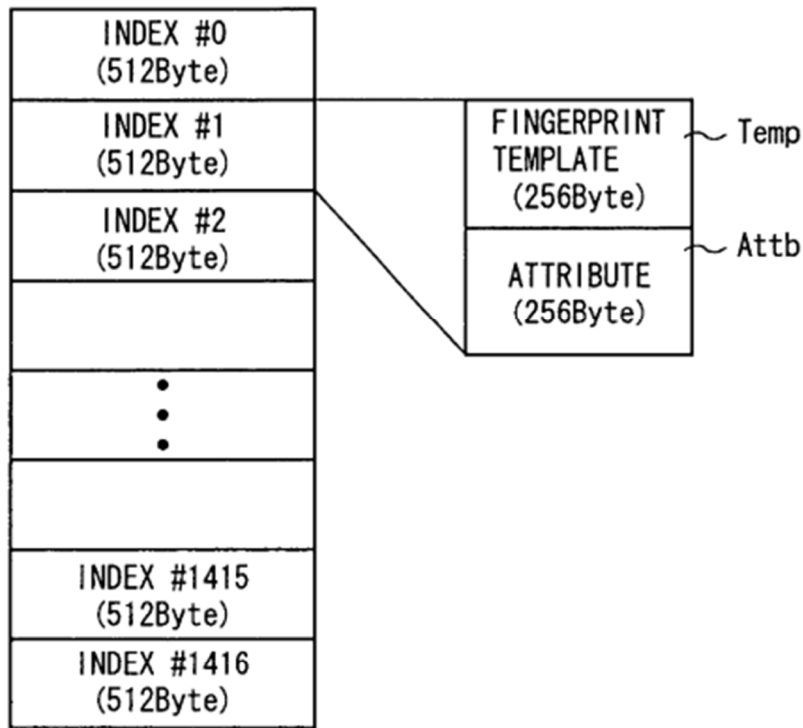


FIG. 3

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.*

400. 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.”).

401. As I explained in Section X.A.1, a POSITA would have understood that “collate” here means “compare” or “verify.”

402. 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. In my opinion, 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.

403. The Sanford-Hsu system specifically aims for speed: “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. In my opinion, 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 corresponding index numbers. Ex. 1005, Fig. 4.

404. Further, when assigning a credit card account number in the Sanford-Hsu-Tsukamura system, it is my opinion that 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, in my opinion, 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.

405. It is my opinion that 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, in my opinion, 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.

2. Claims 4 and 6-11 are rendered obvious by Sanford, Hsu, and Tsukamura

406. As I explained in Ground 1, incorporated herein, Sanford in view of Hsu discloses claims 4 and 6-11. For the same reasons, it is my opinion that Sanford in view of Hsu and Tsukamura also discloses these claims.

3. Claim 15 is rendered obvious by Sanford, Hsu, and Tsukamura

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

408. If the term means “a memory location is specified by the card information” (Second Construction), it is my opinion that Sanford in view of Hsu and Tsukamura discloses claim 15.

409. **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, in my opinion, is disclosed by Sanford, Hsu, and Tsukamura.

410. *First*, for the same reasons I explained for Limitation 3[D(P)+D(1)] (Ground 2), the Sanford-Hsu-Tsukamura system discloses the recited **function**.

411. *Second*, it is my opinion that the Sanford-Hsu-Tsukamura system discloses the same or equivalent **structure**. In addition to the reasons I 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. In my opinion, a POSITA would have understood that RAM stands for Random Access Memory and is a type of memory. Therefore, it is my opinion that a POSITA would have understood that the Sanford-Hsu-Tsukamura system performs the storing function using a processor and memory.

412. **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, in my opinion, is disclosed by Sanford, Hsu, and Tsukamura.

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

414. *Second*, it is my opinion that the Sanford-Hsu-Tsukamura system discloses the same or equivalent **structure**. In addition to the reasons I 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).

