

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Francisco Martinez de Velasco Cortina, et al.
U.S. Patent No.: 8,933,807
Issue Date: January 13, 2015
Appl. Serial No.: 14/028,469
Filing Date: September 16, 2013
Title: SYSTEM AND METHOD FOR PROVIDING SECURE
TRANSACTIONAL 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. 8,933,807
PURSUANT TO 35 U.S.C. §§ 311-319, 37 C.F.R. § 42

TABLE OF CONTENTS

I.	REQUIREMENTS FOR IPR—37 C.F.R. §42.104.....	1
A.	Grounds for Standing—37 C.F.R. §42.104(a).....	1
B.	Challenge and Relief Requested—37 C.F.R. §42.104(b)	1
II.	THE '807 PATENT	2
A.	Summary	2
B.	Prosecution History.....	4
III.	LEVEL OF ORDINARY SKILL	6
IV.	CLAIM CONSTRUCTION—37 C.F.R. §42.104(b)(3)	7
V.	THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	7
A.	Ground 1A: Maes Renders Obvious Claims 1-3, 5-6, 8-11, 13, 15-20, 23	8
1.	Maes (EX1004)	8
2.	Claim Element Analysis.....	11
B.	Ground 1B: Maes-Dorf Renders Obvious Claims 4, 12, and 21	41
1.	Dorf (EX1009)	41
2.	The Maes-Dorf Combination (MDC)	42
3.	Claim Element Analysis.....	44
C.	Ground 1C: Maes-Shults Renders Obvious Claims 7, 14, and 22	45
1.	Shults (EX1008).....	45
2.	The Maes-Shults Combination (MSC).....	46
3.	Claim Element Analysis.....	49
D.	Ground 2A: Walker-Maes Renders Obvious Claims 1-3, 5-6, 8-11, 13, 15-20, 23	50
1.	Walker (EX1007)	50
2.	The Walker-Maes Combination (WMC)	51
3.	Claim Element Analysis.....	57
E.	Ground 2B: Walker-Maes-Dorf Renders Obvious Claims 4, 12, and 21... ..	77
1.	The Walker-Maes-Dorf Combination (WMDC)	77
2.	Claim Element Analysis.....	77
F.	Ground 2C: Walker-Maes-Shults Renders Obvious Claims 7, 14, and 22	78
1.	The Walker-Maes-Shults Combination (WMSC).....	78
2.	Claim Element Analysis.....	78
VI.	PAYMENT OF FEES—37 C.F.R. §42.103.....	79

VII.	MANDATORY NOTICES—37 C.F.R. § 42.8(a)(1)	79
A.	Real Party-In-Interest—37 C.F.R. § 42.8(b)(1)	79
B.	Related Matters—37 C.F.R. § 42.8(b)(2)	79
C.	Lead And Back-Up Counsel—37 C.F.R. § 42.8(b)(3)	79
D.	Service Information	80

LIST OF EXHIBITS

EX1001	U.S. Patent No. 8,933,807 to de Velasco Cortina, et al. (the “’807 Patent”)
EX1002	The Prosecution History of the ’807 Patent (the “Prosecution History”)
EX1003	Expert Declaration of Seth Nielson, Ph.D.
EX1004	U.S. Patent No. 6,016,476 to Maes et al. (“Maes”)
EX1005-1006	RESERVED
EX1007	U.S. Patent No. 6,163,771 to Walker et al. (“Walker”)
EX1008	U.S. Patent App. Pub. No. 2002/0011519 to Shults (“Shults”)
EX1009	U.S. Patent No. 6,000,608 to Dorf (“Dorf”)
EX1010-1023	RESERVED
EX1024	U.S. Patent No. 6,850,147 to Prokoski (“Prokoski”)
EX1025	U.S. Patent No. 6,175,922 to Wang (“Wang”)
EX1026-1029	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](https://www.uscourts.gov/sites/default/files/document/fcms_na_distprofile0630.2026.pdf)

LISTING OF CLAIMS

Element	Claim Language
[1.pre]	A mobile device, comprising:
[1.1]	Radio Frequency (RF) cellular circuitry;
[1.2]	short range RF circuitry;
[1.3.1]	memory configured to store biometric authentication information and transaction information,
[1.3.2]	wherein the biometric authentication information has been previously associated with the transaction information;
[1.4]	a biometric reading device configured to read biometric information;
[1.5]	an authentication module configured to authenticate that the biometric information read by the biometric reading device is associated with the transaction information based at least in part on the biometric authentication information stored in memory; and
[1.6.1]	a transaction module configured to provide the transaction information via the short range RF circuitry for use in a transaction
[1.6.2]	when the biometric information read by the biometric reading device is successfully authenticated as being associated with the transaction information by the authentication module.
[2]	The mobile device of claim 1, wherein the biometric reading device is a fingerprint reading device.
[3]	The mobile device of claim 1, wherein the transaction information is generated based at least in part on credit card information.
[4]	The mobile device of claim 1, wherein the transaction information is generated based at least in part on rewards card information.

