

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Francisco Martinez de Velasco Cortina et al.
U.S. Patent No.: 10,235,513 Attorney Docket No.: 50095-0312IP1
Issue Date: March 19, 2019
Appl. Serial No.: 15/372,317
Filing Date: December 7, 2016
Title: SYSTEM AND METHOD FOR PROVIDING SECURE
IDENTIFICATION SOLUTIONS

Mail Stop Patent Board

Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR *INTER PARTES* REVIEW
OF UNITED STATES PATENT NO. 10,235,513
PURSUANT TO 35 U.S.C. §§311–319, 37 C.F.R. §42

TABLE OF CONTENTS

I.	REQUIREMENTS FOR IPR	1
A.	Grounds for Standing.....	1
B.	Challenge and Relief Requested.....	1
II.	THE '513 PATENT OVERVIEW	2
III.	LEVEL OF ORDINARY SKILL	4
IV.	CLAIM CONSTRUCTION	4
V.	THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	5
A.	GROUND 1A AND 2A.....	5
1.	Wang.....	5
2.	Barnes.....	7
3.	Srey.....	9
4.	The Prior Art References Are Analogous Art.....	10
5.	Combination of Wang and Barnes	12
6.	Combination of Wang and Srey	16
7.	Claim Element Analysis.....	19
B.	GROUND 1B AND 2B	58
1.	Bashan	58
2.	Bashan Combined with Wang-Barnes or Wang-Srey.....	58
3.	Claim Element Analysis.....	61
C.	GROUND 3A.....	61
1.	The '513 Patent's Priority Date is its Filing Date.....	61
2.	Mardikar	62
3.	Cooke.....	63
4.	Combination of Mardikar and Cooke	64
5.	Claim Element Analysis.....	67
D.	GROUND 3B.....	84
1.	Lee	84
2.	Lee Combined with Mardikar and Cooke.....	85
3.	Claim Element Analysis.....	86
VI.	CONCLUSION AND FEES	86
VII.	MANDATORY NOTICES	86
A.	Real Party-In-Interest.....	86
B.	Related Matters	86
C.	Lead And Back-Up Counsel.....	86
D.	Service Information	87

LIST OF EXHIBITS

EX1001	U.S. Patent No. 10,235,513 (“the ’513 patent”)
EX1002	Excerpts from the Prosecution History of the ’513 Patent (“the ’513 Prosecution History”)
EX1003	Declaration of Dr. Seth Nielson
EX1004	PCT Publication No. WO 00/52866 (“Wang”)
EX1005	U.S. Patent No. US 8,611,919 (“Barnes”)
EX1006	U.S. Patent No. 6,141,436 (“Srey”)
EX1007	U.S. Patent No. 6,045,043 (“Bashan”)
EX1008	RESERVED
EX1009	U.S. Patent No. 8,108,318 (“Mardikar”)
EX1010	U.S. Patent Pub. No. 2014/0025513 (“Cooke”)
EX1011	U.S. Patent No. 8,761,665 (“Lee”)
EX1012	U.S. Patent No. 5,144,649 (“Zicker”)
EX1013	U.S. Patent Pub. No. 2002/0003892 (“Iwanaga”)
EX1014	U.S. Patent No. 6,327,376 (“Harkin”)
EX1015	Wikipedia Page for IrDA Communications, https://en.wikipedia.org/wiki/IrDA , Last accessed 9/5/16
EX1016	U.S. Patent No. 5,698,836 (“Fujioka”)

EX1017	U.S. Patent Pub. No. 20010056410 (“Ishigaki”)
EX1018 – 1029	RESERVED
EX1030	Complaint for Patent Infringement, <i>Mobility IP Holdings, Inc. v. Apple Inc.</i> , No. 7:26-cv-00075 (W.D. Tex. Mar. 4, 2026)
EX1031	Complaint for Patent Infringement, <i>Mobility IP Holdings, Inc. v. Samsung Electronics Co, Ltd. and Samsung Electronics America, Inc.</i> , No. 2:26-cv-157 (E.D. Tex. Feb. 27, 2026)
EX1032	Stipulation by Apple
EX1033	Stipulation by Samsung
EX1034	Combined Civil and Criminal Federal Court Management Statistics (Jun. 30, 2026) United States Courts, available at: https://www.uscourts.gov/sites/default/files/document/fcms_na_distprofile0630.2026.pdf

LIST OF CHALLENGED CLAIMS

Claim 1	
[1.pre]	A mobile device, comprising:
[1.1]	a biometric input device configured to receive biometric data;
[1.2]	a short range radio frequency circuit;
[1.3]	memory configured to store biometric information for identifying an individual associated with transaction information;
[1.4]	a processor coupled with the memory and the biometric input device, the processor configured to:
[1.5.1]	receive a signal from a point of sale terminal via the short range radio frequency circuit,
[1.5.2]	the signal comprising a request to access the memory and retrieve the transaction information,
[1.6]	receive the biometric data from the biometric input device,
[1.7]	compare the received biometric data with the biometric information stored in the memory, and
[1.8]	transmit the transaction information to the point of sale terminal using the short range radio frequency circuit when the received biometric data matches the stored biometric information; and
[1.9]	a mobile device body housing the biometric input device, short range radio frequency circuit, memory, and processor.
Claim 2	
[2]	The mobile device of claim 1, wherein the mobile device is one of a cellphone, smartphone, or tablet.
Claim 3	
[3]	The mobile device of claim 1, wherein the biometric input device is a fingerprint scanner.
Claim 4	
[4]	The mobile device of claim 1, wherein the processor is further configured to transmit the received biometric data or the stored biometric information with the transaction information.

Claim 5	
[5]	The mobile device of claim 1, wherein the transaction information is account information.
Claim 6	
[6]	The mobile device of claim 1, wherein the transaction information is credit card information.
Claim 7	
[7]	The mobile device of claim 1, further comprising memory configured to store the transaction information.
Claim 8	
[8]	The mobile device of claim 7, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.
Claim 9	
[9]	The mobile device of claim 1, wherein the processor is configured to compare the received biometric data with the biometric information stored in the memory in response to receiving the request to retrieve the transaction information.
Claim 10	
[10]	The mobile device of claim 1, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz.
Claim 11	
[11.pre]	A cellular telephone, comprising:
[11.1]	a fingerprint scanner configured to receive fingerprint data;
[11.2]	a short range radio frequency circuit;
[11.3]	memory configured to store fingerprint information for identifying an individual associated with transaction information;
[11.4]	a processor coupled with the memory and the fingerprint scanner, the processor configured to:
[11.5.1]	receive a signal from a point of sale terminal via the short range radio frequency circuit,

[11.5.2]	the signal comprising a request to access the memory and retrieve the transaction information,
[11.6]	receive the fingerprint data from the fingerprint scanner,
[11.7]	compare the received fingerprint data with the fingerprint information stored in the memory, and
[11.8]	transmit the transaction information to the point of sale terminal using the short range radio frequency circuit when the received fingerprint data matches the stored fingerprint information; and
[11.9]	a mobile device body housing the fingerprint scanner, short range radio frequency circuit, memory, and processor.
Claim 12	
[12]	The cellular telephone of claim 11, wherein the processor is further configured to transmit the received fingerprint data or the stored fingerprint information with the transaction information.
Claim 13	
[13]	The cellular telephone of claim 11, wherein the transaction information is account information.
Claim 14	
[14]	The cellular telephone of claim 11, wherein the transaction information is credit card information.
Claim 15	
[15]	The cellular telephone of claim 11, further comprising memory configured to store the transaction information.
Claim 16	
[16]	The cellular telephone of claim 15, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.
Claim 17	
[17]	The cellular telephone of claim 11, wherein the processor is configured to compare the received fingerprint data with the fingerprint information stored in the memory in response to receiving the request to retrieve the transaction information.

Claim 18	
[18]	The cellular telephone of claim 11, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz.
Claim 19	
[19.pre]	A cellular telephone, comprising:
[19.1]	cellular circuitry;
[19.2]	a fingerprint scanner configured to receive fingerprint data;
[19.3]	a short range radio frequency circuit;
[19.4]	a memory, the memory configured to store fingerprint information for identifying an individual associated with transaction information;
[19.5]	a processor coupled with the memory and the fingerprint scanner, the processor configured to:
[19.6.1]	receive a signal from a point of sale terminal via the cellular circuitry,
[19.6.2]	the signal comprising a request to access the memory and retrieve the transaction information,
[19.7]	receive the fingerprint data from the fingerprint scanner,
[19.8]	compare the received fingerprint data with the fingerprint information stored in the memory, and
[19.9]	transmit the transaction information to a remote location using the cellular circuitry when the received fingerprint data matches the stored fingerprint information; and
[19.10]	a cellular telephone body housing the fingerprint scanner, short range radio frequency circuit, memory, and processor.
Claim 20	
[20]	The cellular telephone of claim 19, wherein the processor is further configured to transmit the received fingerprint data or the stored fingerprint information with the transaction information.
Claim 21	
[21]	The cellular telephone of claim 19, wherein the transaction information is account information.

Claim 22	
[22]	The cellular telephone of claim 19, wherein the transaction information is credit card information.
Claim 23	
[23]	The cellular telephone of claim 19, further comprising memory configured to store the transaction information.
Claim 24	
[24]	The cellular telephone of claim 23, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.
Claim 25	
[25]	The cellular telephone of claim 19, wherein the processor is configured to compare the received fingerprint data with the fingerprint information stored in the memory in response to receiving the request to retrieve the transaction information.
Claim 26	
[26]	The cellular telephone of claim 19, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz.

Apple Inc. (“Apple”) and Samsung Electronics Co., Ltd. (“Samsung”) (collectively, “Petitioners”) petition for IPR of claims 1-26 (“**Challenged Claims**”) of U.S. Patent No. 10,235,513 (“the ’513 patent”) based on the compelling evidence of obviousness presented throughout this Petition.

I. REQUIREMENTS FOR IPR

A. Grounds for Standing

Petitioners certify that the ’513 Patent is available for IPR, and that Petitioners are not barred or estopped from requesting IPR of the Challenged Claims on the below-identified grounds.

B. Challenge and Relief Requested

This Petition sets forth challenges on grounds below, which are supported by Dr. Seth Nielson’s Declaration (EX1003).

Ground	Claim(s)	Prior Art Basis under 35 U.S.C. §103
1A	1-9, 11-17, 19-25	Wang-Barnes
1B	10, 18, 26	Wang-Barnes-Bashan
2A	1-9, 11-17, 19-25	Wang-Srey
2B	10, 18, 26	Wang-Srey-Bashan
3A	1-3, 5-9, 11, 13-17, 19, 21-25	Mardikar-Cooke
3B	10, 18, 26	Mardikar-Cooke-Lee

The ’513 patent claims priority to a series of continuation applications that each claim priority to U.S. Provisional Application No. 60/394,241, filed 7/9/2002.

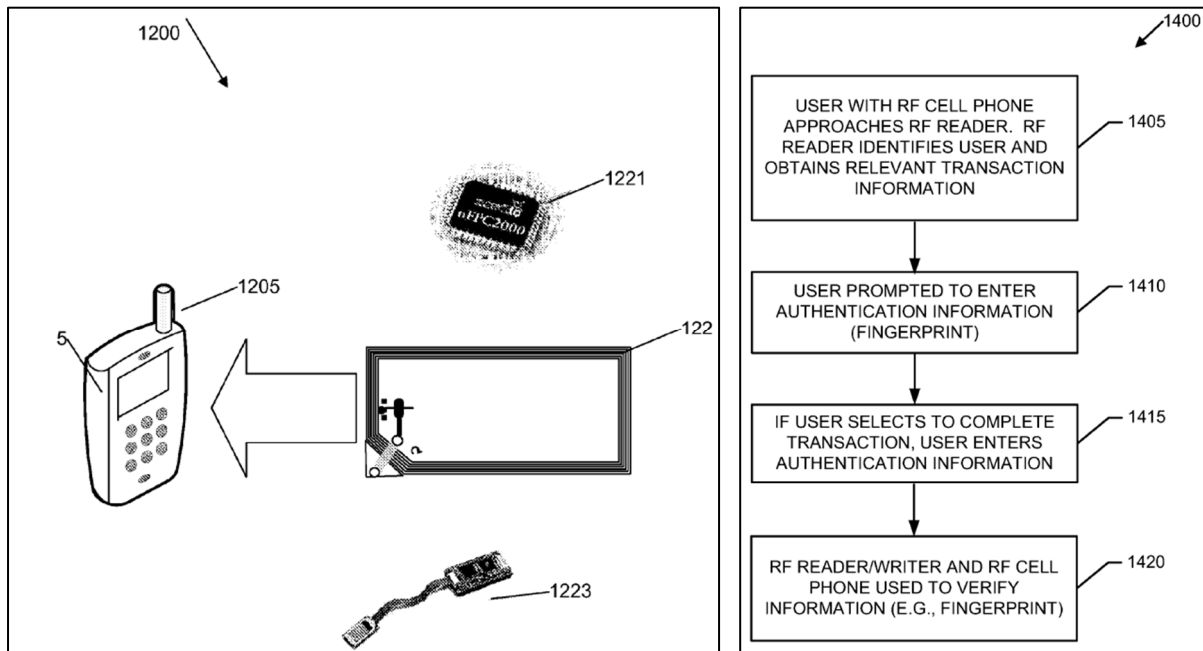
EX1001, Cover. As explained below in §V.C.1, the '513 patent is not entitled to claim priority to this provisional application or its other priority application. References EX1004-EX1007 listed in the table below qualify as prior art if the 7/9/2002 date is used as the “Critical Date,” and References EX1009-EX1011 qualify as prior art if the 12/7/2016 filing date associated with the application resulting in the '513 patent is used as the “Critical Date.”

Reference	Date	Status
Wang (EX1004)	Published Sept. 8, 2000	§102(b)
Barnes (EX1005)	Filed May. 23, 2002, Issued Dec. 17, 2013	§102(e)
Srey (EX1006)	Issued Oct. 31, 2000	§102(b)
Bashan (EX1007)	Issued Apr. 4, 2000	
Mardikar (EX1009)	Issued Jan. 31, 2012	§102(b)/ §102(a)(1)/ §102(a)(2)
Cooke (EX1010)	Published Jan. 23, 2014	
Lee (EX1011)	Issued Jun. 24, 2014	

II. THE '513 PATENT OVERVIEW

The '513 patent discloses a RF cellular telephone that communicates with a point of sale (POS) device. EX1001, FIG. 12 (reproduced below), 14:35-15:67. The RF cellular telephone includes an RF antenna, a chip that “carries authentication

information (e.g., a fingerprint) and transaction information (e.g., credit card information),” and a fingerprint identifier/scanner. EX1001, 14:43-15:22.



EX1001, FIG. 12 (left), FIG. 14 (right).

When a user carrying the RF cellular telephone approaches an RF reader/writer at the POS, the reader identifies the user and obtains the relevant transaction information. EX1001, FIGS. 12-14, 15:24-67. The user is prompted to enter authentication information (a fingerprint), and the RF reader/writer and RF cellular telephone verify that the fingerprint matches the information stored on the telephone to retrieve purchase information. EX1001, FIG. 14, 15:24-67. EX1003, ¶¶[51]-[52].

III. LEVEL OF ORDINARY SKILL

A person of ordinary skill in the art (“POSITA”) relating to the subject matter of the ’513 patent as of July 9, 2002 would have had (1) at least a bachelor’s degree in computer science, computer engineering, or a related field, and (2) at least two years of industry experience including researching or developing software related to secure communication systems/networks. EX1003, ¶¶[35]-[36]. Additional education could substitute for professional experience, and *vice versa*. *Id.*

IV. CLAIM CONSTRUCTION

All claim terms should be construed according to the *Phillips* standard. *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005); 37 C.F.R. §42.100.

This Petition demonstrates obviousness of the Challenged Claims consistent with Apple’s district court constructions (reproduced below):¹

Claim Term	Construction
“transaction information” (Claims 1, 4-9, 11-17, and 19-24)	“information used to process a transaction that includes at least credit card information or rewards card information”

Petitioners respectfully submit that no other claim terms need be construed to resolve issues of controversy in the present Petition. *Wellman, Inc. v. Eastman*

¹ The parties have not yet exchanged terms for construction in Patent Owner’s district court action against Samsung in E.D. Texas.

Chem. Co., 642 F.3d 1355, 1361 (Fed. Cir. 2011); EX1003, ¶¶[56]-[58]. Petitioners reserve the right to respond to any construction offered by Patent Owner or adopted by the Board.

V. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. GROUNDS 1A AND 2A

1. Wang²

Wang³ discloses a portable electronic authorization device (“PEAD”) 200 or portable electronic charge/approval device (PECAD) that communicates with a requesting device 202 to conduct an electronic transaction. EX1004, 10:6-23, 25:19-30. The PECAD incorporates PEAD functionality and “permit[s] the user to conduct transactions vis-a-vis the existing charge card infrastructures.” EX1004, 25:19-35:30.

² Overviews of the prior art references are incorporated in each of the mappings that cite to the prior art references.

³ U.S. Patent No. 6,175,922 is a U.S. patent related to Wang that was cited as one of over a hundred cited references in an IDS. EX1002, 223-236; EX1001, 2. U.S. Patent No. 6,175,922 has overlapping disclosure with Wang but was never applied in any rejection during prosecution. EX1003, footnote-2.

The requesting device 202 sends a transaction request to PEAD 200 via data path 206, and an approval is sent back from the PEAD 200 via data path 212. EX1004, 14:5-15. Examples of the requesting device and PEAD include a point of sale terminal and personal digital assistant (PDA), respectively. EX1004, 20:21-25, 25:11-26:19, 37:8-10; FIG. 2.