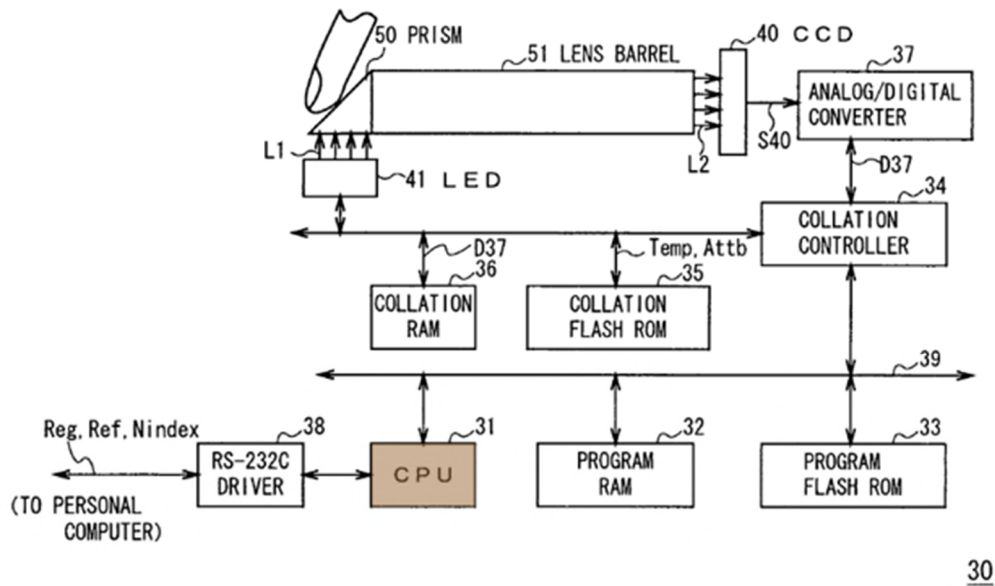


FIG. 2

Ex. 1005, Fig. 2. Because CPU 31 in Tsukamura “control[s] the whole of the fingerprint collating unit 30” (Ex. 1005, 2:50-53), in my opinion, 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.

4. Claim 16 is rendered obvious by Sanford, Hsu, and Tsukamura

415. For the same reasons as in Ground 1, it is my opinion that Sanford in view of Hsu and Tsukamura discloses this claim.

5. Claim 18 is rendered obvious by Sanford, Hsu, and Tsukamura

416. For the same reasons as in Ground 1, it is my opinion that Sanford in view of Hsu and Tsukamura discloses claim 18.

“**control program**” includes the “**code for**” fingerprint verification. Ex. 1005, Abstract, 2:50-53.

E. IPR2022-001094 GROUNDS #3 and #4: Claim 5 is rendered obvious

418. My discussion below explains that the limitations of claim 5 are rendered obvious by Leu.

419. Ground 3 incorporates the below analysis in the context of the Sanford-Hsu system (Ground 1) in view of Leu. I incorporate Ground 1 here.

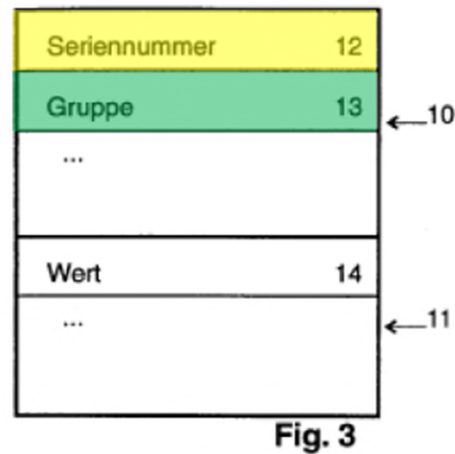
420. Ground 4 incorporates the below analysis in the context of the Sanford-Hsu-Tsukamura system (Ground 2) in view of Leu. I incorporate Ground 2 here.

421. 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.”

422. In my opinion, 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. Thus, Leu’s card reader device is a verification station. I noted

that Ex. 1009 is an English translation of Ex. 1008 (Leu). Citations to Leu are made to Ex. 1009.