[5]	The mobile device of claim 1, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.
[6]	The mobile device of claim 5, wherein the security block is a cryptographic block.
[7]	The mobile device of claim 1, wherein the short range RF circuitry includes a radio frequency identification (RFID) device.
[8]	The mobile device of claim 1, wherein the transaction module configured to provide the transaction information but not the biometric information via the short range RF circuitry for use in the transaction.
[9.pre]	A mobile device, comprising:
[9.1]	Radio Frequency (RF) cellular circuitry;
[9.2]	short range RF circuitry;
[9.3.1]	memory configured to store biometric authentication information and transaction information,
[9.3.2]	wherein the biometric authentication information has been previously associated with the transaction information;
[9.4]	a biometric reading device configured to read biometric information;
[9.5]	an authentication module configured to authenticate that the biometric information read by the biometric reading device is associated with the transaction information based at least in part on the biometric authentication information stored in memory;
[9.6.1]	a transaction module configured to provide the transaction information via the short range RF circuitry for use in a transaction
[9.6.2]	when the biometric information read by the biometric reading device is successfully authenticated by the authentication module

	as being associated with the transaction information by the authentication module; and
[9.7]	a security block configured to secure the transaction information before it is provided by the transaction module.
[10]	The mobile device of claim 9, wherein the biometric reading device is a fingerprint reading device.
[11]	The mobile device of claim 9, wherein the transaction information is generated based at least in part on credit card information.
[12]	The mobile device of claim 9, wherein the transaction information is generated based at least in part on rewards card information.
[13]	The mobile device of claim 9, wherein the security block is a cryptographic block.
[14]	The mobile device of claim 9, wherein the short range RF circuitry includes a radio frequency identification (RFID) device.
[15]	The mobile device of claim 9, wherein the transaction module configured to provide the transaction information but not the biometric information via the short range RF circuitry for use in the transaction.
[16.pre]	A cellular telephone, comprising:
[16.1]	Radio Frequency (RF) cellular circuitry;
[16.2]	short range RF circuitry;
[16.3.1]	memory configured to store biometric authentication information and transaction information,
[16.3.2]	wherein the biometric authentication information has been previously associated with the transaction information;
[16.4]	a biometric reading device configured to read biometric information;

[16.5]	an authentication module configured to authenticate that the biometric information read by the biometric reading device is associated with the transaction information based at least in part on the biometric authentication information stored in memory; and
[16.6.1]	a transaction module configured to provide the transaction information for use in a transaction
[16.6.2]	when the biometric information read by the biometric reading device is successfully authenticated by the authentication module as being associated with the transaction information by the authentication module.
[17]	The cellular telephone of claim 16, wherein the biometric reading device is a fingerprint reading device.
[18]	The cellular telephone of claim 17, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.
[19]	The cellular telephone of claim 18, wherein the security block is a cryptographic block.
[20]	The cellular telephone of claim 16, wherein the transaction information is generated based at least in part on credit card information.
[21]	The cellular telephone of claim 16, wherein the transaction information is generated based at least in part on rewards card information.
[22]	The cellular telephone of claim 16, wherein the short range RF circuitry includes a radio frequency identification (RFID) device.
[23]	The cellular phone of claim 16, wherein the transaction module configured to provide the transaction information but not the biometric information via the short range RF circuitry for use in the transaction.

Apple Inc. (“Apple”) and Samsung Electronics Co., Ltd. (“Samsung”) (collectively, “Petitioners”) petition for IPR of claims 1-23 (“Challenged Claims”) of U.S. Patent No. 8,933,807 (“the ’807 Patent”) assigned to Mobility IP Holdings, Inc. (“Patent Owner” or “Mobility”).

I. REQUIREMENTS FOR IPR—37 C.F.R. §42.104

A. Grounds for Standing—37 C.F.R. §42.104(a)

Petitioners certify that the ’807 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—37 C.F.R. §42.104(b)

Petitioners request an IPR of the Challenged Claims on the grounds set forth in the table below, and request that each of the Challenged Claims be found unpatentable for the reasons described within the Petition and the supporting evidence cited herein, including the Declaration of Seth Nielson, Ph.D. (EX1003, ¶¶1-34, 37-50, 295-296, *generally*).

Ground	Claims	Prior Art Basis
1A	1-3, 5-6, 8-11, 13, 15-20, 23	§103 - Maes (EX1004)
1B	4, 12, 21	§103 - Maes in view of Dorf (EX1009)

1C	7, 14, 22	§103 - Maes in view of Shults (EX1008)
2A	1-3, 5-6, 8-11, 13, 15-20, 23	§103 - Walker (EX1007) in view of Maes
2B	4, 12, 21	§103 - Walker in view of Maes and Dorf
2C	7, 14, 22	§103 - Walker in view of Maes and Shults

The '807 Patent was filed on September 16, 2013 and claims priority to several earlier-filed applications, the earliest of which was filed on July 9, 2002. As shown below, each of the references applied in Grounds 1A-2C qualifies as prior art even if the July 9, 2002 date is taken as the date of the alleged invention of the Challenged Claims. Without conceding that the Challenged Claims are entitled to its priority claims, this Petition nonetheless treats July 9, 2002 as the “Critical Date” of the claimed subject matter for purposes of the analysis herein.