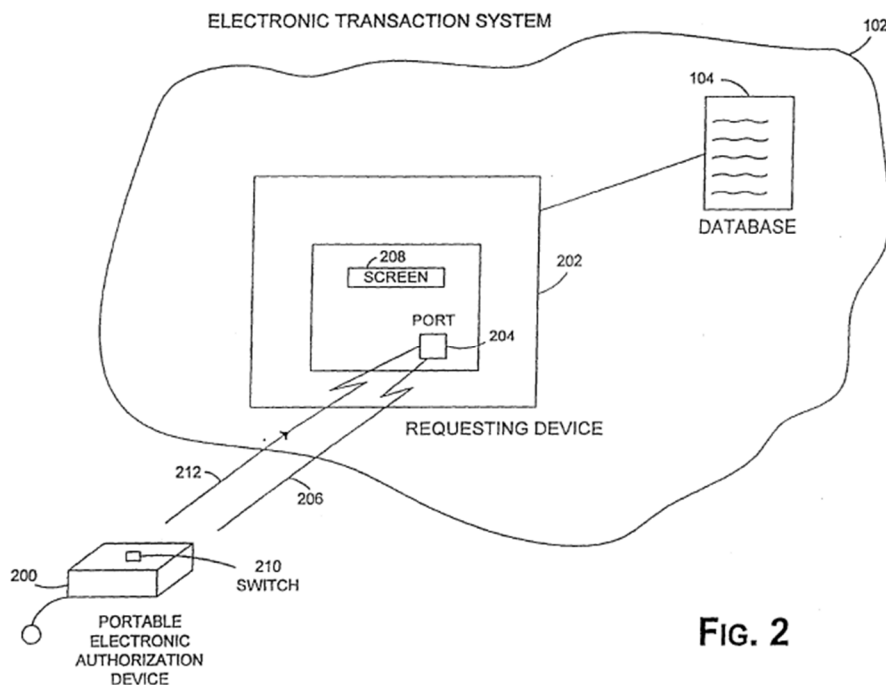


FIG. 2

EX1004, FIG. 2.

A user can approve the transaction. EX1004, 14:16-25. “In some cases, the transaction approval data requires the inclusion of certain pieces of identification data 302,” which can include “unique biometrics or unique identifying data such as fingerprint.” EX1004, 13:16-29, 15:12-23. User identification data and user private

key information is stored in memory 504, which can only be accessed by logic circuitry 502. EX1004, 18:31-19:32, FIG. 5A (reproduced below).

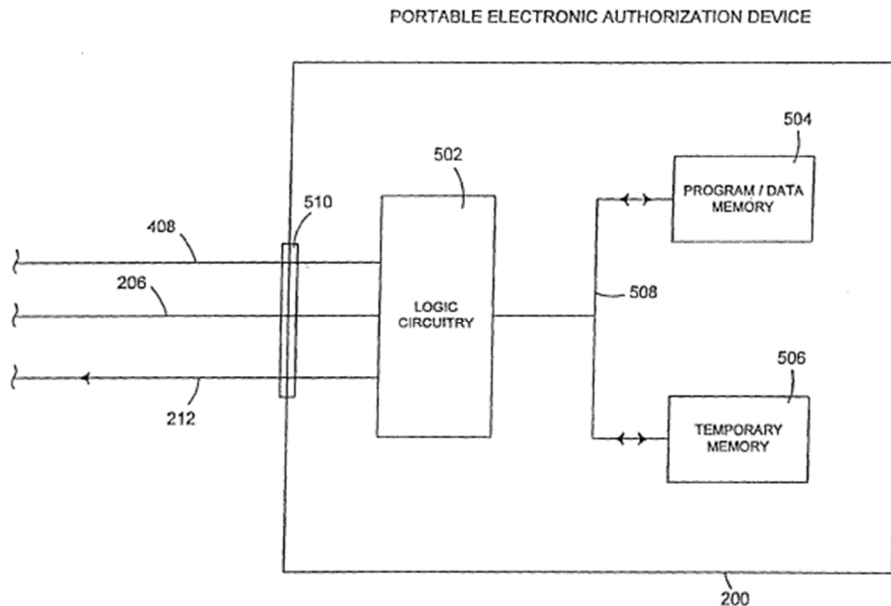


FIG. 5A

EX1004, FIG. 5A.

Before approving a transaction, a user may be required to input the user identification data, such as fingerprints, for user authentication. EX1004, 22:14-25, 13:16-22, 24:24-32, 38:5-6, 40:27-28. The transaction approval is sent only after the user authentication is complete. EX1004, 22:14-25, 24:24-32, 26:20-28; EX1003, ¶¶[59]-[62].

2. Barnes

Barnes discloses a “multi-function communications device 101 that includes conventional mobile phone and personal digital assistant (PDA) capabilities ... such

as a communications module 105.” EX1005, 4:27-30, FIG. 1. The device can take the form of a mobile phone or PDA. EX1005, 5:35-51. Barnes’s device has a cell phone profile and communicates with cell towers, 2.5G and 3G networks, GSM networks, and GPRS networks. EX1005, 7:48-50, 16:36-39. Therefore, a POSITA would have understood the Barnes’s device encompasses a cellular/mobile phone. EX1003, ¶[63].

Barnes’s communication module “is implemented with one or more application specific integrated circuits (ASICs) and software stored in memory” and “includes hardware and software to allow” a processor (e.g., CPU 150) “to communicate with external devices and systems.” EX1005, 6:1-13. The communication module enables Barnes’s device to communicate with various networks including cellular networks, 2G, 2.5G, and 3G networks, GSM networks, GPRS networks, and short range networks, like Bluetooth networks and other local/personal area networks. EX1005, 6:14-9:24.

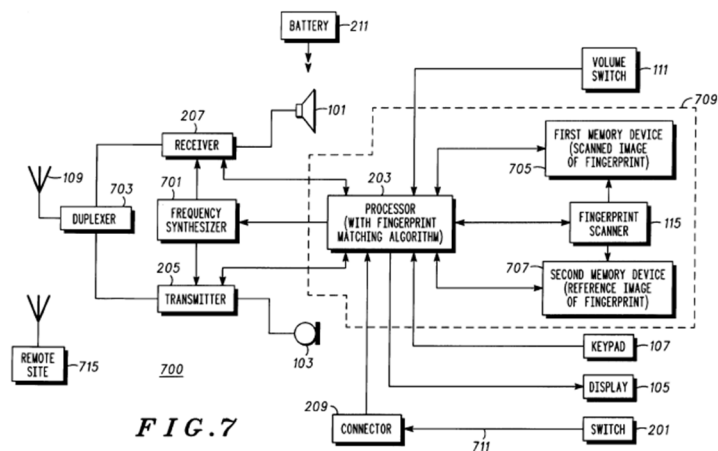
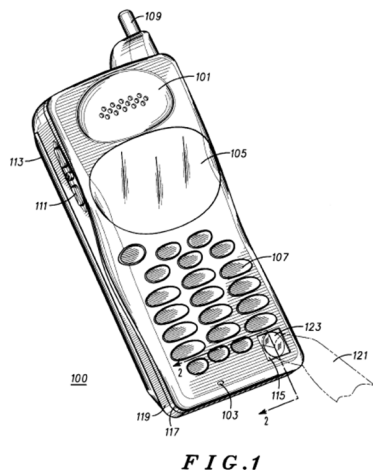
Barnes’s device utilizes antennas respectively configured to operate with the different networks to support contemporaneous wireless communications with multiple networks. EX1005, 9:25-11:53. Thus, a POSITA would have understood the Barnes’s device is configured to communicate over short distances (e.g., using Bluetooth networks and its short range wireless local area network (LAN) module) and long distances (e.g., using a cellular network module such as its wireless wide

area network (WWAN) module). EX1005, 6:14-9:24; EX1003, ¶¶[64]-[65]. Upon detection of a network switching condition, Barnes's device can switch between networks. EX1005, 9:25-10:36, 11:5-12:44, 29:4-30:33.

When Barnes's device is used for a commercial transaction, the user may be required to input authentication data. EX1005, 18:33-36. The device contains a module that authenticates the user with fingerprint data, e.g., by comparing fingerprint data received through a fingerprint scanner to stored user fingerprint data. EX1005, 17:33-48; 18:13-18, 21:1-14; EX1003, ¶[66].

3. Srey

Srey discloses a cellular telephone that includes an antenna 109 and “a fingerprint identification system (709) including a scanner (115) for scanning a fingerprint (123) of a finger (121) to generate an image of the fingerprint (123).” EX1006, Abstract, 2:46-64, 3:36-42, FIG. 1.



EX1006, FIG. 1 (left), FIG. 7 (right).

As depicted in FIG. 7 above, the fingerprint identification system 709 includes a fingerprint scanner 115 coupled to a first memory device that stores a scanned image of a fingerprint, a second memory device that stores a reference image of a fingerprint, and a processor that performs a fingerprint matching algorithm to determine if the scanned image of the fingerprint matches the stored reference image of a fingerprint. EX1006, 3:57-4:20, 4:64-5:20; EX1003, ¶¶[67]-[68].

4. The Prior Art References Are Analogous Art

Wang, Barnes, Srey, Bashan⁴, Mardikar⁵, Cooke,⁵ and Lee⁶ are analogous art to the '513 patent at least because they: (1) are from the same field of endeavor as the purported claimed invention of the '513 patent; and/or (2) are reasonably pertinent to the problem faced by the inventors of the '513 patent. *In re Bigio*, 381 F.3d 1320, 1325, 72 USPQ2d 1209, 1212 (Fed. Cir. 2004).

The '513 patent describes security solutions for a radio frequency (RF) device to communicate with a RF reader/writer, e.g., a POS device. EX1001, 1:35-62, 2:5-6, Abstract, 14:35-38. The '513 patent purports to address problems such as security and user verification by implementing a user authentication protocol involving authenticating user fingerprints before authorizing a transaction. EX1001, 1:28-31,

⁴ Reference applied in Grounds 1B and 2B.

⁵ References applied in Ground 3A.

⁶ Reference applied in Ground 3B.

15:24-67. The applied references are directed to the same field and/or address the same problems. EX1003, ¶¶[69]-[72].

Wang is directed to communications between a PEAD and POS device that requires user approval and fingerprint authentication. EX1004, 13:16-15:23, 22:14-25, 24:24-32, 38:5-6, 40:27-28. 26:20-28; *see* §V.A.1. Barnes requires user fingerprint authentication before its cellular device can be used to authorize a transaction. EX1005, 7:48-50, 16:36-17:48, 18:13-36, 21:1-14; *see* §V.A.2. Srey describes performing fingerprint verification to verify a user and unlock a cellular phone before use. EX1006, 2:16-17, 2:65-3:36; *see* §V.A.3. Bashan is analogous art to the '513 patent at least because it's field of endeavor relates to wireless transactions using a mobile device. EX1007, Abstract, 1:5-47. Mardikar describes secure, biometrically authenticated contactless payment from a personal mobile/cellular device at an NFC POS. EX1009, Abstract, 6:42-8:61, 9:35-12:55; *see* §V.C.2. Cooke describes contactless payment transactions between a payment-enabled mobile device and a proximity reader incorporated with a POS terminal. EX1010, Abstract, ¶¶[0003], [0025]; *see* §V.C.3. Lee describes controlling wireless RF communications between a mobile phone and an external RF reader. EX1011, Abstract, *see* §V.D.1. Thus, Wang, Barnes, Srey, Mardikar, Cooke, and Lee are all analogous art to the '513 patent. EX1003, ¶[71].

As explained in more detail below in §§V.A.5 and V.A.6, a POSITA would have combined the teachings of Wang with Barnes or Srey because doing so would have merely involved combining prior art elements according to known methods (e.g., fingerprint matching and cellular network connectivity on cellular phones) to yield the predictable result of an electronic transaction system in which a portable device (cellular/mobile phone) having security features, such as fingerprint authentication, communicates with a point of sale device using short range and wide area networks. EX1003, ¶[72]; *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-421, 82 USPQ2d 1385, 1395-97 (2007); M.P.E.P. §2143.

5. Combination of Wang and Barnes

A POSITA would have combined Wang and Barnes such that:

- 1) Wang's portable device would have been implemented as or part of Barnes's cellular phone and would have included Barnes's short range wireless LAN module and WWAN (cellular) module.
- 2) Wang's device would have incorporated Barnes's teachings of connecting to multiple networks at the same time and switching networks upon the satisfaction of a switching condition.
- 3) Barnes's user authentication involving a fingerprint scanner and performing a comparison of scanned and stored user fingerprints would be part of Wang's user authentication.

- 4) Retrieving payment information in response to transaction requests, as taught by Barnes, in Wang's device.

EX1003, ¶[73].

Wang describes conducting an electronic transaction between a portable device and a second device, such as a POS device, using a computer network (e.g., the Internet). EX1004, 1:23-35, 15:24-35. Transaction communications are performed using infrared or wireless RF technology, thereby indicating that the communications are short range communications. EX1004, 19:13-26; EX1003, ¶[74] (explaining that infrared technology was primarily designed for short range transmissions). Moreover, while Wang's user authentication method utilizes biometric data such as fingerprint data, Wang does not reveal all the details of the user authentication method. EX1004, 22:14-25.

A POSITA would have combined Wang and Barnes in the above-noted manner for the following reasons.

First, Wang's device would have been modified to incorporate hardware and software that permits Wang's device to communicate using multiple networks. EX1003, ¶¶[75]-[76]. For example, Wang's device would have been modified to include cellular circuitry (e.g., ASICs, antennas) and related software, as described by Barnes, so that the device can communicate using WWAN cellular networks, such as 2G, 3G, and GSM networks. EX1005, 8:19-10:36, 6:1-14; EX1003, ¶[76].

Effectively, the combined Wang-Barnes device would operate as a cellular/mobile phone with long distance (e.g., cellular) and short distance communications capabilities, e.g., using Bluetooth technology. *Id.*

Second, adding Barnes's long distance communication capabilities would have allowed the Wang device to conduct electronic transactions over long and short ranges. EX1003, ¶[77]. Consequently, the user would experience enhanced convenience, accessibility, and usability. *Id.* For instance, with the Wang-Barnes device, a user could pay for a transaction remotely while traveling in a car several kilometers from a vendor point of sale device or in-person a few feet away from a vendor point of sale device. *Id.*

Third, incorporating the ability to switch between different networks, as taught by Barnes, would have allowed Wang's device to avoid a single point of failure and switch networks when a currently-connected network fails or has data transmission issues. By incorporating Barnes's network switching capabilities, Wang's device would improve reliability to maintain communications and complete a transaction. EX1005, 11:63-12:65; EX1003, ¶[78].

Fourth, a POSITA looking to implement Wang's user authentication mechanism would have turned to Barnes because Barnes provides the details of fingerprint-based authentication. EX1003, ¶[79]. For instance, both Wang and Barnes disclose using biometric matching to authenticate a user. EX1004, 22:14-

25, 13:16-29; EX1005, 17:38-18:18. Barnes additionally reveals that in doing so, a fingerprint is scanned and then compared with stored fingerprint data to authenticate the user. EX1005, 18:13-18. In both Wang and Barnes, such authentication can be required before completing transactions that require high security. EX1004, 22:14-25, 38:5-7, 40:27-28; EX1005, 18:1-18, 21:1-14; EX1003, ¶[79].

Fifth, a POSITA looking to implement Wang's electronic transaction payment would have turned to Barnes because Barnes provides the details of providing payment information as part of the transaction. EX1003, ¶[80]. For instance, Barnes explains that a receiving mobile device provides stored payment information, such as credit card or bank account information, in response to receiving a transaction request that requests payment information stored in the receiving device. EX1005, Abstract, 3:53-4:2, 7:3-24, 21:52-22:10, 29:39-46, 30:22-33, 22:57-23:48, 49:37-67.

The combination of Wang and Barnes would have been predictable and had a reasonable expectation of success. EX1003, ¶[81]. Both Wang and Barnes describe their devices as being configurable to operate as a PDA. EX1004, 20:21-25; EX1005, 4:26-40. Due to the similarities of the devices, a POSITA would have predictably turned to Barnes to enhance the capabilities of the Wang device, in the manner described above. EX1003, ¶[81]. Moreover, because Wang was directed to a portable device involved in electronic transactions, it would have been predictable for a POSITA to turn to Barnes's cellular device (and communication systems) that

is also directed to electronic transactions, and implement Barnes's known techniques (including e.g., network switching). *Id.* For instance, as the drive for enhanced connectivity and portability using the Internet grew in the 2000s, expanding the use of Wang's device into cellular networks using known cellular hardware and software would have been predictable and had a reasonable chance of success because incorporating cellular connectivity for portable devices was known and increasingly common in the 2000s. *Id.*

Lastly, incorporating the details of Barnes's authentication method would also have been predictable with a reasonable chance of success because Barnes provided conventional and known implementation details for fingerprint-based user authentication, such as comparing scanned fingerprint data with stored fingerprint data. EX1003, ¶[82].

6. Combination of Wang and Srey

A POSITA would have combined Wang and Srey such that:

- 1) Wang's portable device is implemented as or part of Srey's cellular phone including Srey's cellular network communication capabilities in addition to Wang's ability to communicate across a short range network; and
- 2) Wang's user authentication includes Srey's user authentication method and system architecture involving a fingerprint scanner coupled to

processor and memory devices to perform a comparison of scanned and stored user fingerprints

EX1003, ¶[83].

A POSITA would have combined Wang and Srey in the above-noted manner for the following reasons.

First, Wang's device would have been modified to include cellular circuitry such as a cellular receiver and transmitter, as described in Srey, so that the device can communicate using cellular networks. EX1006, FIGS. 5, 9; 8:25-37, 9:39-67. Effectively, the combined Wang-Srey device would have operated as a cellular phone with long range (e.g., cellular) and short range communications capabilities, e.g., using infrared or RF technology. EX1003, ¶¶[84]-[85].

Second, modifying Wang's device into or to incorporate Srey's cellular phone capabilities would have allowed the Wang device to conduct electronic transactions over long and short ranges. EX1003, ¶[86]. Consequently, the user would experience enhanced convenience, accessibility, and usability. EX1003, ¶[86]. For instance, a user could pay for a transaction remotely while traveling in a car several kilometers from a vendor point of sale device or in-person a few feet away from a vendor point of sale device. EX1003, ¶[86].

Third, a POSITA looking to implement Wang's user authentication mechanism would have turned to Srey because Srey provides the details of

fingerprint-based authentication. EX1003, ¶[87]. For instance, both Wang and Srey disclose using biometric matching to authenticate a user. EX1004, 22:14-25, 13:16-29; EX1006, 5:55-6:17. Srey additionally reveals that the memory, processor, and input device (scanner) architecture to scan and compare fingerprints to authenticate the user. EX1005, 18:13-18. EX1003, ¶[87].