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

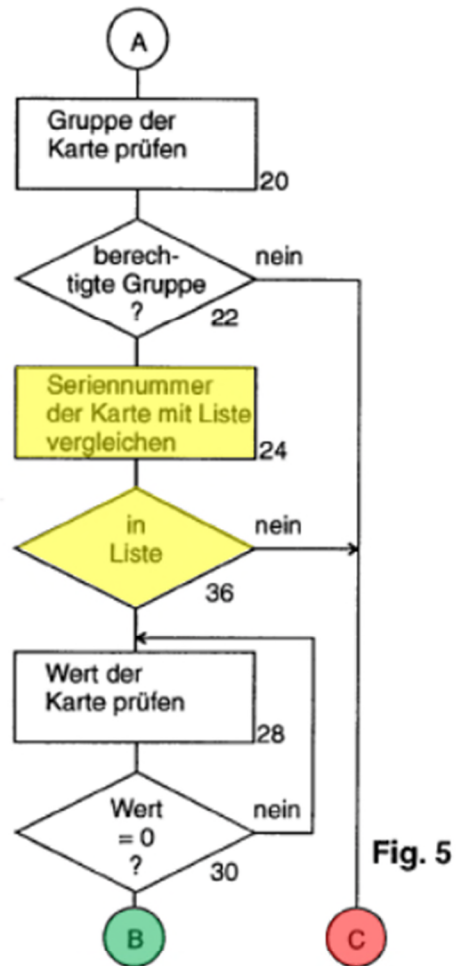


[Fig. 3 Translation Key:]
12 = serial number
13 = group
14 = value

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. In my opinion, 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.

424. It is my opinion that 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.

425. 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 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

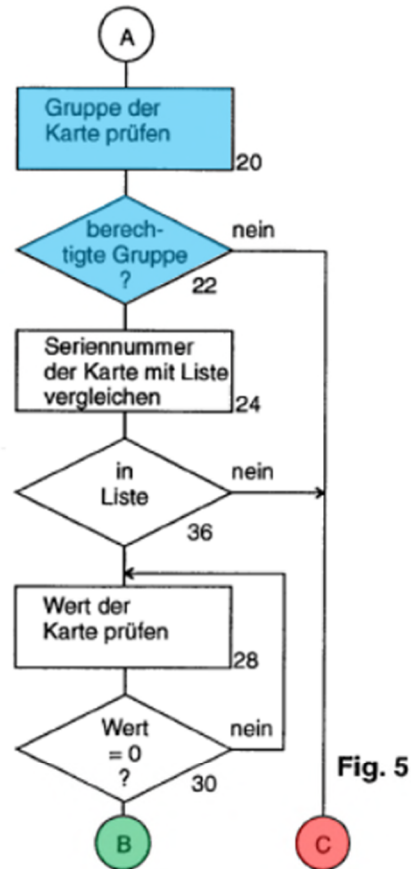
28 = check the value of the card

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 is able to interpret the serial number and determine whether the card belongs to a

subset of cards, it is my opinion that a POSITA would have understood the subset of cards is associated with the card reader (verification station).

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



[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. In my opinion, 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).

427. As would have been common knowledge to a POSITA, it was well-known to use header-data when transmitting information. 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, it is my opinion that 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.



Fig. 3

[Fig. 3 Translation Key:]

12 = serial number

13 = group

14 = value

Ex. 1009, Fig. 3.

428. In my opinion, it would have been obvious to transmit card information in the Sanford-Hsu system in a header-data format such as disclosed by Leu.

429. 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.

430. In my opinion, 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.”). In my opinion, 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.

431. 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”). In my opinion, 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.

432. Further, it is my opinion that a POSITA would also have 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.

F. IPR2022-001094 GROUNDS #5 and #6: Claim 12 is rendered obvious

433. My discussion below explains that the limitations of claim 12 are rendered obvious by Houvener.

434. Ground 5 incorporates the below analysis in the context of the Sanford-Hsu system (Ground 1) in view of Houvener. I incorporate Ground 1 here.

435. Ground 6 incorporates the below analysis in the context of the Sanford-Hsu-Tsukamura system (Ground 2) in view of Houvener. I incorporate Ground 2 here.

436. 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.”

437. 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.

438. Therefore, it is my opinion that a POSITA would have understood that Houvener discloses storing success transaction records to “monitor transaction patterns” and output these records for audit purposes (*e.g.*, fraud detection). 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.”

439. In my opinion, it would have been obvious to implement Houvener’s audit trail and fraud detection in the Sanford-Hsu (or Sanford-Hsu-Tsukamura) system.