Reference	Filed	Published	Pre-AIA Prior Art Basis
Maes (EX1004)	01/16/1998	01/18/2000	§102(a), (b), (e)
Shults (EX1008)	05/03/2001	01/31/2002	§102(a), (e)
Dorf (EX1009)	07/10/1997	12/14/1999	§102(a), (b), (e)
Walker (EX1007)	08/28/1997	12/19/2000	§102(a), (b), (e)

II. THE '807 PATENT

A. Summary

The '807 Patent “generally relates to a system and method for providing secure identification solutions, and specifically to a system and method for verifying

and tracking identification information.” EX1001, 1:7-12 (describing the “Field of the Invention”). EX1003, ¶¶51-58.

As shown in the '807 Patent's Fig. 1 (reproduced below), a “General RF Identification System and Method of Use” may include, for example, “an RF device 110 connected to or embedded on an RF identification mechanism 105, and an RF reader/writer 125. The RF device 110 includes a chip 115 and an RF antenna 120.” EX1001, 2:3-9.

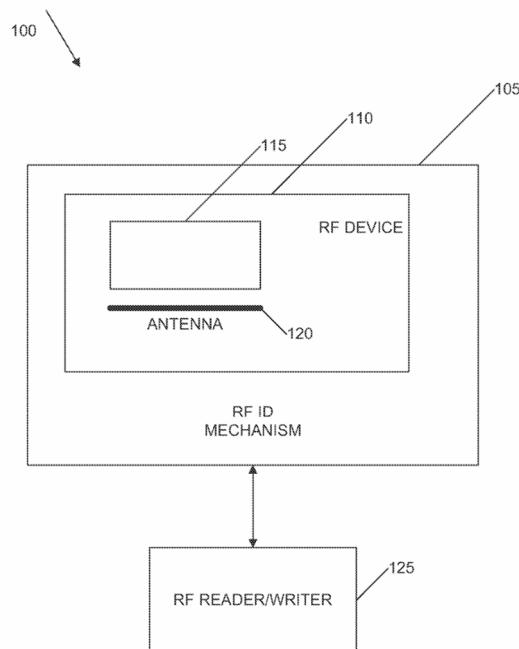


FIG. 1

EX1001, Fig. 1.

In an embodiment that is “discussed in the context of an RF cellular telephone,” the “RF communication device creates a communication through a

network to a point of sale (“POS”),” for example, “by a wireless RF device that stores a person’s identification information, and can thus become a person’s identification ‘document.’” EX1001, 13:6-16.

“As a user with an RF cellular telephone approaches a POS with an RF reader/writer, the RF reader/writer identifies the user and obtains any relevant information stored on the RF cellular telephone.” EX1001, 13:17-20. “The user is then asked to enter authentication information (*e.g.*, a fingerprint),” and [a]n exchange of information via the RF reader/writer and the RF cellular telephone results in verification that the authentication information matches the RF cellular telephone information.” EX1001, 13:20-26.

The “RF cellular telephone can [thus] be used as a substitute for credit cards, transforming the cellular telephone into the media of commercial transactions and transform telephony into the identification media for commercial establishments or authorities” EX1001, 13:43-49.

B. Prosecution History

During prosecution of the application for the ’807 Patent, the examiner issued a series of office actions rejecting the presented claims as obvious over multiple references. In one of these office actions (mailed August 8, 2014), the examiner rejected the claims under §103 over U.S. Patent No. 6,850,147 to Prokoski (“Prokoski”, EX1024) in view of U.S. Patent No. 6,175,922 to Wang (“Wang”,

EX1025). *See* EX1002, 50-65. The applicant responded by amending limitations into the independent claims requiring that:

(i) “the biometric authentication information has been previously associated with the transaction information” such that the authentication module is configured to “authenticate that the biometric information ready by the biometric reading device is associated with the transaction information,” and

(ii) the transaction module is configured to provide the transaction information “via [] short range RF circuitry.” EX1002, 35-39.

The applicant explained the amendments as follows:

The device can compare the biometric information input by the user with the stored biometric authentication information, which has already been associated with the transaction information. As such, verification of the user’s identity allows the device to also authenticate the user’s authorization with respect to the stored transaction information.

EX1002, 41.

In its response, the applicant represented to the examiner that the applied prior art failed to teach the features of the amended claims because the prior art’s authentication operations were either not performed on the mobile device or the prior art “biometric information only authenticates the user with respect to the PEAD ...

in order to verify that the user is authorized to use the device” rather than “used to indicate approval of the transaction.” *Id.*, 42-43.