The combination of Wang and Srey would have been predictable and had a reasonable expectation of success. EX1003, ¶[88]. Because Wang was directed to a portable device involved in electronic transactions, it would have been predictable for a POSITA to allow Srey's cellular phone to additionally communicate in a cellular communication system, which offers Internet access in a larger coverage area than short range networks. EX1003, ¶[88]. In particular, as the drive for enhanced connectivity and portability using the Internet grew in the 2000s, expanding the use of Wang's device into cellular networks using known cellular hardware and software would have been predictable and had a reasonable chance of success because incorporating cellular connectivity for portable devices was known and increasingly common in the 2000s. EX1003, ¶[88].

Lastly, incorporating the details of Srey's authentication method would have been predictable with a reasonable chance of success because Srey provided conventional and known implementation details for fingerprint-based user authentication, such as storing fingerprint data in a memory, scanning fingerprint

data, and then comparing the scanned fingerprint data with the stored fingerprint data. EX1003, ¶[89].

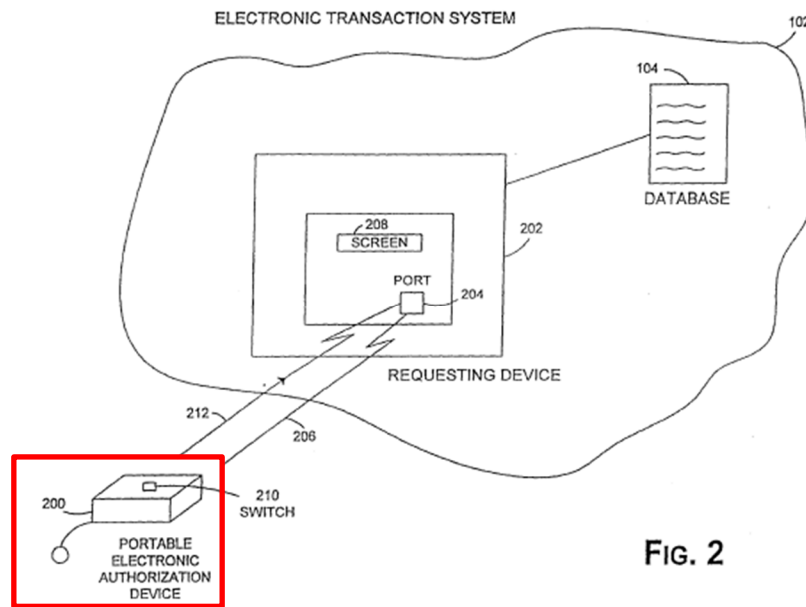
7. Claim Element Analysis

The mappings described below apply to Grounds 1A and 2A unless explicitly noted otherwise.

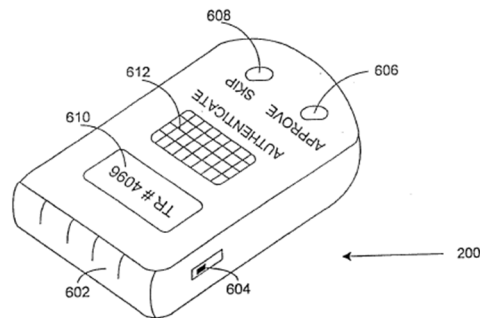
(a) Claims 1 and 11

[1.pre], [11.pre]

Wang discloses a PEAD 200 that is “implemented using a general purpose portable computing device, such as any of the miniaturized portable computers or personal digital assistants (PDA’s) that are currently popular. A PDA such as the Apple Newton®, for example, may be employed to implement PEAD 200.” EX1004, 20:21-25, 10:6-23. An example of a PEAD is shown in FIGS. 2 and 6 below. EX1004, 8:9-26; EX1003, ¶¶[133]-[134].



EX1004, FIG. 2⁷.



EX1004, FIG. 6A.

Wang's PEAD "is small enough to be comfortably carried with the user at all times." EX1004, 21:22-25. Accordingly, at least because the PEAD is a portable

⁷ Here and throughout the Petition, annotations to the figures have been added in color.

electronic device and because portable computers and PDAs are mobile devices, Wang discloses a “*mobile device*.” EX1003, ¶[135].

The PECAD incorporates PEAD functionality and “permit[s] the user to conduct transactions vis-a-vis the existing charge card infrastructures.” EX1004, 25:19-35:30. Thus, the remarks associated with the PEAD also apply to the PECAD, and the PECAD also maps onto the “*mobile device*.” EX1003, ¶[136].

As explained above in §§V.A.2-3 and §§V.A.5-6, in the Wang-Barnes or Wang-Srey combination systems, the PEAD operates as a “*cellular telephone*” thereby enhancing its capability to communicate over a cellular network. EX1005, 4:27-30, FIG. 1, 5:35-51, 7:48-50, 16:36-39; EX1006, Abstract, 2:46-64, 3:36-42, FIG. 1; EX1003, ¶[137]. And because “*cellular telephone[s]*” are also “*mobile device[s]*,” the combination of Wang with Barnes or Srey renders [1.pre]/[11.pre] obvious. *Id.*; EX1005, 4:27-30 (“communications device 101 that includes *conventional mobile phone*”)⁸.

[1.1], [11.1]

Referring to Wang’s FIG. 6A, Wang’s PEAD includes a user authentication mechanism 612 that, in some cases, requires a user “to furnish a fingerprint or a

⁸ Here and throughout the Petition, emphasis is added to prior art quotes using italicized font.

voice print, or other biometrics and/or identifying characteristics specific to the authorized user before [the] PEAD 200 can be activated and employed for approving transactions.” EX1004, 22:14-25.

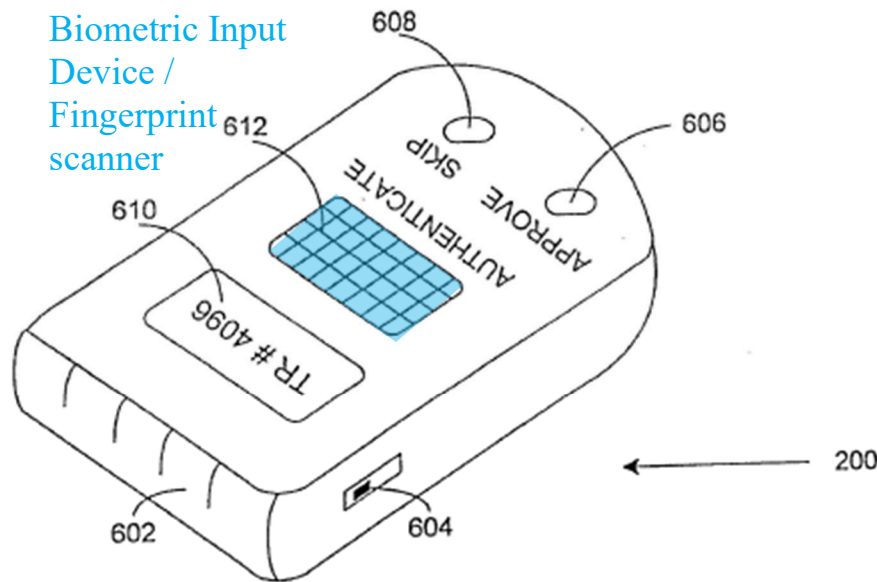


FIG. 6A

EX1004, FIG. 6A.

Relatedly, Wang’s claims 12 and 30 recite “wherein said authentication mechanism employs fingerprint for authentication,” and such an authentication mechanism is illustrated above as item 612 with the label “AUTHENTICATE.” EX1004, 38:5-7, 40:27-28. Accordingly, a POSITA would have understood that Wang’s authentication mechanism (“*biometric input device*”/“*fingerprint*

scanner”) is configured to receive “*biometric data*”/“*fingerprint data*.” EX1003, ¶¶[138]-[140]. Barnes and Srey corroborate this understanding.

Ground 1A

Barnes teaches that authentication information such as fingerprint data is stored on the cellular phone to authenticate a user. EX1005, 17:38-48, 18:42. Like Wang, user authentication may be required to permit a commercial transaction. EX1005, 18:1-6. To authenticate a user, fingerprint data is received through a fingerprint scanner and then compared to stored fingerprint data. EX1005, 18:13-18, 21:1-14. Accordingly, it would have been obvious to a POSITA that in the Wang-Barnes combination, Wang’s authentication mechanism would have been a “*biometric input device*”/“*fingerprint scanner*.” EX1003, ¶[141].

Ground 2A

Similarly, Srey discloses the use of a fingerprint scanner 115 to obtain fingerprints which are then compared with stored fingerprints to authenticate a user. EX1006, 2:46-67, 3:33-4:5, 4:49-6:16, FIGS. 2, 7. Thus, in the Wang-Srey combination, it would have been obvious to a POSITA that Wang’s authentication mechanism would have been a “*biometric input device*”/“*fingerprint scanner*.” EX1003, ¶[142].

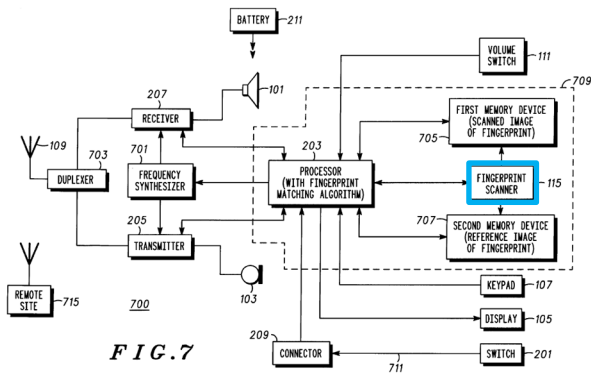


FIG. 7

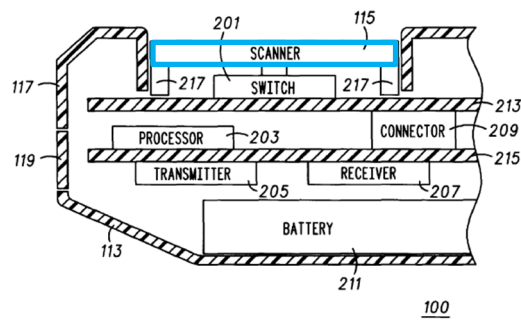


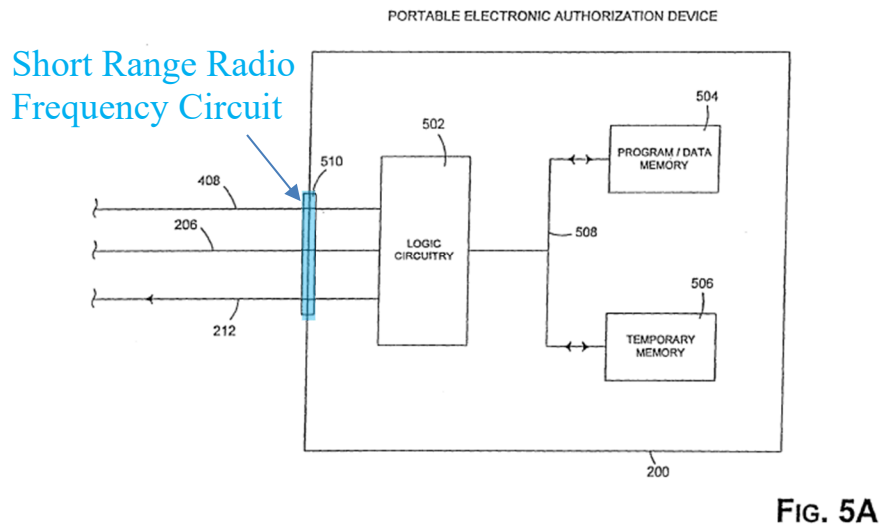
FIG. 2

EX1006, FIGS. 7, 2.

[1.2], [11.2]

Wang's PEAD is used to conduct transactions with point of sale terminals, including e.g., charge card readers and ATM terminals, that are known to be used in short range transactions. EX1004, 10:6-23, 25:11-18. Accordingly, it would have been obvious to a POSITA that Wang's communication port 510 is "*a short range radio frequency circuit*," e.g., when it is communicating using wireless RF signals with charge card readers and ATM terminals located in close proximity to the PEAD. EX1004, 19:13-26; EX1003, ¶[143]-[144].

Moreover, a POSITA would have understood that because infrared communications are short range, Wang's communication port is designed to operate over short range communications, e.g., from between 5 centimeters to 2 meters. EX1003, ¶[145] (citing EX1015, 1-3).



EX1004, FIG. 5A.

Additional Disclosure Relevant to Ground 1A

Barnes's device includes a short range wireless LAN module (e.g., a Bluetooth module) that allows the device to communicate and wirelessly exchange payment information with point of sale (POS) devices using a RF frequency, e.g., 2.4 GHz. EX1005, 7:3-25. Barnes's device can include different circuitries in the form of different antennas to communicate with different networks, respectively. EX1005, 9:25-50. Barnes also teaches that all or part of its communication module (used to communicate with external devices) "is implemented with one or more application specific integrated circuits (ASICs) and software stored in memory." EX1005, 6:1-13. Thus, Barnes teaches the use of antennas and ASICs to support LAN or short range communications. EX1003, ¶[146]. In the Wang-Barnes combination and for the reasons previously explained in §V.A.5, it would have been

obvious to a POSITA that Wang's communication port would have included or been implemented as Barnes's short range RF wireless LAN module and LAN circuitry to facilitate transaction communication with a POS device. EX1003, ¶[146].

[1.3], [11.3]

Wang's "[p]rogram/data memory 504 stores, among others, the codes which operate PEAD 200 as well as the user identification data and the user's private key." EX1004, 18:31–33; FIG. 6B – flash memory 656; 22:27-35.

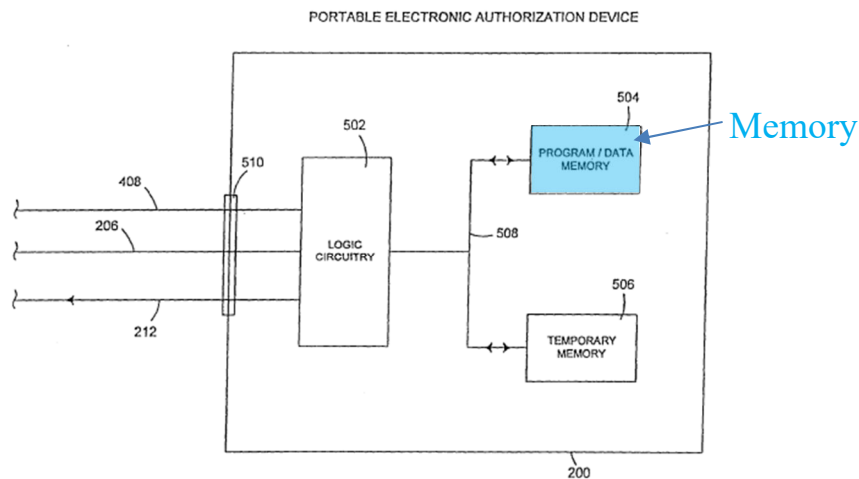


FIG. 5A

EX1004, FIG. 5A.

Wang's user identification data "may include any of the user's name, his birth date, his social security number, or *other unique biometrics or unique identifying data such as fingerprint, DNA coding sequence, voice print*, or the like." EX1004, 13:19–22. The identification data is for the user associated with a charge card (e.g., credit card) and a charge card transaction ("*individual associated with transaction*

information”) using the charge card. EX1004, Abstract, 5:8-10; 25:32-35 (The charge cards themselves may represent credit cards (such as Visa or Master Cards)). In some cases, the user must “furnish a fingerprint ... or other biometrics and/or identifying characteristics” for authentication prior to approval of a transaction involving the user. EX1004, 22:14-25.

As explained above in [1.1], Barnes and Srey also teach storing fingerprint data (“*biometric/[fingerprint] information for identifying an individual associated with transaction information*”) to be used for comparison with received fingerprint data when authenticating a user. EX1005, 18:1-18, 21:1-14; EX1006, 2:46-67, 3:33-4:5, 4:49-6:16, FIGS. 2, 7. Accordingly, each of the Wang-Barnes and Wang-Srey combinations renders [1.3]/[11.3] obvious. EX1003, ¶¶[147]-[150].

[1.4], [11.4]

As shown in Wang’s FIG. 5A below, Wang’s “PEAD 200 includes logic circuitry 502, which may represent a *central processing unit such as a microprocessor or a microcontroller*, discrete logic, programmable logic, an application-specific integrated circuit (ASIC).” EX1004, 18:26-30; FIG. 6B (microcontroller 654), 22:26-23:9. “*A bus 508 couples program/data memory 504 and temporary memory 506 with logic circuitry 502.*” EX1004, 19:13-14. Thus, the Wang-Barnes and Wang-Srey devices each include “*a processor coupled with the memory.*” EX1003, ¶¶[151]-[152].

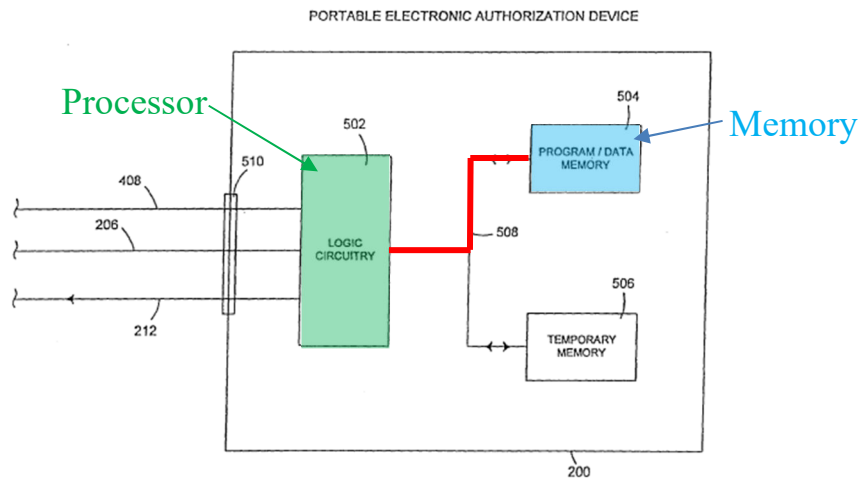


FIG. 5A

EX1004, FIG. 5A.