440. 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.

441. It is my opinion that a POSITA implementing the Sanford-Hsu system would have been **motivated** to look to Houvener. In my opinion, 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), it is my opinion that 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). In my opinion, a POSITA would have

looked to teachings of Houvener to make use of the “history” data disclosed by Hsu.

442. Similarly, Sanford also aims to “reduce[] fraudulent use of credit cards” by “having an identifying image captured.” Ex. 1004, ¶0043. In my opinion, 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.

443. In my opinion, 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.

444. Further, Hsu already discloses storing “history” data in the database. Therefore, in my opinion, 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.

445. When combining Houvener with the Sanford-Hsu (or Sanford-Hsu-Tsukamura) system, it is my opinion that 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.

G. IPR2022-001094 GROUNDS #7 and #8: Claim 17 is rendered obvious

446. My discussion below explains that the limitations of claim 17 are rendered obvious by McCalley.

447. Ground 7 incorporates the below analysis in the context of the Sanford-Hsu system (Ground 1) in view of McCalley. I incorporate Ground 1 here.

448. Ground 8 incorporates the below analysis in the context of the Sanford-Hsu-Tsukamura system (Ground 2) in view of McCalley. I incorporate Ground 2 here.

449. Claim 17 requires a "**memory** [that] is incorporated in a **tamper-proof** manner in the verification station."

450. 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.

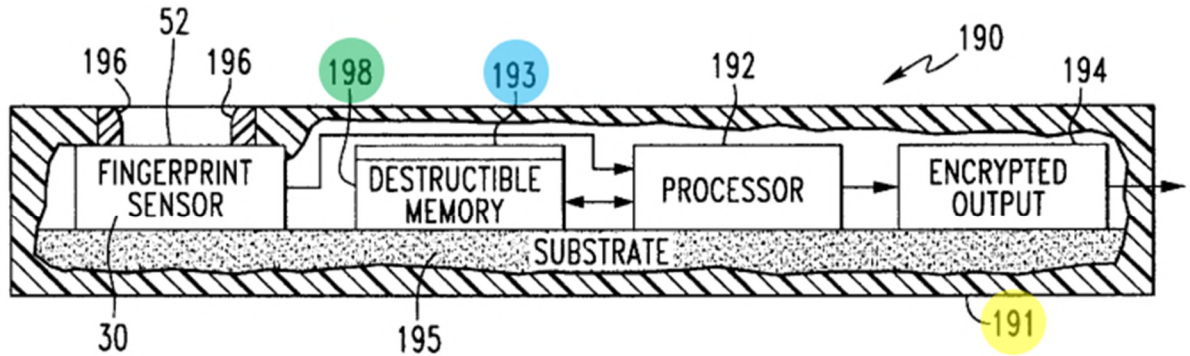


FIG. 22

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.”).

451. Accordingly, McCalley discloses a memory that is incorporated in a tamper-proof manner by keeping memories in a tamper-resistant housing (tamper-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. 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.

452. In my opinion, 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.

453. 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.

454. It is my opinion that 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. In my opinion, 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. It is my opinion that 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.

455. In my opinion, 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.

XI. CONCLUDING STATEMENTS

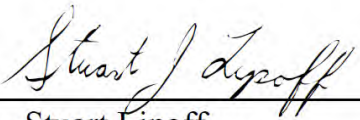
456. In my opinion, the challenged claims 1, 2, 13, 14, 19, and 20 are rendered obvious by the Hsu-Sanford combination or the Hsu-Sanford-Tsukamura combination. As such, in my opinion, these claims should be found unpatentable and cancelled.

457. In my opinion, the challenged claims 3, 4, 6-11, 15, 16, and 18 are rendered obvious by the Sanford-Hsu combination or the Sanford-Hsu-Tsukamura combination. As such, in my opinion, these claims should be found unpatentable and cancelled.

458. In my opinion, claims 5, 12, and 17 are obvious in view of at least the references discussed above. As such, in my opinion, these claims should be found unpatentable and cancelled.

459. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the results of these proceedings.

Executed on June 13, 2022 in Las Vegas, Nevada.



Stuart Lipoff