The examiner subsequently allowed the application. EX1002, 8-14. The examiner’s reasons for allowance asserted that the prior art of record failed to teach multiple limitations of the allowed claims including “authenticating that the biometric information input by a user corresponds to the biometric authentication information associated with the transaction information.” *Id.*, 13.

The examiner’s decision to allow the application at this juncture, however, was in error. Indeed, the examiner failed to identify other highly relevant prior art later cited during prosecution of applications in the ’807 Patent family, including Maes (EX1004) and Walker (EX1007). Grounds 1A-2C of this Petition show that the ’807 Patent never should have issued. EX1003, ¶¶59-66.

III. LEVEL OF ORDINARY SKILL

A person of ordinary skill in the art (“POSITA”) relating to the ’807 Patent’s subject matter 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 professional experience for education. *Id.*

IV. CLAIM CONSTRUCTION—37 C.F.R. §42.104(b)(3)

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.

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

Claim Term	Construction
“transaction information” (Claims 1, 3, 4, 5, 8, 9, 11, 12, 15, 16, 18, 20, 21, 23)	“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 Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011); EX1003, ¶¶67-69. Petitioners reserve the right to respond to any construction offered by Patent Owner or adopted by the Board.

V. THE CHALLENGED CLAIMS ARE UNPATENTABLE

Grounds 1A-2C below demonstrate that the Challenged Claims of the ’807 Patent would have been obvious to a POSITA before the Critical Date based on

¹ The parties have not yet exchanged terms for construction in the district court action that Patent Owner initiated against Petitioner Samsung in E.D. Texas.

Maes, and on prior-art combinations involving Maes, Walker, Shults, and Dorf. Each of these references is analogous art in the same field as the '807 Patent (*e.g.*, secure transactions and communications) and/or reasonably pertinent to problem(s) purportedly addressed by the '807 Patent (*e.g.*, verifying or authenticating users in secure transactions). *See* EX1001, Abst., Figs. 12-17; EX1004, 1:10-17; EX1008, [0003], [0009], [0030], Abst.; EX1007, 1:6-10, 3:59-4:4, Abst.; EX1009, Abst., 1:24-35 (“secure environment”), 7:5-9; EX1003, ¶80.

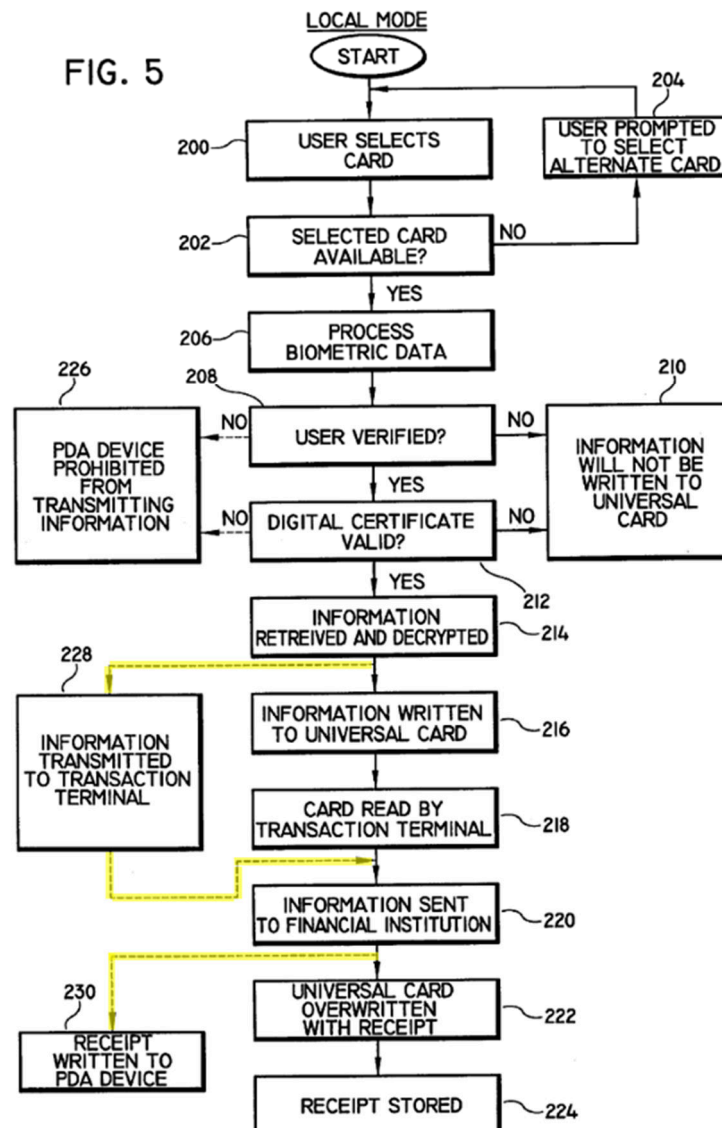
A. Ground 1A: Maes Renders Obvious Claims 1-3, 5-6, 8-11, 13, 15-20, 23

1. Maes (EX1004)

Maes describes a “portable information and transaction processing device,” such as a “portable client PDA” that “provide[s] direct communication capability with peripheral devices (such as POS [point-of-sale] ... terminals) ... through wireless communications such as radio frequency (RF) ... communication.” EX1004, Abstract, 4:16-28, 4:65-6:27, Fig. 1.