It would have been obvious to a POSITA that the logic circuitry (“*processor*”) is also coupled to the user authentication mechanism (“*biometric input device*”/“*fingerprint scanner*”) under both grounds for several reasons. EX1003, ¶[153].

First, as noted above in [1.3], the memory 504 stores user identification data such as the user’s fingerprints. EX1004, 18:31–33, 13:19–22. It would have been obvious to a POSITA that a user would have scanned the user’s fingerprint through the user authentication mechanism (e.g., fingerprint scanner) and the scanned fingerprint data would then be sent to memory 504 for storage. EX1003, ¶[154]; EX1004, 22:14-25; *see* [1.1]. Thus, a POSITA would have recognized that the user authentication mechanism is coupled to memory 504, which itself is coupled to the

logic circuitry. EX1003, ¶[154]. Therefore, the authentication mechanism would have been at least indirectly coupled to the logic circuitry. *Id.*

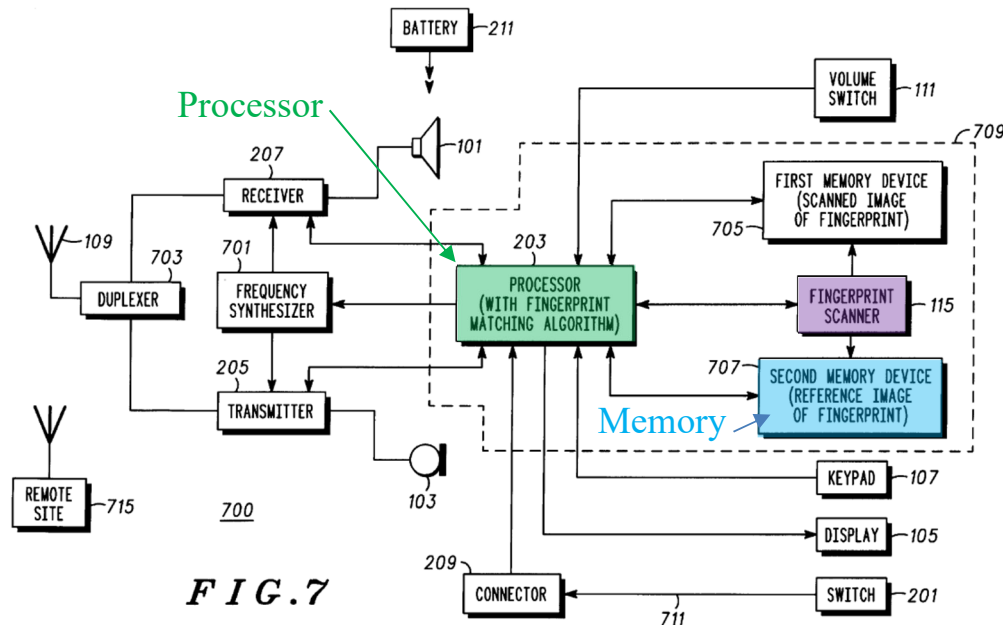
Second, Wang teaches that “*reading the user identification data and accessing the user’s private key can only be accomplished via the encryption logic of logic circuitry 502.*” EX1004, 20:5-10. And because Wang teaches that “access to program/data memory 504 and the data therein ... can only be made by logic circuitry 502,” a POSITA would have understood that the logic circuitry would have been coupled to the user authentication mechanism from which user identification data is obtained or the memory 504 storing the fingerprint data. EX1004, 19:27–29; EX1003, ¶[155].

Third, it would have been obvious to a POSITA that a processor would have authenticated a user’s fingerprints prior to approving a transaction, as explained above in [1.3]. EX1004, 22:14-25; EX1003, ¶[156] (citing EX1013, EX1014). And because the logic circuitry is the only processor shown in FIG. 5A, it would have been obvious that the logic circuitry would have been coupled to the user authentication mechanism, through which a user would have provided the user’s fingerprints. EX1003, ¶[156].

Additional Disclosure Relevant to Ground 2A

As shown in Srey’s FIG. 7 below, Srey’s fingerprint scanner 115 and second memory 707 storing a reference fingerprint image are both coupled to a processor

203. EX1006, FIG. 7, 4:64-5:10. Because the fingerprint scanner is implemented as part of Wang's user authentication mechanism ("*biometric input device*") and Wang's logic circuitry would perform the same fingerprint comparison operations as Srey's processor, it would have been obvious to a POSITA that in the Wang-Srey device, the "*processor [is] coupled with the memory and the biometric input device*" / "*fingerprint scanner.*" EX1003, ¶¶[157]-[158]; see §V.A.6.



EX1006, FIG. 7.

As explained below in [1.5.1]-[1.8]/[11.5.1]-[11.8], Wang's logic circuitry also performs the recited operations in [1.5.1]-[1.8]/[11.5.1]-[11.8].

[1.5.1], [11.5.1]

As shown below in Wang's FIG. 2, the PEAD receives a signal 206 from a requesting device. EX1004, 10:13-22, 14:6-7. Various types of requesting devices

can be used including “for example, an ATM machine, a computer terminal in a network, an automated library check-out terminal, or *similar devices for permitting the user to transact business with the electronic transaction system.*” EX1004, 10:13-16. Wang explains that point-of-sale systems are devices used to permit a user to conduct an electronic transaction with the PEAD. EX1004, 3:26-4:9; 25:11-13; 25:19-24. Accordingly, it would have been obvious to a POSITA that Wang teaches “*receiv[ing] a signal from a*” requesting device that is a “*point of sale terminal.*” EX1003, ¶¶[159]-[160].

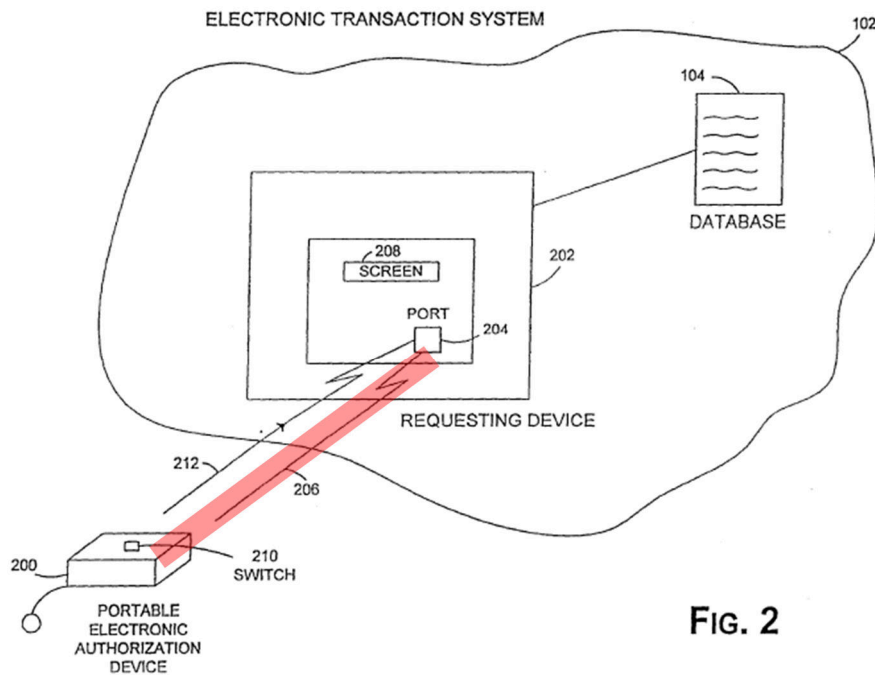


FIG. 2

EX1004, FIG. 2.

Wang also teaches that the signal 206 is received via the communication port 510 (“*via the short range radio frequency circuit*”). As shown in FIG. 2 above and

FIG. 5A below, “[c]ommunication port 510 represents the communication gateway between PEAD 200 and the electronic transaction system,” and data received through the port 510 is then provided to the logic circuitry (“*processor*”). EX1004, 19:13-26.

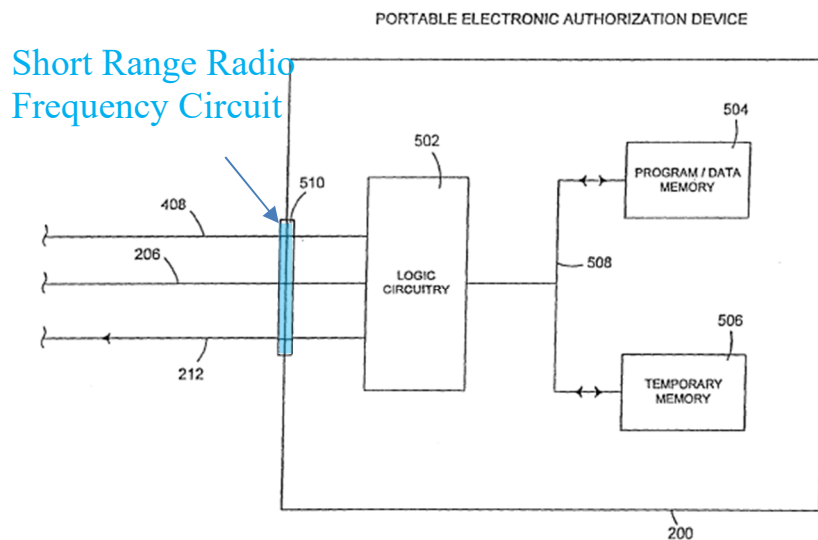


FIG. 5A

EX1004, FIG. 5A.

As explained above in [1.2], in the Wang-Barnes and Wang-Srey devices, the communication port is a “*short range radio frequency circuit.*” Accordingly, Wang in view of Barnes or Srey renders obvious [1.5.1]/[11.5.1]. EX1003, ¶¶[161]-[162].

Additional Disclosure Relevant to Ground 1A

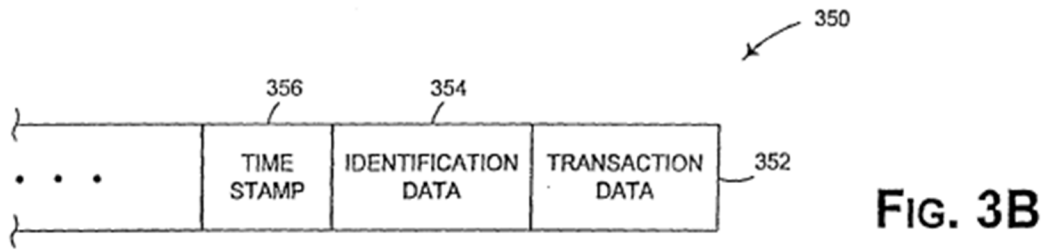
Barnes explicitly teaches that its device communicates with a point of sale device to conduct a transaction using its short range wireless LAN module. EX1005, 3:53-4:25, 7:3-24, 29:39-50. As explained above in [1.2], the short range wireless

LAN module is the “*short range radio frequency circuit*” in the Wang-Barnes device. For this additional reason, Wang-Barnes renders [1.5.1]/[11.5.1] obvious. EX1003, ¶[163].

[1.5.2], [11.5.2]

“Request to Access the Memory”

Wang teaches that when a transaction request in the “*signal*” is received from the requesting device (as explained above in [1.5.1]), a user approves or disapproves the request. EX1004, 14:6-25, 10:13-22. Wang explains that “[i]n some cases, *the transaction approval data requires the inclusion of certain pieces of identification data* 302. For example, a transaction embodied in the transaction request from the electronic transaction system may be appended with data representative of an ‘electronic signature’ prior to being encrypted and retransmitted back to the electronic transaction system.” EX1004, 15:11-23, FIG. 3B. Wang also explains that transaction information, such as credit card information, is stored in the device memory, and, after user authentication, the credit card information is transmitted to the POS reader. EX1004, Abstract, 14:17-25, 15:11-24.



EX1004, FIG. 3B.

Recall from [1.3] that user identification data and a user's private key are written into the PEAD's memory. EX1004, 17:12-16; 18:31-33, 15:6-10; FIG. 6B – flash memory 656; 22:27-35.

A POSITA would have understood that for transactions that *require* “the inclusion of certain pieces of identification data 302,” the received transaction request would have obviously included a “*request to access the memory*” so that identification data and/or transaction information can be accessed from the memory to respond. EX1004, 15:11-23; EX1003, ¶¶[164]-[167].

US Patent No. 5,698,836 (“Fujioka”) corroborates this POSITA understanding. Fujioka explains that a memory can be divided into a user area UA (that stores personal information and account information) and a system area SA. EX1016, 5:14-34, FIG. 2. When a first device is seeking information from a second device with this memory, the first device sends a read command to request the second device to access its memory and provide the requested information. EX1016, 6:3-20. In the same manner, Wang's request for the inclusion of certain pieces of

identification data 302 in a response, would have been understood as an instruction to read the identification data from the memory of Wang's mobile device. EX1003, ¶[168].

Relatedly, for highly sensitive, encrypted transactions: 1) a received transaction request is encrypted and has to be decrypted by the PEAD, and 2) an approval response may be encrypted before being transmitted to the requesting device. EX1004, FIGS. 3A-4, 15:11-18:23. For instance, Wang explains that “[f]or highly sensitive transactions, however, the transaction requests may be encrypted and transmitted to PEAD 200 via data path 206 and input into decryption logic 402 to be decrypted.” EX1004, 16:13-18. “Once decrypted, the transaction request is then displayed to the user for approval. The transaction approval data may be furnished to encryption logic 300 ... to be encrypted if approved The encryption is preferably performed with the user's private key 304,” which is stored in memory 504. EX1004, 16:20-26, 18:31-19:12, 19:22-26, 14:33-15:10, 38:11-14, 40:5-8. Access to the memory for encryption or decryption purposes is controlled by the logic circuitry to prevent unauthorized access to the memory. EX1004, 19:27-20:11.

A POSITA would have understood that a received transaction request for a sensitive transaction would have obviously included *a request to access memory* locations where: 1) a decryption key is stored so that the received encrypted request can be decrypted, and 2) an encryption key is stored to encrypt a response to the

transaction request. EX1004, 15:24-29, 16:7-19, 16:20-26, 17:12-16, 18:31-33.
EX1003, ¶¶[169]-[170].

“[R]etrieve the transaction information”

As a preliminary matter, it would have been obvious that Wang’s PEAD would have to retrieve and return transaction information to the POS device (requesting device) in an electronic transaction system to complete a transaction. EX1003, ¶[171]. Thus, a POSITA would have understood that a signal received from the POS device would have obviously included a request to retrieve transaction information to complete the transaction. *Id.* Wang’s disclosure confirms the same.

Recall from [1.3] that Wang’s transaction information encompasses credit card information to be used in a credit card transaction and that Wang’s system is configured to “permit[] a user *to conduct a charge card transaction* vis-a-vis a charge card terminal of an electronic transaction system.” EX1004, Abstract. Recall from [1.5.1] that the transaction is conducted between Wang’s PEAD and a POS device (requesting device) in an electronic transaction system. EX1004, 3:26-4:9; 25:11-13, 10:13-22, 14:6-7, 25:19-24, FIG. 2. Thus, when the transaction request involves a transaction such as a “purchase from a vendor” having a POS device, it would have been obvious that the request would have requested payment information for the transaction including at least credit card information. EX1003, ¶[172]; EX1004, 1:23-35, 15:12-23.

Wang describes an example in which a credit card-based transaction is described. For instance, Wang discloses a “portable electronic charge/approval device (PECAD)” that includes “the aforementioned PEAD functionality to permit a user to approve a transaction vis-a-vis a PEAD-enabled point of sale terminal” and “permit[s] the user to conduct transactions vis-a-vis the existing charge card infrastructures. In particular, the complete PECAD system includes a PECAD and an associated emulation card which conforms to current charge card standards as far as its interface with existing charge card readers is concerned.” EX1004, 25:19-30. “The charge cards themselves may represent credit cards (such as Visa or Master Cards), ATM cards, royalty cards, discount cards, as well as any other type of cards with which a user may employ vis-a-vis a point-of-sale terminal to obtain cash, goods, and/or services.” EX1004, 25:33-26:6. “Prior to conducting a transaction, the PECAD has in its memory charge card data pertaining to one or more charge cards of the user. To perform the PEAD functionality, the memory may include other data items discussed earlier in connection with the PEAD.” EX1004, 26:7-10.

The charge/credit card information can be stored in a nonvolatile, tamper-proof memory that also stores the user’s private key. EX1004, 28:27-35, FIG. 9. Thus, a POSITA would have understood that charge/credit card information is stored

in memory 504 (when in a PEAD, or in memory 904 when used in a PECAD). EX1003, ¶¶[173]-[174].

Because the emulation card can be used “as if it were a charge card” and can emulate a number of charge cards, a POSITA would have understood that a transaction request would have included a request to access and provide charge/credit card information (“*retrieve the transaction information*”) to pay for the transaction. EX1004, 26:20-35; EX1003, ¶[175] (citing EX1012); EX1005, 22:57-23:48, 30:22-33.

Similarly, for transactions that require “the inclusion of certain pieces of identification data 302,” an electronic signature is obtained from the memory and included as part of a transaction response. EX1004, 15:11-23, FIG. 3B. A POSITA would have understood that the electronic signature is part of the “*transaction information*” at least because it is used to complete the transaction. EX1003, ¶[176] (citing EX1017). Accordingly, it would have been obvious to a POSITA that a transaction request (for a transaction that requires the inclusion of certain pieces of identification data 302) would have also included “*a request to ... retrieve the transaction information.*” EX1003, ¶[176].

Additional Disclosure Relevant to Ground 1A

Barnes “facilitate[s] commercial exchanges by wirelessly exchanging payment and product information with vendors.” EX1005, Abstract, 2:28-41, 3:53-

4:2. Payment information, including credit card or bank information, can be provided to a POS device using the commerce module and the short range wireless RF LAN module. EX1005, Abstract, 3:53-4:2, 7:3-24, 21:52-22:10, 29:39-46, 30:22-33. Barnes explains that data indicating the format type for a payment is provided by a vendor to the user, and the commerce module then selects a payment account and corresponding format that is acceptable to the vendor by retrieving the information from a memory. EX1005, 22:11-56. The commerce module then “formats the payment information data in a manner that is appropriate for the receiving computer system” and transmits the payment information to the desired destination. EX1005, 22:57-23:48, 30:22-33.

Accordingly, it would have been obvious to a POSITA that, in the Wang-Barnes combination, the request received from the requesting device would have included a request to *retrieve*, from the memory, *transaction information* such as payment information (e.g., credit card information) and format information to use when responding to the transaction request. EX1003, ¶¶[177]-[178].

Barnes describes an example scenario in which a vendor’s point of sale device sends a request to store vendor stored user information (VSUI) in the device or a request for identification information stored on the device when the device enters the vendor’s store. EX1005, 49:37-67. It would have been obvious to a POSITA that both requests would have involved a request to access the memory in the Wang-

Barnes device. EX1003, ¶[179]. For these additional reasons, Wang-Barnes render [1.5.2]/[11.5.2] obvious.

[1.6], [11.6]

As explained above in [1.1], each of the Wang-Barnes and Wang-Srey devices “*receive[s]*” fingerprint data (“*biometric data*”/“*fingerprint data*”) from the user authentication mechanism 612 (“*biometric input device*”/“*fingerprint scanner*”). EX1004, 22:14-25, 38:5-7, 40:27-28, FIG. 6A (reproduced below); EX1005, 17:38-48, 18:1-42, 21:1-14; EX1006, 2:46-67, 3:33-4:5, 4:49-6:16, FIGS. 2, 7.

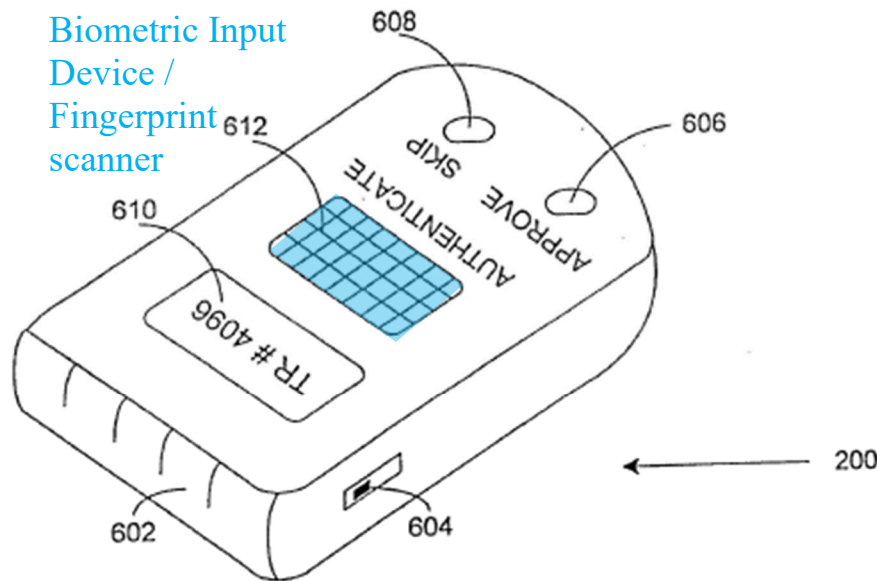


FIG. 6A

EX1004, FIG. 6A.

Wang teaches that user identification data, such as fingerprints, are never exposed and are only accessible to the logic circuitry (“*processor*”). EX1004, 19:27-20:11, 13:16-35, 22:18-25. And because the logic circuitry is the only processor in Wang’s PEAD it would have been obvious to a POSITA that the logic circuitry (“*processor*”) receives the biometric/fingerprint data from the biometric input device/fingerprint scanner for comparing, as further explained in the next section. EX1003, ¶¶[180]-[181]⁹.

[1.7], [11.7]

As explained in [1.1], Wang teaches that before approving a transaction, a user may be required to input the user identification data, such as fingerprints, for user authentication. EX1004, 22:14-25, 13:16-22, 24:24-32, 38:5-6, 40:27-28. Only after the user authentication is complete is the transaction approval sent. EX1004, 22:14-25, 24:24-32, 26:20-28. Such user identification data is stored in memory 504. EX1004, 22:14-25, 34:23-25, 14:26-15:24, 18:31-33. Recall from [1.6], that

⁹ Wang does not impose strict limits on when its fingerprint-based user authentication method leaving implementation of the method open to routine design choices known to a POSITA. EX1003, ¶[182]. For instance, to the extent a switch 210 should be activated to approve a transaction, the fingerprint matching can be performed before or after activation of the switch. EX1004, 11:5-22.

the logic circuitry (“*processor*”) receives the biometric data from the biometric input device. And because only the logic circuitry can access the memory 504 and user identification information, it would have been obvious that the logic circuitry (“*processor*”) performs the user authentication by comparing the received and stored fingerprints. EX1003, ¶¶[183]-[184]; *see* §V.A.7.(a).[1.6].

For the Wang-Barnes device under Ground 1A, Barnes teaches that fingerprint data is received through a fingerprint scanner and then compared to stored fingerprint data. EX1005, 18:13-18, 21:1-14.

For the Wang-Srey device under Ground 2A, Srey also teaches that fingerprints obtained through fingerprint scanner 115 are compared by processor 203 to stored fingerprints to authenticate a user. EX1006, 2:46-67, 3:33-4:5, 4:49-6:16, FIGS. 2, 7.

Accordingly, under both Wang-Barnes and Wang-Srey, a POSITA would have understood that fingerprint authentication involves the processor comparing received (via fingerprint scanner) user fingerprint data (“*fingerprint/biometric data*”) with fingerprint data (“*fingerprint/biometric information*”) stored in memory 504 (“*memory*”). EX1003, ¶¶[185]-[187].

[1.8], [11.8]

Specifically, Wang’s user authentication involving fingerprint matching, as explained above in [1.6]-[1.7]/[11.6]-[11.7], can be implemented and “employed for

approving transactions.” EX1004, 22:14-25. And once a user approves the transaction, an approval message is created with the user's identification data, encrypted and transmitted back to requesting device 202 via path 212.” EX1004, 11:5-22, FIG. 2 (reproduced below). As shown in Wang’s FIGS. 2 and 5A below, “data path 212 outputs transaction approval data from logic circuitry 502 [“*processor*”)] to the electronic transaction system.” EX1004, 19:13-26. An example of the transaction approval data is shown below in FIG. 3B. EX1004, 15:15-17.

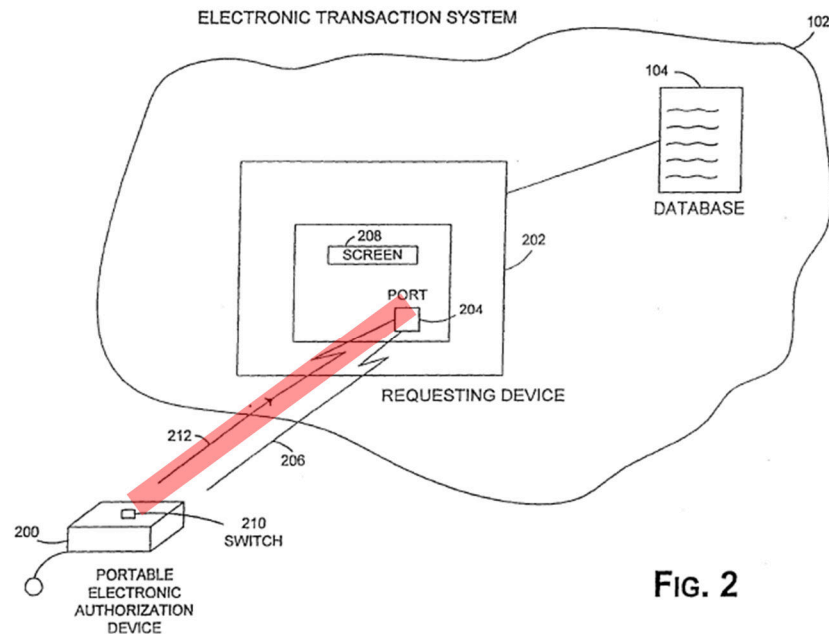
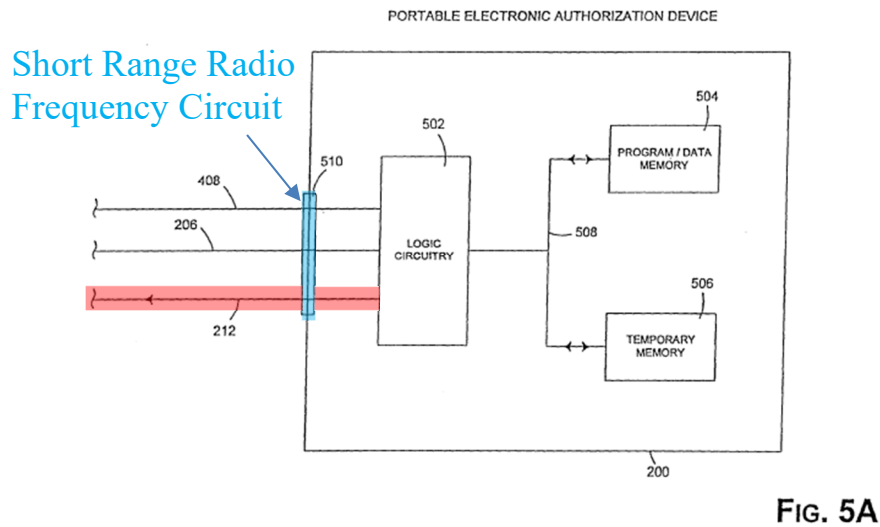
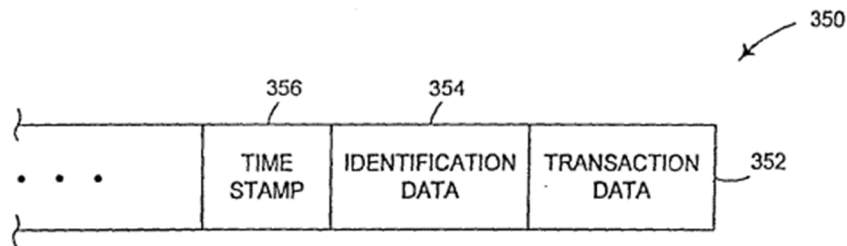


FIG. 2

EX1004, FIG. 2.



EX1004, FIG. 5A.



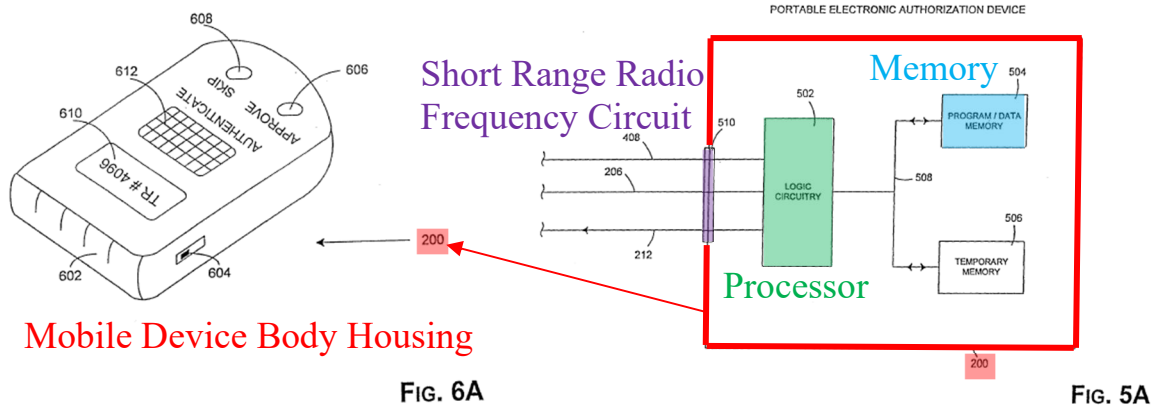
As explained above in [1.5.2] and shown in FIG. 3B above, the transaction information includes time stamp data, identification data, and transaction data such as credit card information, electronic signature and even the transaction ID, the merchant's name, the merchant's ID, and the time of the proposed purchase. EX1004, 15:11-23, 1:23-35, 10:13-23, FIG. 3B. For at least these reasons, Wang discloses the logic circuitry ("*processor*") being configured to "*transmit the*

transaction information to the point of sale terminal using the short range radio frequency circuit.” EX1003, ¶¶[188]-[190].

Recall from [1.6] and [1.7] that user authentication, involving fingerprint matching, is required for highly secure transactions in Wang, and that the transaction information is sent when the received and stored fingerprints match. EX1004, 22:14-32, 13:16-22, 38:5-6, 40:27-28, 26:20-28, FIG. 6A. Accordingly, Wang renders obvious that the transaction information is transmitted “*when the received biometric data matches the stored biometric information.*” EX1003, ¶[191].

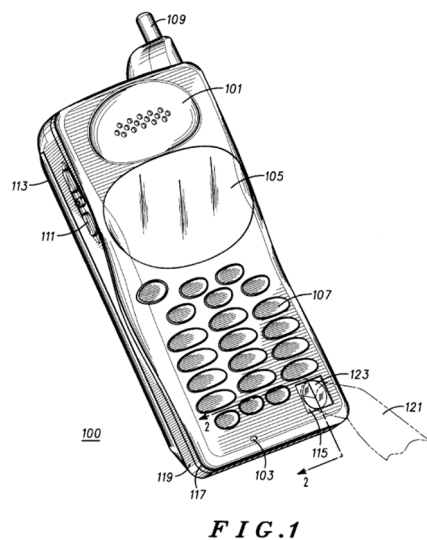
[1.9], [11.9]

Wang explains that the “PEAD 200 may be implemented using a general purpose portable computing device, such as any of the miniaturized portable computers or personal digital assistants (PDA's) that are currently popular.” EX1004, 20:21-24. FIG. 6A depicts an example external view of the PEAD in a mobile device body housing, and FIG. 5A shows that the PEAD houses the biometric input device, short range radio frequency circuit, memory, and processor. EX1004, 20:18-21:35.



EX1004, FIGS. 6A, 5A.

As explained above, in the Wang-Barnes and Wang-Srey combinations, Wang's mobile device is implemented as or part of a cellular phone. EX1003, ¶¶[192]-[194]. An example of a cellular phone housing is shown in Srey's FIG. 1 below, and a POSITA would have understood that the cellular phone body would have housed the biometric input device, short range radio frequency circuit, memory, and processor. *Id.*



EX1006, FIG. 1.

(b) Claim 19

Independent claim 19 differs from claims 1 and 11 in that the claimed device includes cellular circuitry (feature [19.1]) that is used to 1) receive a signal from a POS terminal (feature [19.6.1]), and 2) transmit the transaction information to a remote location, in place of a short range radio frequency circuit performing these operations (feature [19.9]). EX1003, ¶[195]. As explained below, Wang-Barnes and Wang-Srey still render claim 19 obvious.

[19.pre]

See [1.pre]/[11.pre]; EX1003, ¶[196].

[19.1]

Ground 1A

As explained above in §V.A.2, §V.A.5, and [1.1], the Wang-Barnes device is a cellular phone. EX1005, 4:27-30, 5:35-51, 7:48-50, 16:36-39, FIG. 1; EX1003, ¶[197]. The Wang-Barnes's cellular phone can communicate with multiple networks at the same time, including networks that a POSITA would have understood are cellular networks, such as 2G, 2.5G, 3G, and GSM networks. *Id.*; EX1005, 8:19-54, 9:51-12:49.

The Wang-Barnes's cellular phone includes ASICs and antennas to communicate with other networks, including the cellular networks noted above. EX1005, 6:1-14, 8:19-54, 9:7-50. Accordingly, it would have been obvious to a

POSITA that Wang-Barnes’s cellular phone includes “*cellular circuitry*” such as an ASIC and antenna. EX1003, ¶[198].

Ground 2A

Wang-Srey renders obvious [19.1] at least because Srey teaches that its cellular phone includes “cellular circuitry” such as a transmitter 205 and receiver 207 that are “mounted on the keypad printed circuit board 213” to facilitate cellular communications. EX1006, FIG. 2, FIG. 7, 4:49-5:10, 3:37-42; EX1003, ¶[199].

[19.2]

See [1.1]; EX1003, ¶[200].

[19.3]

Each of the cellular phones in the Wang-Barnes and Wang-Srey combinations include “*a short range radio frequency circuit.*” See [1.2]; EX1003, ¶[201] (noting that claim 19 does not require the short range radio frequency circuit to perform any operations).

[19.4]

See [1.3]; EX1003, ¶[202].

[19.5]

See [1.4]; EX1003, ¶[203].

[19.6.1]

Ground 1A

Barnes teaches that its device can communicate with multiple networks contemporaneously using its antennas, and that it can switch networks when one or more network switching conditions are present or a network is unavailable. EX1005, 9:25-10:36, 11:5-12:23. Examples of when network switching conditions occur include when a network fails, has reduced bandwidth, capacity, or availability, and experiences increased noise among numerous other conditions. EX1005, 11:5-12:23. When “more than one network may be operated by the same computer system,” the system determines which network the cellular phone should use for communications and switches networks accordingly. EX1005, 12:24-44. The networks can be chosen based on various factors such as available bandwidth, volume, capacity, and speed of data, communication capabilities, and more. EX1005, 11:20-31. For instance, if a short distance network, like a Bluetooth network, does not have sufficient bandwidth or capacity, communications can be carried over a cellular 3G network. EX1005, 11:33-62. Barnes describes an example of this situation when a user driving a vehicle initially communicates with a food vender’s point of sale device to place an order from a far distance and then establishes a new communication link when within a predetermined distance of the vendor’s restaurant to make the payment. EX1005, 29:4-30:33. Barnes explains

that communication can take place “irrespective of the distance from the place of commerce exchange” indicating that the communications encompass long distance cellular communications. EX1005, 29:39-50; EX1003, ¶[204].

Consistent with this example, it would have been obvious to a POSITA that when short range communication between a POS device and the Wang-Barnes cellular phone conducted through short range wireless RF LAN module is unavailable (or any other network switching condition is satisfied), the Wang-Barnes cellular phone would switch to another network to complete the transaction described above with respect to claims 1-18. EX1003, ¶[205]. Barnes explains that a WWAN network can be used for communication between its device and a POS device. EX1005, 7:16-24. Accordingly, because the Wang-Barnes device is a cellular phone that is configured to use cellular circuitry (such as ASIC and an antenna) to communicate across a cellular network, it would have been obvious to a POSITA that the Wang-Barnes device would have switched to the cellular network and used cellular circuitry to conduct communications with the POS device. EX1003, ¶[205]. When this switch happens, it would have been obvious to a POSITA that the logic circuitry (“*processor*”) in the Wang-Barnes cellular telephone “receive[s] a signal from a point of sale terminal via the cellular circuitry.”