In some embodiments, “[t]he PDA includes a Universal Card, which is [a] common generic smartcard with a unique imprint provided by a service provider, on which selected financial or personal information stored in the PDA can be downloaded to perform certain consumer transactions.” EX1004, Abstract; *see also id.*, 4:29-30, 5:24-35. Maes emphasizes, however, “that the invention may interact

with electronic fund transfer systems or transaction terminals having wireless or direct communication capabilities without even having to use the Universal Card 26.” EX1004, 12:5-8. “Specifically, as demonstrated by the dotted lines in Fig. 5” (reproduced below), “the consumer transaction may be performed by transmitting the selected card information directly from the PDA device to the ... POS transaction terminal through an established communication link” EX1004, 12:8-13.



EX1004, Fig. 5 (highlighting added).

“Upon biometric verification ... selected card information” is “used to initiate a consumer transaction.” EX1004, Abstract. Fig. 5 depicts operations in the local mode of operation. EX1004, Fig. 5 (“LOCAL MODE”). However, in the absence of an “unexpired digital certificate” no transaction will take place. EX1004, Abstract; *see also id.*, 12:55-13:5; *see also* 6:56-7:35, Fig. 3.

“The local mode of operation is commenced by the user selecting a pre-enrolled credit card that is stored in memory 14 (step 200).” EX1004, 10:31-34. “If the requested card information is found in memory, biometric verification must be performed ...” EX1004, 10:50-52. “If the user is verified, the digital certificate (previously obtained in the client/server mode) is retrieved from memory 14 and loaded into the digital certificate processor module 20,” which “determine[s] whether the digital certificate is still valid” (*i.e.*, unexpired); if so, “the requested card information is then retrieved from memory 14 and stored in the encrypter/decrypter module 24,” which decrypts the selected card information “using an encryption key unique to the PDA device 10 (step 214).” EX1004, 11:15-32. “The decrypted card information is then sent to the smartcard reader/writer 30 where it is then written to the Universal Card 26,” which can then be “removed from the smartcard reader/writer 30 and swept through the magnetic reading device of the transaction terminal 80 (Fig. 3) (step 218).” EX1004, 11:32-37.

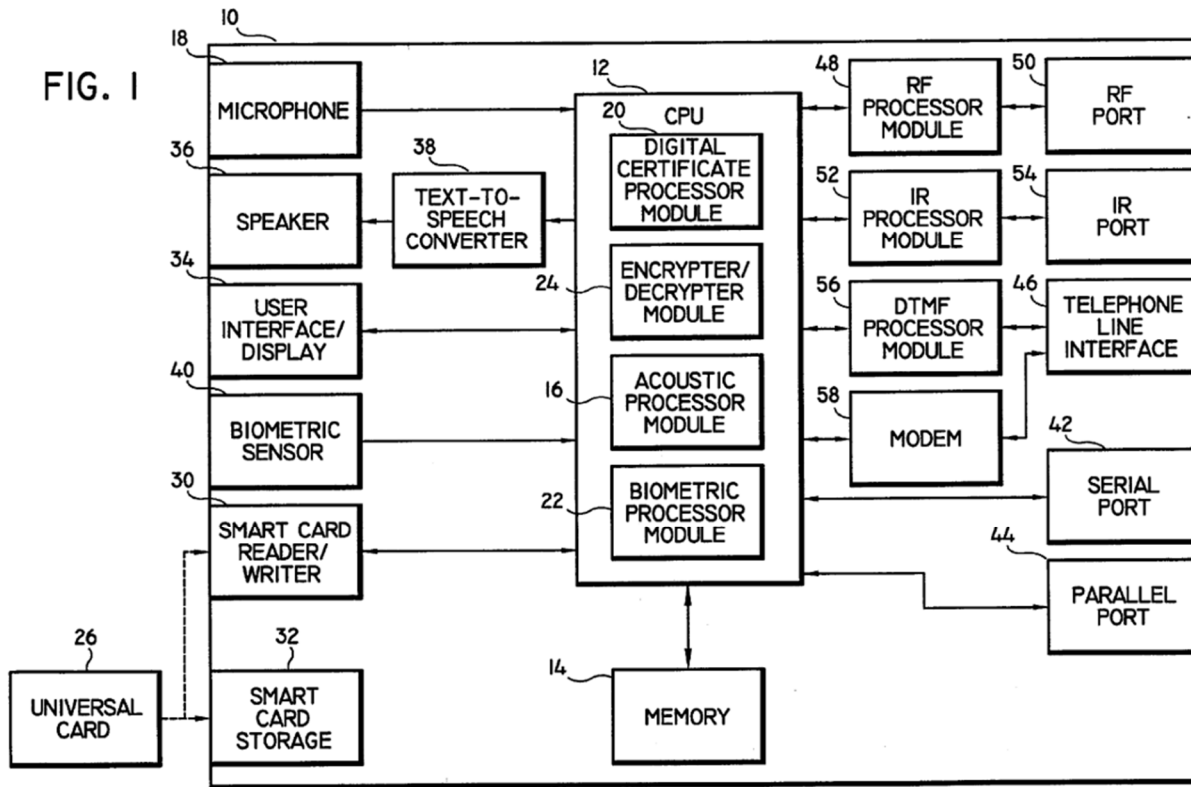
Alternatively, “the consumer transaction may be performed by transmitting the selected card information directly from the PDA device to the ... POS transaction terminal through an established communication link L2 (step 228, Fig. 3)” EX1004, 12:9-14, Figs. 1, 3, 5.