Barnes discloses that its device can communicate with another device simultaneously through multiple networks, including, e.g., mobile 3G networks and

wireless LAN and PANs. EX1005, 9:40-45, 11:5-20. Communication across multiple networks can occur when a vendor or point of sale device does not know how far a user mobile/cellular device is from the point of sale device and therefore transmits a signal via the cellular circuitry to a cellular network, and to a short-distance LAN/PAN. EX1003, ¶[206]; EX1005, 16:63-17:36. In circumstances when the POS device and the Wang-Barnes cellular telephone are communicating with each other simultaneously across short range and long range (e.g., cellular) networks, it would have been obvious that the POS device would have transmitted signals simultaneously across both networks such that the Wang-Barnes cellular telephone “receive[s] a signal from a point of sale terminal via the cellular circuitry.” EX1003, ¶[206].

Ground 2A

Srey teaches that its receiver receives and demodulates received information. EX1006, 10:55-60, 5:57-67, FIGS. 2, 7. In the Wang-Srey cellular telephone, it would have been obvious that the receiver in the cellular circuitry would have received a signal from the requesting device (“*point of sale terminal*”), as explained above in [1.5.1] and shown below in Wang’s FIG. 2. EX1003, ¶[207]. Similar to the explanation above under the Ground 1A mapping of this feature, a signal from the POS terminal would have been received through the cellular circuitry instead of the short range radio frequency circuit in [1.5.1] when, e.g., short range

communication between a POS device and the Wang-Srey cellular phone conducted through short range wireless RF LAN module is unavailable (or any other network switching condition is satisfied), such that the Wang-Srey device utilizes the cellular network for POS communications. EX1003, ¶[207].

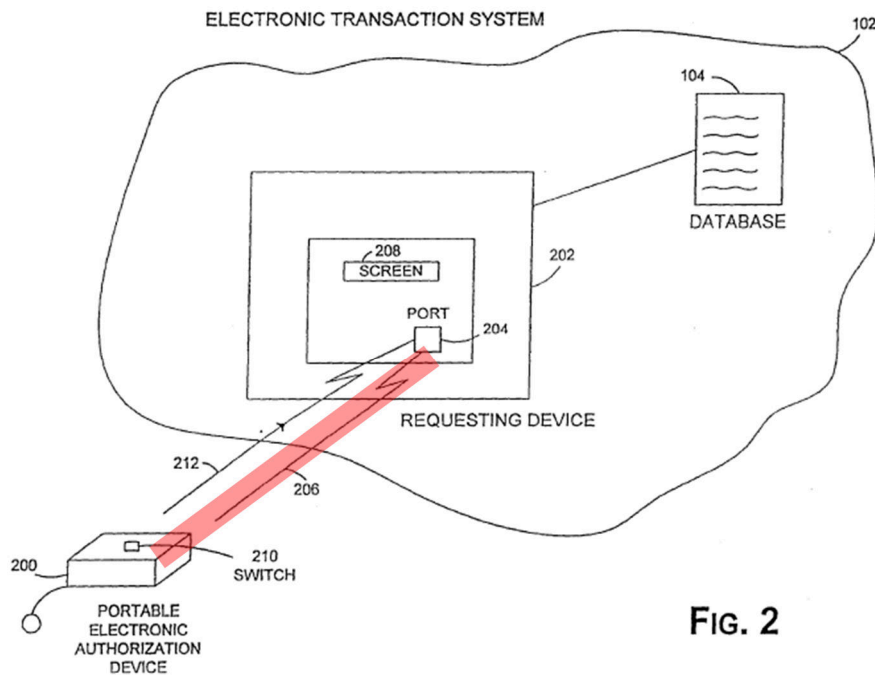


FIG. 2

EX1004, FIG. 2.

[19.6.2]

See [1.5.2]; EX1003, ¶[208].

[19.7]

See [1.6]; EX1003, ¶[209].

[19.8]

See [1.7]; EX1003, ¶[210].

[19.9]

Ground 1A

As explained in [19.6.1], communications between the Wang-Barnes cellular telephone and the POS device would have been performed using the cellular circuitry (ASIC and antennas used to communicate with a cellular network) when the short range network communications fail or a network switch condition is satisfied. EX1005, 9:25-10:36, 11:5-12:44, 29:4-30:3, 7:16-24. In these circumstances, the logic circuitry (“*processor*”) in the Wang-Barnes cellular telephone would have “*transmit[ed] the transaction information to a remote location*” associated with the POS device when the fingerprints match (instead of the short range radio frequency circuit as noted in the mapping of [1.8] above). EX1003, ¶[211].

In Wang, the POS is positioned at a “remote location” from the mobile/cellular device. EX1004, FIG. 2. This is consistent with the ’513 patent, which does not specify a particular distance associated with the “remote location,” but provides examples such as a cellular telephone approaching a RF reader/writer (e.g., when a user of the cellular phone is in a hotel), indicating that the RF reader/writer is located away from and not physically connected to the cellular telephone and is communicating wirelessly with the same. EX1001, 15:16-22. Moreover, it would have been obvious to a POSITA that the “*transaction*

information” would have been transmitted to a remote location, such as a remote location of the POS device, when the POS device and cellular telephone are communicating over a cellular network and are not within a short range of each other, having invoked the network switch condition to communicate via the cellular network, as explained above in [19.6.1]. EX1003, ¶[212].

The rest of the mapping of [1.8] applies here. EX1003, ¶[213].

Ground 2A

As explained in [19.6.1], communications between the Wang-Srey cellular telephone and the POS device would have been performed using the cellular circuitry (cellular transmitter) when the short range network communications fail or a network switch condition is satisfied. EX1005, 9:25-10:36, 11:5-12:44, 29:4-30:3, 7:16-24. Like in Ground 1A, it would have been obvious to a POSITA that the “*transaction information*” would have been transmitted to a remote location, such as a remote location of the POS device, when the POS device and cellular telephone are communicating over a cellular network and are not within a short range of each other, having invoked the network switch condition to communicate via the cellular network, as explained above in [19.6.1]. EX1003, ¶[214]. In these circumstances, the logic circuitry (“*processor*”) in the Wang-Srey cellular telephone would have “*transmit[ted] the transaction information to a remote location*” associated with

the POS device when the fingerprints match (instead of the short range radio frequency circuit as noted in the mapping of [1.8] above). EX1003, ¶[214].

The rest of the mapping of [1.8] applies here. EX1003, ¶[215].

[19.10]

See [1.9]; EX1003, ¶[216].

(c) Claim [2]

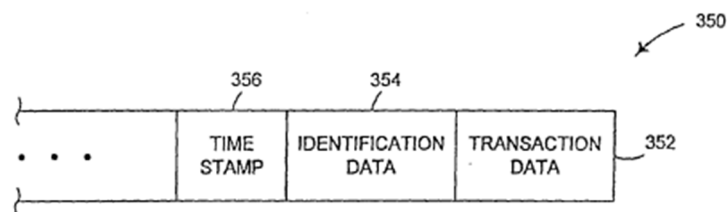
See [1.pre], [1.9]. EX1003, ¶[217].

(d) Claim [3]

See [1.1]. EX1003, ¶[218].

(e) Claims [4], [12], and [20]

Wang's FIG. 3B (reproduced below) illustrates "the format of representative transaction approval data." EX1004, 15:16-17.



EX1004, FIG. 3B.

Wang explains that "transaction data 352, representing a portion of or the entire transaction request received from the electronic transaction system, is appended with certain user identification data 354 and optionally a time stamp 356."

EX1004, 15:17–20. Wang adds that, “[o]nce appended, transaction approval data 350 is then encrypted prior to being retransmitted back to the electronic transaction system.” EX1004, 15:22–23. Wang further explains that the “user identification data ... may include ... unique identifying data such as fingerprint, DNA coding sequence, voice print, or the like.” EX1004, 13:19–22.

Wang's logic circuitry transmits, after encryption, the transaction approval data, in which the stored user identification data (which may include a fingerprint) is appended to the transaction data. EX1004, 13:19-22, 15:17-20, 11:5-30; §V.A.7.(a).[1.2]. Therefore, a POSITA would have understood that the processor transmits the stored biometric/fingerprint information together with the transaction information. EX1003, ¶¶[219]-[221].

(f) Claims [5], [13], and [21]

As explained in [1.3] and [1.5.2], the transaction information includes charge card information used to complete a transaction. EX1004, Abstract, 1:23-35, 15:12-23. Wang teaches that “[t]he charge cards themselves may represent credit cards (such as Visa or Master Cards), ATM cards, royalty cards, discount cards, as well as any other type of cards with which a user may employ vis-a-vis a point-of-sale terminal to obtain cash, goods, and/or services.” EX1004, 25:32-26:6, 33:16-18 (explaining that a bank can issue a PEAD). These cards typically store account

information related to the user. EX1003, ¶[222]; EX1004, 12:12-13, 16:5-6, 3:10-16.

A POSITA would have understood the stored charge-card information, e.g., an ATM card or credit card information, to be account information associated with the user's credit card account or bank account to enable transaction payment. EX1003, ¶[223]; EX1004, 12:12-13, 16:5-6, 3:10-16, 33:16-18.

(g) Claims [6], [14], and [22]

See [5]/[13]/[21]; EX1003, ¶[224].

(h) Claims [7], [15], and [23]

See [1.5.2], [1.3]; EX1003, ¶[225].

(i) Claims [8], [16], and [24]

See [1.5.2], [1.3]; EX1003, ¶[226].

(j) Claims [9], [17], and [25]

As explained in [1.7], in each of the Wang-Barnes and Wang-Srey devices, *“the processor is configured to compare the received biometric data with the biometric information stored in the memory.”* Claim 9 (and similarly claims 17 and 25) further notes that this comparison is *“in response to receiving the request to retrieve the transaction information.”*

Recall from [1.3], [1.5.1], and [1.5.2] that in response to a transaction request in the *“signal”* being received from requesting device requesting transaction

information (e.g., payment information) and user authentication is required to approve the transaction, Wang's user authentication mechanism 612 performs a fingerprint authentication procedure in which the user fingerprint is scanned and then compared to stored user fingerprint data in the memory. EX1004, 22:14-25, 38:5-7, 40:27-28, 14:16-25, 15:11-23, FIG. 3B. Accordingly, it would have been obvious to a POSITA that each of the Wang-Barnes and Wang-Srey devices performs the biometric data comparison "*in response to receiving the request to retrieve the transaction information.*" EX1003, ¶¶[227]-[228].

B. GROUNDS 1B AND 2B

1. Bashan

Bashan relates to "a data transaction device having an on-board processor for effecting both 'contact' and 'contactless' modes of data transfer." EX1007, 1:5-7. Bashan explains that where contactless transmission is used, "a coil antenna in the chip card is adapted to receive data from and transmit data to a reading device having a similar antenna." EX1007, 1:45-47. In the contactless mode, a clock output CLK signal "is set to a frequency equal to f_0/N where f_0 is the input frequency of the carrier signal typically equal to 13.56 MHz." EX1007, 9:13-15; EX1003, ¶[90].

2. Bashan Combined with Wang-Barnes or Wang-Srey

As explained above in §§V.A.5-6, the portable devices in the Wang-Barnes and Wang-Srey combinations are configured to operate across various

communication networks, including wireless wide area networks, such as cellular networks, and short range networks, such as Bluetooth or infrared. *See* §§V.A.5-6; EX1005, 7:3-8:55; EX1006, FIGS. 5, 9; 8:25-37, 9:39-67. Thus, a POSITA would have understood that the portable devices in both combination systems are configured to operate at various frequencies. EX1003, ¶¶[91]-[93]; EX1005, 7:3-24, 8:25-55; EX1006, FIG. 7, 9:39-67. Relatedly, Bashan teaches conducting a wireless transaction in its contactless mode using a carrier frequency f_0 of 13.56 MHz, which is firmly within the radio frequency spectrum. EX1007, Abstract, 4:11-65, 9:13-15; EX1003, ¶[94].

It would have been obvious to a POSITA that the short range radio frequency circuit in the Wang-Barnes device or the Wang-Srey device would have been configured to also operate in the 13.56 MHz. EX1003, ¶[95]. As explained below, doing so would have simply amounted to combining prior art elements according to known methods to yield predictable results. *KSR*, 550 U.S. at 415-421; *M.P.E.P.* §2143.

Dr. Nielson explains that 13.56 MHz was a highly used frequency for short range communication because it offered a good balance of wireless communication distance (e.g., a few centimeters to a meter) with a desirable data speed and power transfer within an internationally approved, license-free band. EX1003, ¶[96].

Thus, using it in the Wang-Barnes device or Wang-Srey device to realize the same benefits would have been an obvious choice for a POSITA. *Id.*

Although Bashan is directed to “a card,” using its teaching of conducting contactless communications at a frequency of 13.56 MHz would have been applicable to a cellular phone. EX1003, ¶[97]. Doing so would have involved modifying the operational configurations of the frequency synthesizer or modulator in Wang’s communication port 510 (the short range radio frequency circuit in the Wang-Barnes device and Wang-Srey device) to permit processing (including transmission and reception) of signals at 13.56 MHz. *Id.* Furthermore, using a cellular phone would still offer the benefits of contactless operation because cellular phone-based wireless transactions can be completed “without imposing the overhead incurred in manually introducing the smart card into the slot of a card reader.” EX1007, 1:23–24.

A POSITA would have had a reasonable expectation of success in combining Bashan with Wang-Barnes or Wang-Srey because, as noted above, Bashan’s 13.56 MHz frequency was a known frequency for the type of short range card-to-reader transactions Wang’s device carries out. EX1007, 9:13–15; EX1003, ¶[98]. Operating Wang’s wireless RF circuit at 13.56 MHz neither alters Wang’s principle of operation nor requires any redesign of Wang’s transaction flow; it merely specifies the frequency of the already-disclosed wireless RF link. *Id.*

3. Claim Element Analysis

(a) Claims [10], [18], and [26]

See §V.B.2. EX1003, ¶[229].

C. GROUND 3A

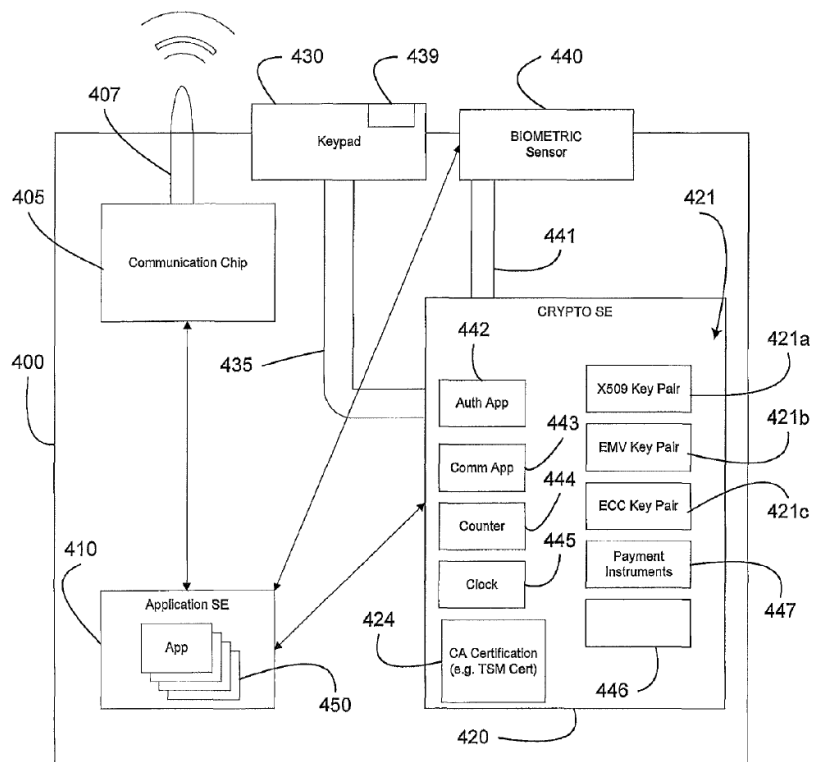
1. The '513 Patent's Priority Date is its Filing Date

The '513 patent issued from US Patent Application No. 15/372,317 (the "'317 application"), which was filed on 12/7/2016. EX1002, 476-568. The '513 patent claims priority to several earlier patents and ultimately to a provisional application filed on July 9, 2002. EX1001, 2. But none of the earlier patents or the provisional application provide support for the claimed features. EX1003, ¶[53].

Specifically, each of the independent claims of the '513 patent recites a processor that is configured to perform receive, compare, and transmit operations. *See e.g.*, [1.4]-[1.8], [11.4]-[11.8], [19.5]-[19.9]. A processor or CPU is only mentioned at 20:23-36 and 21:43-63 of the specification (in addition to the claims section), but none of these sections describe a processor performing the claimed operations. The processor-related features were first recited at the time the '317 application was filed. Because the claimed subject matter was first introduced into the application as of the filing date (12/7/2016), the earliest priority date that the '513 patent should be accorded is 12/7/2016. EX1002, 526; EX1003, ¶¶[54]-[55].

2. Mardikar

Mardikar is directed to conducting secure financial transactions between a personal electronic device, such as a mobile or cellular telephone, and a point of sale device using contactless technology. EX1009, Abstract, 1:15-2:43. Mardikar utilizes a Point of Sale (POS) system including a client device 400 and a retailer or merchant server 210. EX1009, 4:27-5:22. The client device 400 is “a mobile phone, cellular phone” that includes “a communication chip 405, an antenna 407, secure elements 410, 420, ... and a biometric sensor 440.” EX1009, 6:42-50, FIG. 4 (reproduced below); EX1003, ¶¶[99]-[100].



EX1009, FIG. 4.