2. Claim Element Analysis

(a) [1.pre]

Maes renders [1.pre] obvious. EX1003, ¶¶118-120.

Maes discloses a “portable client PDA” (*mobile device*), *e.g.*, PDA device 10 depicted in Fig. 1 below and embodied in a “cellular phone.” EX1004, Abstract, 4:65-6:27, 14:12-16 (“the functions and components of the PDA device 10 may be built into a cellular phone”); EX1003, ¶119.



EX1004, Fig. 1; EX1003, ¶119.

Maes's PDA "provide[s] direct communication capability with peripheral devices (such as POS ... terminals) and is capable of transmitting or receiving information through wireless communications such as radio frequency (RF) ... communication." EX1004, Abstract; *see also id.*, 6:8-19, 12:5-29, Fig. 3.

(b) [1.1]

Maes renders [1.1] obvious. EX1003, ¶¶121-123.

Maes explains that its *mobile device* may be implemented as a cellular phone using cellular communication protocols, expressly disclosing that "the functions and

components of the PDA device 10 may be built into a cellular phone, whereby communication with the central server 60 may be achieved through a cellular communication channel, which may be analog or digital (e.g., CDMA, GSM, etc.).” EX1004, 14:12-17.

From these and related descriptions, a POSITA would have understood that Maes’s mobile device includes “*RF cellular circuitry*” that allows it to establish “communication ... through a cellular communication channel.” EX1003, ¶123.

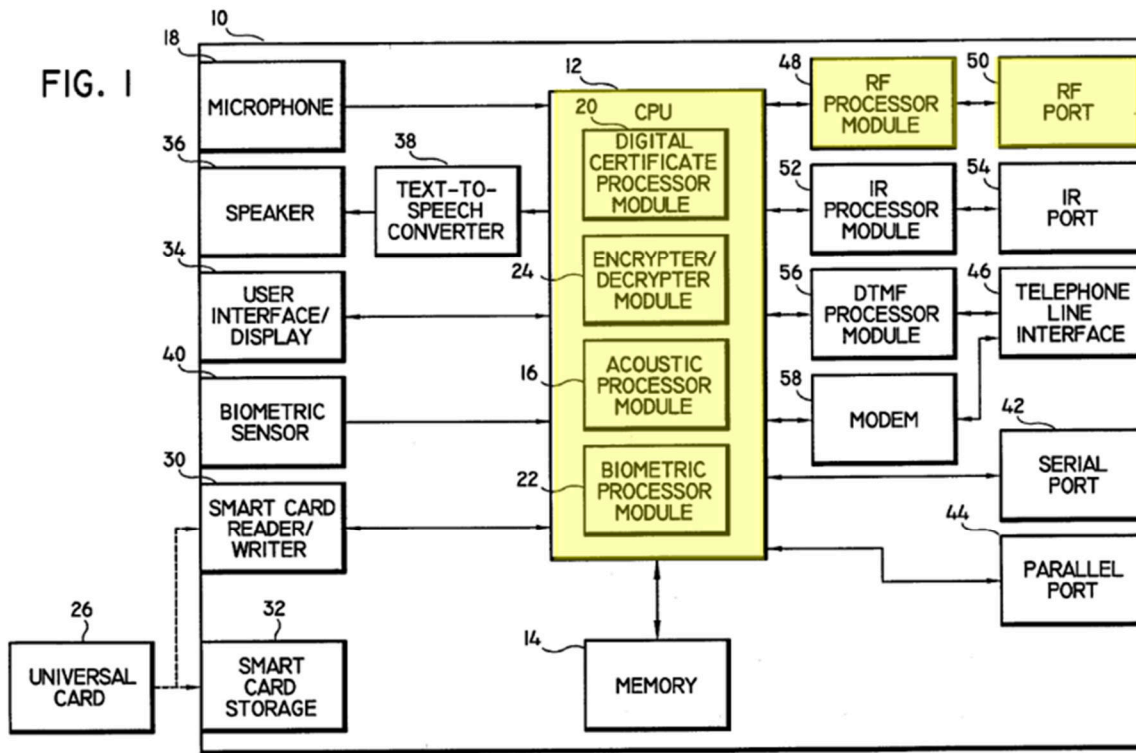
(c) [1.2]

Maes renders [1.2] obvious. EX1003, ¶¶124-127.

Maes’s mobile device “is capable of transmitting or receiving information through wireless communications such as radio frequency (RF) ... communication.” EX1004, Abstract.

With reference to Fig. 1 (reproduced below), Maes explains that “the portable information and transaction processing (PDA) device 10” is “equipped with an RF processor module 48, operatively connected between the CPU 12 and an RF port 50, for processing incoming RF information received by the RF port 50, and for generating transmission signals which are outputted from the RF port 50 using conventional constructions and techniques.” EX1004, 6:1-27, 4:65-5:26. From these and related descriptions, a POSITA would have understood that Maes’s mobile

device includes *short range radio frequency (RF) circuitry* such as RF port 50, RF processor module 48, and/or CPU 12. EX1003, ¶126.



EX1004, Fig. 1 (highlighted).

A POSITA would have understood Maes's RF circuitry depicted in Fig. 1 to be "*short range*" circuitry. EX1003, ¶127. Maes describes an RF link L2 as a direct wireless channel between the PDA held by the user and the POS ... terminal 80. EX1004, 12:5-29 ("the consumer transaction may be performed by transmitting the selected card information directly from the PDA device to the ... POS transaction terminal"), Figs. 3, 5. Maes identifies its RF port 50 and IR port 54 as interchangeable options for the direct link, and IR communication is a short range

line-of-sight technology. EX1004, 3:34-36, 12:16-17, 13:35-36. Maes also distinguishes its direct device-to-terminal RF link from the long-range wireless communications used to connect the PDA to remote central server 60 in client/server mode. EX1004, 7:65-8:14. Accordingly, Maes's RF circuitry that is used for a direct link between the PDA and a nearby transaction terminal to be "***short range RF circuitry***." EX1003, ¶127.

(d) [1.3.1]

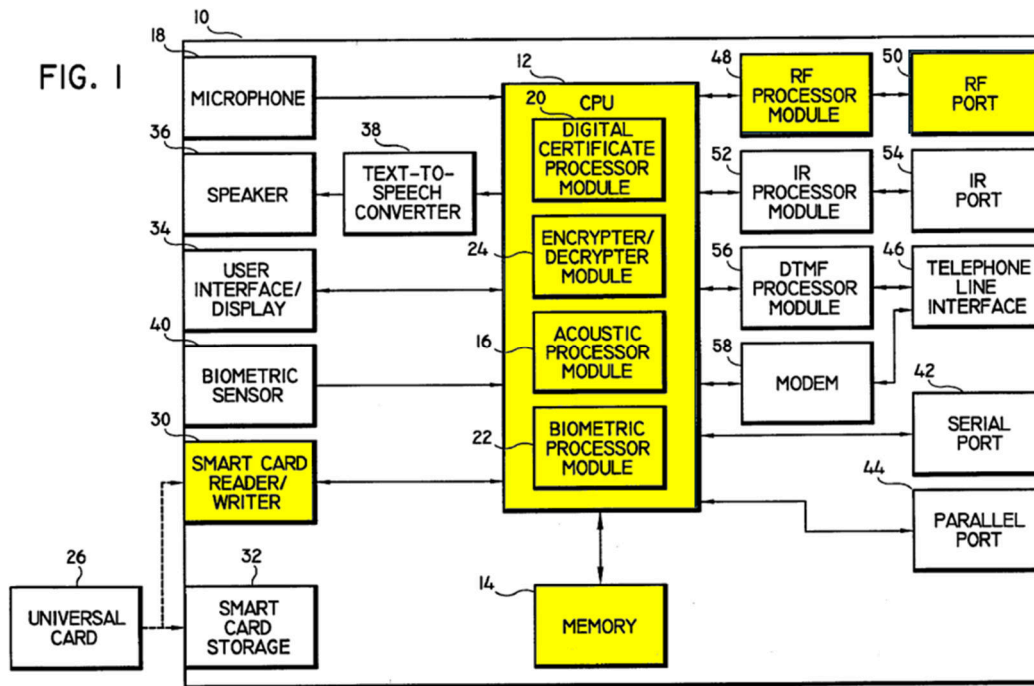
Maes renders [1.3.1] obvious. EX1003, ¶¶128-132.