The communication chip 405 supports “one or more modes of communication, including, for example, Near Field Communication (NFC), Bluetooth, infrared, GSM, UMTS and CDMA cellular phone protocols, SMS and Internet access via a mobile network or local network.” EX1009, 6:50-55. Mardikar explains that NFC “is a short-range, high frequency, wireless communication technology” and that Mardikar’s device is “compatible with Near Field Communication Point of Sale devices (NFC POS) located at the point of sale at a vendor’s place of business.” EX1009, 6:50-7:3.

Mardikar’s biometric sensor 440 is “a finger/thumb-print sensor,” and captured biometric data is tunneled directly to a payment/credential secure element (the “Crypto SE” 420). EX1009, 7:28-43, 11:30-12:30, FIG. 6a. A biometric authentication application 442 resident on the Crypto SE “evaluate[s] the biometric data and compare[s] the data to data from a registered user.” EX1009, 9:60-65; 15:55-16:45, 11:30-12:30, FIG. 6a; EX1003, ¶¶[100]-[115].

3. Cooke

Cooke discloses conducting contactless payment transactions between a proximity payment device and a proximity reader incorporated with a point-of-sale terminal. EX1010, Abstract, ¶¶[0003]-[0004], [0014]-[0017]. Cooke’s teaches that a proximity payment device is not limited to a card: “mobile telephones, personal digital assistants (PDAs), tablet computers, laptop computers, and the like can be

equipped with integrated circuitry having the same functionality as the RFID IC of a contactless payment card,” thereby “turning such mobile devices into contactless payment devices.” EX1010, ¶¶[0004], [0016], [0021], [0025], [0041], [0050]; EX1003, ¶¶[116]-[117].

Cooke discloses the POS-initiated request/response operation that governs such transactions: “the payment circuit of the proximity payment device is configured to respond to an interrogation signal from an NFC reader by transmitting payment account information such as a payment card account number (PAN) or other identifying data.” EX1010, ¶[0025], FIGS. 2-3. “The RF reader transmits an interrogation signal and then listens for a response signal and/or message from the RFID circuitry of the proximity payment device.” EX1010, ¶[0025]; EX1003, ¶[118].

4. Combination of Mardikar and Cooke

A POSITA would have combined Mardikar and Cooke such that:

- 1) Mardikar’s biometrically-secured mobile/cellular device would have been configured to respond to a POS-incorporated NFC reader’s interrogation signal, as taught by Cooke; and
- 2) Mardikar’s device would have returned its stored transaction information (e.g., payment instrument / account number) in response to that

interrogation signal, as taught by Cooke, gated by Mardikar's on-device biometric authentication.

EX1003, ¶[119].

Mardikar's mobile/cellular device captures a fingerprint, compares it against a stored biometric signature on the Crypto SE, and — only upon a match — transmits a secure payment message containing the payment instrument to an NFC POS reader. EX1009, 6:42-10:24, 11:29-12:43, 15:53-16:45 (cl. 1), FIGS. 6a, 6c. Mardikar does not dwell on the reader-side signaling that initiates the exchange. EX1003, ¶[120].

Cooke supplies that reader-side detail. Cooke expressly teaches that the proximity reader is “conventionally incorporated with a Point-of-Sale (POS) terminal” and transmits an interrogation signal, and that the payment circuit of the proximity payment device “respond[s] to an interrogation signal from an NFC reader by transmitting payment account information such as a payment card account number (PAN) or other identifying data.” EX1010, ¶¶[0003], [0025], FIGS. 2-3. Cooke further teaches that the responding proximity payment device may be a payment-enabled mobile telephone. EX1010, ¶¶[0004], [0016], [0021], [0025], [0041], [0050]; EX1003, ¶[121].

A POSITA would have predictably combined Mardikar and Cooke for the following reasons.

First, both references are directed to NFC contactless payment in the same ecosystem (ISO 14443 / NFC / PayPass), and Cooke expressly names payment-enabled mobile telephones as the proximity payment device. EX1009, 6:50-7:3; EX1010, ¶¶[0003], [0025], [0029]. Configuring Mardikar's mobile/cellular device to answer a standard POS NFC interrogation, as taught by Cooke, would have made Mardikar's device interoperable with the widely-deployed contactless-POS infrastructure that Cooke describes. EX1003, ¶¶[122]-[123].

Second, the combination is nothing more than the use of a known technique (Cooke's reader-initiated interrogation/response) to improve a similar device (Mardikar's NFC-enabled mobile/cellular device) in the same way it improves contactless payment cards, yielding the predictable result of a POS-initiated, device-response transaction. EX1003, ¶[124]; *KSR*, 550 U.S. at 415-421.

Third, the combination would have had a reasonable expectation of success because Mardikar's device already includes the NFC communication chip 405 and antenna 407 used to receive an interrogation signal and transmit a response, and Cooke's interrogation/response operation is the conventional PayPass/ISO 14443 exchange those components are designed to perform. EX1009, 5:34-7:26; EX1010, ¶¶[0003], [0025], [0029]; EX1003, ¶[125].

5. Claim Element Analysis

(a) Claims 1 and 11

[1.pre], [11.pre]

Mardikar discloses a client device 400 “such as a mobile phone, [or] cellular phone.” EX1009, Abstract, 6:42-50, FIG. 4; EX1003, ¶[230].

[1.1], [11.1]

The Mardikar-Cooke Combination (“**MCC**”) renders obvious [1.1]/[11.1] at least because Mardikar’s device 400 (“*mobile device/cellular telephone*”) includes a biometric sensor 440 (“*biometric input device*”/“*fingerprint scanner*”) that receives “*biometric/fingerprint data*.” EX1003, ¶[231].

Mardikar’s device 400 includes a biometric sensor 440 that “may be any sensor that provides data representative of a unique, biological user attribute that may be used to identify a user, for example a finger/thumb-print sensor, retina scan or voice identifier.” EX1009, 6:43-50, 7:28-32, FIG. 4 (reproduced below). A user “input[s] their biometric identifying data (ID) or signature by placing or swiping a thumb or finger on biometric sensor 440.” EX1009, 11:44-55, FIG. 6a; EX1003, ¶[232].

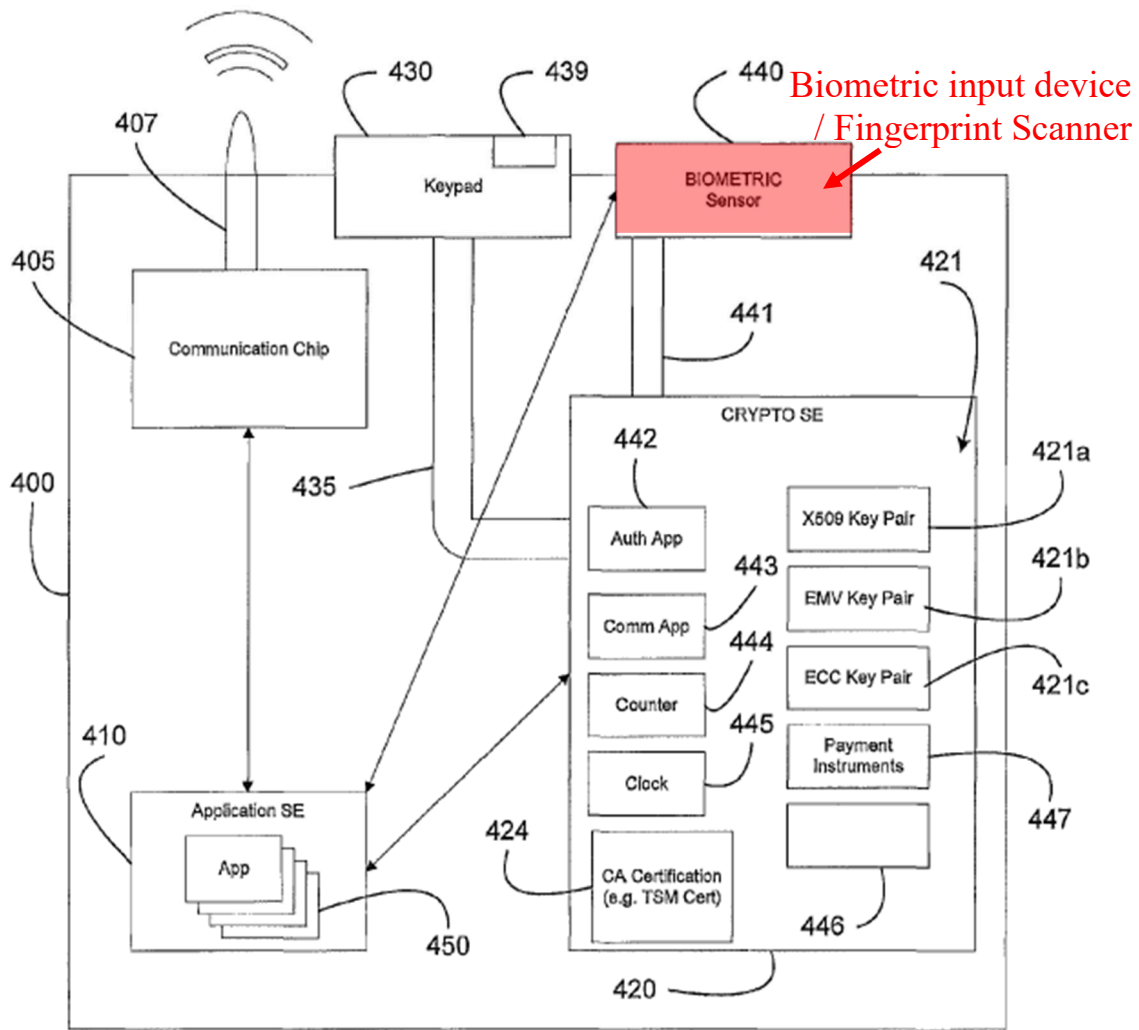


FIG. 4

EX1009, FIG. 4.

[1.2], [11.2]

MCC renders obvious [1.2]/[11.2] at least because the MCC client device includes RF (NFC) circuitry such as a communication chip 405 and antenna 407

(collectively “*a short range radio frequency circuit*”). EX1009, FIG. 4; EX1003, ¶[233].

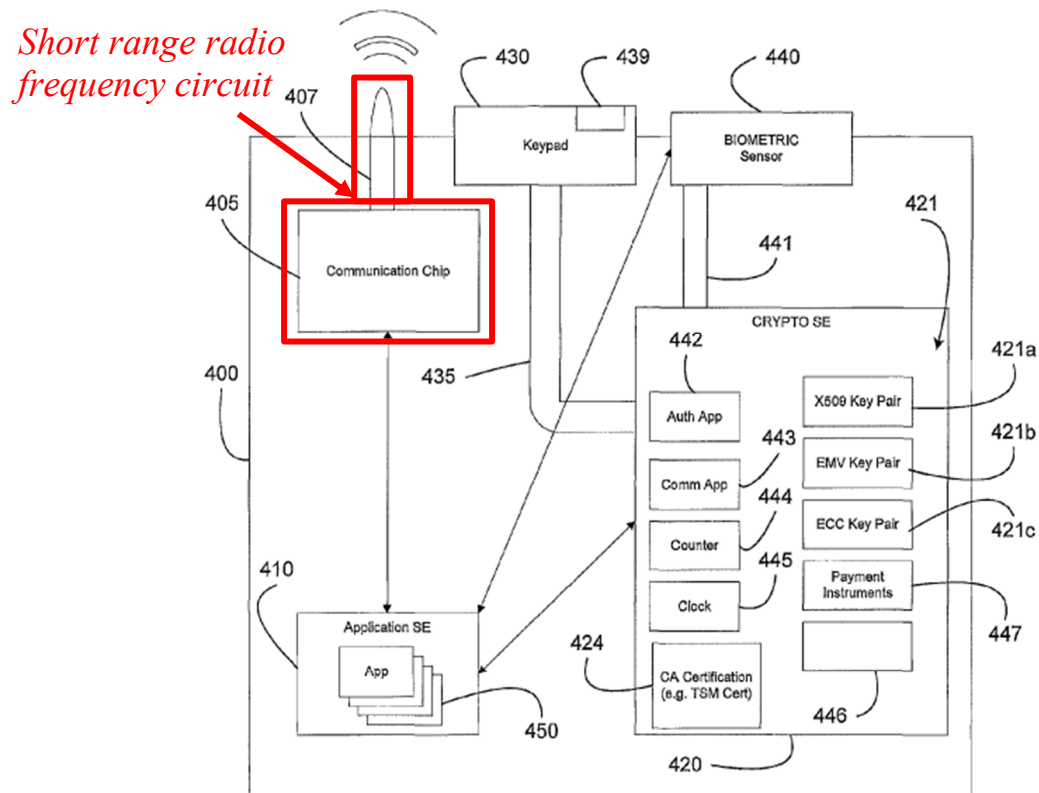


FIG. 4

EX1009, FIG. 4.

Mardikar’s communication chip “support[s] one or more modes of communication, including, for example, Near Field Communication (NFC),” which is “a short-range, high frequency, wireless communication technology” used to exchange data that employ radio frequencies, such as RFIDs. EX1009, 6:43-67.

Cooke also teaches that short range RF (NFC) circuitry can be used in the proximity payment device to communicate with the POS reader. EX1010, ¶¶[0003], [0025]. Thus, a POSITA would have understood that, in MCC, the communication chip and antenna are used to facilitate RF communications with a POS device/reader. EX1003, ¶[234]; EX1010, ¶[0003], ¶[0025].

[1.3], [11.3]

Mardikar's SE 420 includes a data storage, and is used "for loading and storing authentication data 446 (for example a PIN or biometric signature), payment instruments 447, certificates 424, crypto keys 421 ... including ... unique biometric authentication information related to a specific user." EX1009, 9:36-47, 7:44-63, FIG. 4. Mardikar also discloses registering a user based on biometric attribute information such as thumbprint or fingerprint and using the authentication application 442 (part of the Crypto SE 420) to compare biometric data with the registered biometric data (e.g., thumbprint or fingerprint). EX1009, 9:60-65, 10:41-62, 11:44-12:3. After the user's biometric identification is authenticated, a payment (credit card information) associated with the user can be made. EX1009, 9:60-65, 10:41-62, 11:44-12:3. Accordingly, it would have been obvious to a POSITA that the data storage ("***memory***") in Mardikar's Crypto SE 420 stores fingerprint data to identify the user associated with the transaction information ("***biometric/fingerprint***

information for identifying an individual associated with transaction information”). EX1003, ¶¶[235]-[236].

[1.4], [11.4]

As a preliminary matter, Mardikar’s mobile device and computer system include one or more processors, that are interconnected with other system elements such as memory through “a bus or other communication mechanism,” and the processor executes the operations described in Mardikar. EX1009, 14:20-15:51 (“[l]ogic may be encoded in a computer readable medium, which may refer to any medium that participates in providing instructions to the processor for execution.”) At least for this reason (and the reasons noted in §V.C.4), it would have been obvious to a POSITA that Mardikar, in combination with Cooke, teaches [1.4]/[11.4] and the recited operations in [1.5.1]-[1.8]/[11.5.1]-[11.8]. EX1003, ¶¶[237]-[238].

Additionally, Mardikar teaches that the SE 420 may be a smart card or smart card-like chip embedded inside device 400. EX1009, 7:45-57. “The smart card itself may contain a CPU and some non-volatile storage.” EX1009, 7:45-57. Mardikar’s “authentication application 442, for example a biometric authentication application, may reside on the Crypto SE 420 and may evaluate the biometric data.” EX1009, 9:60-65. “[B]iometric signature data from the biometric sensor 440 may be tunneled through a biometric tunneling circuit 441, directly to the Crypto SE 420.” EX1009, 7:37-40.

It would have been obvious to a POSITA that: (1) a processor, such as CPU, in SE 420, would have performed the biometric data comparison/evaluation as part of the biometric authentication conducted by the authentication application 442 in SE 420; (2) the CPU in SE 420 would have been directly or indirectly coupled to the memory/storage within SE 420 e.g., to perform the biometric data comparison; and (3) the CPU and memory within SE 420 are coupled to the biometric sensor 440 (“*biometric input device/fingerprint scanner*”), as shown in Mardikar’s FIG. 4. EX1003, ¶¶[239]-[240]; EX1009, 7:37-40, 9:60-65, 16:31-32, FIG. 6a.

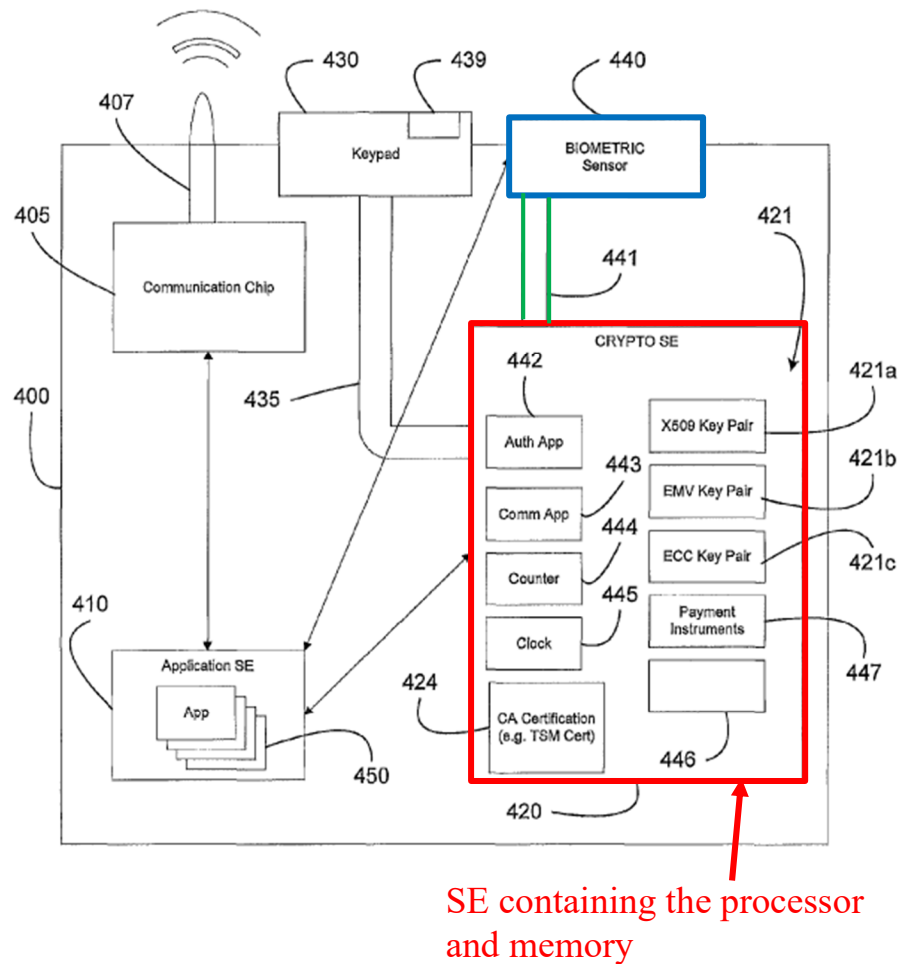


FIG. 4

EX1009, FIG. 4.

As explained below in [1.5.1]-[1.8]/[11.5.1]-[11.8], Mardikar's processor also performs the recited operations in [1.5.1]-[1.8]/[11.5.1]-[11.8].

[1.5.1], [11.5.1]

Recall from [1.2] that Mardikar's device 400 communicates with a POS device to secure financial transactions at an NFC POS" using MCC's RF NFC circuitry, including a communication chip 405 and antenna 407, that corresponds to

the claimed “*short range radio frequency circuit.*” EX1009, 6:43-67, 3:30-33, FIG. 4; EX1010, ¶¶[0003], [0025]; EX1003, ¶¶[241]-[243].

Cooke teaches “the RF reader transmits an interrogation signal [to a proximity payment device such as a payment-enabled mobile telephones] and then listens for a response signal and/or message from the RFID circuitry of the proximity payment device.” EX1010, ¶¶[0003], [0025], [0028], FIGS. 2-3. “[T]he payment circuit of the proximity payment device is configured to respond to [the] interrogation signal from an NFC reader by transmitting payment account information.” EX1010, ¶[0025].

Because (1) Cooke expressly identifies payment-enabled mobile telephones as the responding proximity payment device; (2) Cooke explains that RF readers were incorporated with a POS Terminal; and (3) the payment device receives an interrogation signal from the RF reader, a POSITA would have understood that, in the combination, MCC’s mobile/cellular device 400 “*receive[s] a signal from a point of sale terminal via the short range radio frequency circuit.*” EX1010, ¶¶[0003], [0016], [0025]; EX1003, ¶[244]. Indeed, because MCC’s device is “compatible with Near Field Communication Point of Sale devices (NFC POS)” and includes the NFC communication chip and antenna, a POSITA would have recognized that the interrogation signal would have been received through the

MCC's NFC communication chip and antenna. EX1009, 6:67-7:3, FIG. 4; EX1003, ¶¶[244]-[245].

Recall that in the MCC system, payment information is sent in response to the interrogation signal. EX1010, ¶[0025], FIGS. 2-3. The payment instruments 447 are stored in MCC's SE 420 along with other certificates and keys (e.g., crypto keys 421) needed to communicate with other devices. EX1009, 9:37-47, 10:17-40. Accordingly, it would have been obvious that the processor in SE 420 receives the interrogation signal and processes it to determine and obtain the payment information needed to respond. EX1009, 14:20-15:5; EX1003, ¶[246].

[1.5.2], [11.5.2]

As noted above in [1.5.1], Cooke teaches that the NFC RF reader transmits an interrogation signal and “the payment circuit of the proximity payment device is configured to respond to an interrogation signal from an NFC reader by transmitting payment account information such as a payment card account number (PAN) or other identifying data” that is stored on the device. EX1010, ¶¶[0003], [0025], [0028]. Relatedly, Mardikar teaches that the transaction information (e.g., payment information, account number) is stored in the Crypto SE memory and is read out and provided for transmission upon authorization. EX1009, 9:37-47 (“load[s] and stor[es] authentication data 446 (for example a PIN or biometric signature), payment instruments 447, certificates 424, crypto keys 421 and other security-related

information”), 11:8-27, 12:22-30, 13:16-37, FIGS. 5b, 6a. Accordingly, it would have been obvious to a POSITA that the interrogation signal received from the RF reader in the MCC system includes “*a request to access the memory and retrieve the transaction information.*” EX1010, ¶¶[0003], [0025]; EX1003, ¶¶[247]-[248].

[1.6], [11.6]

Mardikar teaches that a user “input[s] their biometric identifying data (ID) or signature by placing or swiping a thumb or finger on biometric sensor 440,” and “[t]he input biometric ID may be directly sent or tunnelled to Crypto SE 420.” EX1009, 11:44-12:3, FIG. 6a (steps 606-608). As explained in more detail below in [1.7]/[11.7], it would have been obvious that the processor in SE 420 “*receive[s]*” fingerprint data (“*biometric/fingerprint data*”) from the biometric sensor 440 (“*the biometric input device*”/“*fingerprint scanner*”) to perform a comparison. EX1009, 14:20-15:5; EX1003, ¶¶[249]-[250].

[1.7], [11.7]

As explained in [1.3], Mardikar’s SE 420 includes data storage that stores registered biometric attribute information such as thumbprint or fingerprint. EX1009, 9:36-47, 7:44-63, FIG. 4. After receiving the fingerprint data (“*biometric/fingerprint data*”) from the biometric sensor 440, this data is compared with the stored biometric/fingerprint data. EX1009, 9:60-65, 10:41-62, 11:44-12:3, 16:30-33 (cl. 1). It would have been obvious to a POSITA that for SE 420 to receive

and compare registered and received biometric/fingerprint data, the processor in SE 420 would have performed these operations. EX1003, ¶¶[251]-[252]; *see* [1.4], [1.5.1]; EX1009, 14:20-15:5.

[1.8], [11.8]

As explained above in [1.2] and [1.5.1]-[1.5.2], in response to the interrogation signal, payment information is sent using the RF (NFC) circuitry, which in the MCC includes Mardikar's communication chip and antenna. EX1010, ¶¶[0003], [0021], [0025], FIGS. 2, 3. Mardikar teaches that, for security reasons, the information is sent after biometric authentication by virtue of fingerprint matching is performed. EX1003, ¶¶[253]-[254]. In particular, Mardikar teaches "generating a secure payment information message in response to an authentication including a match of the biometric data with the stored biometric signature ... the secure payment information message includes the payment instrument; and transmitting the secure payment information message to a POS reader by ... near field communication (NFC)." EX1009, 16:30-33 (cl. 1), FIG. 6a. Mardikar further teaches that, once authenticated, "the App SE 410 may then send the payment information ... to the communication chip 405 for further transmission or transport to a reader ... located at the POS, for example a POS NFC reader." EX1009, 11:55-12:30, FIG. 6a (steps 612-614). Because the processor in the SE 420 is performing the biometric authentication (using Auth App 442 in SE 420) and obtains payment

information from payment instruments 447 (also located in SE 420), it would have been obvious to a POSITA, that the processor in MCC's SE 420 would have transmitted the transaction information to the POS NFC reader ("*to the point of sale terminal*") using communication chip and antenna ("*short range radio frequency circuit*") "*when the received biometric/fingerprint data matches the stored biometric/fingerprint information.*" EX1003, ¶[254]; EX1009, 14:20-15:5.

[1.9], [11.9]

MCC renders obvious [1.9]/[11.9] at least because Mardikar's device 400 houses the biometric sensor 440, the NFC communication chip 405/antenna 407, the secure-element memory, and the CPU. EX1003, ¶[255]. For example, Mardikar's device 400 "include[s] a communication chip 405, an antenna 407, secure elements 410, 420, a keypad 430 and a biometric sensor 440," and describes the SEs 410, 420 as containing a CPU and being "embedded inside device 400, for example inside of a cell phone." EX1009, 6:42-7:65, FIG. 4; EX1003, ¶[255].

(b) Claim 19

[19.pre]

See [1.pre]; EX1003, ¶[256].

[19.1]

Mardikar's communication chip "supports one or more modes of communication, including, for example, Near Field Communication (NFC),

Bluetooth, infrared, GSM, UMTS and CDMA cellular phone protocols, SMS and Internet access via a mobile network or local network.” EX1009, 6:43-67. Accordingly, in the context of claim 19 and its dependent claims, a POSITA would have understood that Mardikar’s communication chip is also “*cellular circuitry*” that facilitates communications with mobile/cellular networks. EX1003, ¶[257].

[19.2]

See [1.1]; EX1003, ¶[258].

[19.3]

MCC’s cellular phone includes “*a short range radio frequency circuit.*” See [1.2]. Note that because the communication chip can support different communications, including NFC, the communication chip, alone or in combination with the antenna, also corresponds to “*a short range radio frequency circuit.*” EX1003, ¶[259]. Thus, MCC renders obvious [19.3].

[19.4]

See [1.3]; EX1003, ¶[260].

[19.5]

See [1.4]; EX1003, ¶[261].

[19.6.1]

As a preliminary matter, MCC renders obvious [19.6.1.] for the same or similar reasons as in [1.5.1] because Mardikar's communication chip 405 operates as the cellular circuitry and the short range radio frequency circuit. EX1003, ¶[262].

In addition, Mardikar teaches that a user can complete a transaction with a merchant/service provider having a POS device over a mobile network such as Sprint, Verizon or other mobile network service providers. EX1009, 5:34-6:12, FIG. 3. This flexibility (of using a cellular/mobile network in addition to NFC networks) is particularly helpful in the "ever changing electronic communications environment." EX1009, 6:1-12; 4:32-36, 5:55-61. Cooke explains that the NFC protocol is only used "in some payment application implementations" indicating that its disclosure is applicable beyond NFC communications. EX1010, ¶¶[0003], [0001], [0021].

Accordingly, it would have been obvious to a POSITA that when multiple communication networks are available for communication, the MCC cellular phone would have conducted the transaction with the POS device using a cellular network and its cellular circuitry in addition to or in place of short distance communication. EX1003, ¶¶[263]-[264]; *see* §V.A.7.(b).[19.6.1]. In such an event, it would have been obvious to a POSITA that cellular circuitry would have been used for receiving an interrogation signal from a point of sale terminal and also transmitting any

response back. EX1003, ¶[264]; EX1009, 1:45-2:28. Because Mardikar’s communication chip is configured to support multiple modes of communication, including NFC communications and cellular communications, the cellular circuitry in the communication chip would have been configured to receive an interrogation signal. EX1003, ¶[264]. For this additional reason, MCC renders obvious [19.6.1].

[19.6.2]

See [1.5.2]; EX1003, ¶[265].

[19.7]

See [1.6]; EX1003, ¶[266].

[19.8]

See [1.7]; EX1003, ¶[267].

[19.9]

MCC renders obvious [19.9] for at least the reasons noted above in [1.8] and [19.6.1] (explaining that cellular circuitry would have been used to transmit responsive information). EX1003, ¶[268].

Moreover, Mardikar teaches that “payments and financial transactions may be made using secure SMS communication,” in which the Crypto SE “generate[s], encrypt[s], and send[s] encrypted [messages] to the TSM” over the cellular channel. EX1009, 13:38-49. “When fully authenticated by the PIN and/or the biometric signature, the Crypto SE 420 may send the payment information to the App SE 410

for forwarding via NFC or other communication mode.” EX1009, 13:14-29. Because the secure-SMS transport carries the payment information over the cellular circuitry to a remote location (e.g., the TSM/server) after biometric authentication, MCC renders obvious “*transmit the transaction information to a remote location using the cellular circuitry when the received fingerprint data matches the stored fingerprint information.*” EX1009, 13:14-49; EX1003, ¶[269]. The remainder of the mapping of [1.8] otherwise applies. *Id.*

[19.10]

See [1.9]; EX1003, ¶[270].

(c) Claim [2]

See [1.pre]; EX1003, ¶[271].

(d) Claim [3]

See [1.1]; EX1003, ¶[272].

(e) Claims [5], [13], and [21]

See [1.5.2], [1.3]; EX1003, ¶[273].

(f) Claims [6], [14], and [22]

Mardikar teaches that credit cards are used for payments and that the Service providers in its system include banks and credit card issuers. EX1009, 1:45-67, 3:53-56, 6:15-41, 13:3-15. “In an example embodiment, the Crypto SE 420 may be certified, for example by a credit processing company such as MasterCard or VISA,”

and Crypto SE 420 stores the security key pairs for several cards, Europay, MasterCard, VISA. EX1009, 10:5-24. A POSITA would have understood that Mardikar's system is configured in the above-noted manner, e.g., with credit card issuers as service providers and SE 420 storing security keys for credit cards, so that Mardikar's device is used to make credit card payments to complete a transaction. EX1003, ¶[274].

Consistent with Mardikar, Cooke teaches that payment information, including e.g., MasterCard account number, is provided to the POS terminal in response to the interrogation signal to conduct a wireless transaction. EX1010, ¶¶[0003], [0025], [0016], [0034]. Accordingly, in the MCC system, when transaction information is sent to the card reader, the transaction information includes payment information such as credit card information to complete the transaction. EX1003, ¶¶[275]-[276]; *see* [1.3], [1.5.2].

(g) Claims [7], [15], and [23]

See [1.5.2]; EX1003, ¶[277].

(h) Claims [8], [16], and [24]

Mardikar's single SE 420 stores both the authentication data 446, such as fingerprint data ("*biometric information*") and the payment information ("*transaction information*"). *See* [1.3], [1.5.2], [7]. Thus, it would have been

obvious to a POSITA that the same memory in SE 420 stores the “*biometric information*” and the “*transaction information*.” EX1003, ¶[278].

(i) Claims [9], [17], and [25]

As explained above in [1.5.1]-[1.8], a processor in SE 420 receives an interrogation signal from Cooke’s NFC reader, and responds with transaction information. EX1010, ¶¶[0003], [0025]. However, for security reasons, Mardikar teaches that in preparation for a payment, biometric authentication is performed to authentication the user. EX1009, 11:44-12:30, 16:30-33 (cl. 1), FIG. 6a. Biometric authentication involves a comparison of the received fingerprint data with stored fingerprint data, as explained in [1.7]. Accordingly, it would have been obvious to a POSITA that, in the MCC system, the biometric authentication is performed in response to receiving the interrogation signal that requests retrieval of the transaction information. EX1003, ¶[279].

D. GROUND 3B

1. Lee

Lee is directed to a mobile phone that conducts NFC communications with an external RF reader at 13.56 MHz. EX1011, 5:30-48, 6:27-50. For example, the RF antenna in the mobile phone operates at 13.56 MHz. EX1011, 6:27-50, 7:53-65; EX1003, ¶[126].

2. Lee Combined with Mardikar and Cooke

It would have been obvious for a POSITA looking to implement the NFC communications described in the MCC system to turn to Lee's teachings to determine which frequency (13.56 MHz) to use for conducting the NFC communications performed between the mobile/cellular device and the POS device. EX1003, ¶¶[127]-[128]. Doing so would have simply amounted to combining prior art elements according to known methods to yield predictable results. EX1003, ¶[129]; *KSR*, 550 U.S. at 415-421; M.P.E.P. §2143.

Combining the teachings of Lee with MCC would have been predictable with a reasonable expectation of success for several reasons. EX1003, ¶[130].

First, using Lee's 13.56 MHz frequency would have been an obvious choice for a POSITA because 13.56 MHz was a well-known ISO 14443A standard frequency used for NFC communications. EX1003, ¶[131].

Second, like the MCC system, Lee describes using an RF antenna for near field communications between a mobile device and a RF reader. EX1011, Abstract, 5: 207:65. The MCC system would only have to be predictably modified to the extent of configuring its short range communication settings and components to use 13.56 MHz. EX1003, ¶[132]. Doing so would have been consistent with Mardikar's system, which is already designed to support various networks, and a routine

modification well within the capabilities of a person of ordinary skill in the art.
EX1009, 6:43-67; EX1003, ¶[132].

3. Claim Element Analysis

(a) Claims [10], [18], and [26]

See §V.D.2. EX1003, ¶[280].

VI. CONCLUSION AND FEES

The Challenged Claims are unpatentable. Petitioner authorizes charge of fees to Deposit Account 06-1050.

VII. MANDATORY NOTICES

A. Real Party-In-Interest

Apple Inc., Samsung Electronics Co., Ltd., and Samsung Electronics America, Inc. are the real parties-in-interest.

B. Related Matters

Petitioners are not aware of any disclaimers, reexamination certificates or petitions for inter partes review for the '513 Patent. The '513 Patent is the subject of civil actions *Mobility IP Holdings, Inc. v. Apple Inc.*, No. 7:26-cv-00075 (W.D. Tex. Mar. 4, 2026) and *Mobility IP Holdings, Inc. v. Samsung Electronics Co, Ltd. and Samsung Electronics America, Inc.*, No. 2:26-cv-157 (E.D. Tex. Feb. 27, 2026).

C. Lead And Back-Up Counsel

Petitioners provide the following designation of counsel.

Lead Counsel	Backup counsel
W. Karl Renner, Reg. No. 41,265 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email: IPR50095-0312IP1@fr.com	Andrew B. Patrick, Reg. No. 63,471 Usman A. Khan, Re. No. 70,439 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 IPR50095-0312IP1@fr.com

D. Service Information

Please address all correspondence and service to the address listed above.

Petitioner consents to electronic service by email at IPR50095-0312IP1@fr.com.

Respectfully submitted,

Dated: September 18, 2026

/W. Karl Renner/
W. Karl Renner, Reg. No. 41,265
Andrew B. Patrick, Reg. No. 63,471
Usman A. Khan, Re. No. 70,439
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. IPR2026-00503)

Counsel for Petitioners

CERTIFICATION UNDER 37 C.F.R. §42.24

Under the provisions of 37 C.F.R. §42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter partes* Review totals 13,909 words, which is less than the 14,000 allowed under 37 C.F.R. §42.24.

Dated: September 18, 2026

/W. Karl Renner/

W. Karl Renner, Reg. No. 41,265
Andrew B. Patrick, Reg. No. 63,471
Usman A. Khan, Re. No. 70,439
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

Counsel for Petitioners

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on September 19, 2026, a complete and entire copy of this Petition for *Inter partes* Review, Power of Attorney, and all supporting exhibits were provided via Federal Express, to the Patent Owner by serving the correspondence address of record as follows:

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101
(619) 238-1900

/Crena Pacheco/
Crena Pacheco
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
pacheco@fr.com