Maes discloses that the mobile device "includes a memory for storing financial and personal information of the user." EX1004, Abstract; *see also id.*, ("selecting one of the pre-enrolled credit cards that are stored in the PDA").²

With reference to Fig. 1 (reproduced below), Maes explains that "[t]he heart of the device is a central processing unit (CPU) 12, which controls the operations of the PDA device 10 via programs stored in a memory 14 and executed by the CPU 12." EX1004, 5:1-4. "The CPU 12 also includes a digital certificate processor module 20, for processing a digital certificate obtained in the client/server mode of operation ... a biometric processor module 22 for processing biometric data ... to provide user verification," and "an encrypter/ decrypter module 24 for encrypting

² All emphasis in this Petition is added unless otherwise indicated.

the personal and financial information before being stored in memory 14 and for decrypting such information when accessed by the user.” EX1004, 5:8-17; *see also id.*, 5:18-24 (describing special-purpose processors and associated memory).



EX1004, Fig. 1 (highlighted).

The “financial information” that Maes’s memory 14 stores includes information for at least one credit card (*transaction information*). EX1003, ¶131. For example, Maes explains that “the user may ... download [credit card] information into the PDA device 10 by establishing a communication link (L1) with [a] central server 60.” EX1004, 7:1-4. “Alternatively, the credit ... may be loaded into the PDA device 10 by directly reading information contained on such cards through a smartcard reader/writer 30 of the PDA device 10.” *Id.*, 7:4-7. In “[t]he

local mode of operation,” “the user select[s] a pre-enrolled credit card that is stored in memory 14” of the PDA device 10. *Id.*, 10:29-33, Figs. 1, 5. Then, a “consumer transaction may be performed by transmitting the selected card information directly from the PDA device to the ... POS transaction terminal through an established communication link” *Id.*, 12:10-13; *see also id.*, 13:33-38. Accordingly, Maes’s “card information” constitutes *transaction information* stored in *memory* (e.g., memory 14) of PDA-integrated cellular phone (*mobile device*) as claimed. *Supra*, §IV; EX1003, ¶131.

The “personal information” stored in memory 14 further includes *biometric authentication information*, such as voice or fingerprint data belonging to an authorized user of the PDA. EX1003, ¶132. For example, Maes explains that “biometric voice data is [] sent to [an] acoustic processor module 16 wherein such data is processed (step 206) by comparing the current biometric voice data with the user’s voice models stored in memory 14.” EX1004, 10:57-61. Maes further discloses that “[a] biometric sensor 40 of any conventional type may also be provided for collecting biometric data ... such as a finger, thumb or palm print, a handwriting sample, a retinal vascular pattern, or a combination thereof, to provide biometric verification” EX1004, 5:54-60; *see also id.*, 5:13-17 (“encrypting the personal and financial information before being stored in memory 14”), 10:66-11:8, Figs. 1, 5. From these and related descriptions, a POSITA would have understood

that the *memory* of Maes's PDA's stores *biometric authentication information* that the biometric processor module 22 uses to authenticate the user in a POS transaction. EX1003, ¶132.

(e) [1.3.2]

Maes renders [1.3.2] obvious. EX1003, ¶¶133-137.

As discussed at [1.3.1], *supra*, Maes's mobile device's memory 14 stores the user's enrolled credit card information (*transaction information*) together with biometric records for that same user, such as voice data or data for the alternative biometric modalities Maes discloses (e.g., "finger, thumb or palm print, ... a retinal vascular pattern, or a combination thereof"). EX1004, 5:54-60; *supra*, [1.3.1]. Maes discloses that an association between the stored credit card information and biometric authentication information is created during an enrollment process that precedes later authentication event(s) at the time of a transaction. EX1003, ¶134.

For example, at enrollment, the service provider ties the user's designated account to the user's own credit card information, and that record is centrally stored. EX1004, 6:56-7:35, Fig. 3; EX1003, ¶135. Maes explains that "[e]nrollment involves ... providing the service provider with the user's credit card ... information so that such information can be verified with the financial institutions 70 that issued such cards." EX1004, 6:60-7:1. "This information is then stored on a central server 60 of the service provider." EX1004, 6:60-7:1.

This same enrollment record includes the user's biometric authentication information that has been captured and stored alongside account and PIN information for the user. For example, Maes discloses that "[a] personal identification number PIN and ... a unique account number 27 is provided by the service provider," and "[t]his information, as well as biometric data such as voice prints (models) of the user, are also stored in central server 60 of the service provider for user verification during the client/server mode to obtain a digital certificate." EX1004, 7:25-32. From these and related descriptions, a POSITA would have understood that the user's *biometric authentication information* in Maes is stored under, and tied to, the same account and PIN record established for that user's enrolled credit card information (*transaction information*), thereby forming an association between the biometric authentication information and the transaction information created at enrollment. EX1003, ¶136.

That the association was formed in advance, rather than at the moment of the transaction, for example, is confirmed by Maes's description of the "local mode" of operation following enrollment and the "client/server mode" of operation. EX1003, ¶137. Maes discloses that "[t]he local mode of operation is commenced by the user selecting a pre-enrolled credit card that is stored in memory 14 (step 200)," using voice commands such as "I want to use my American Express Card." EX1004, 10:32-36; *see also id.*, Fig. 5 (flowchart depicting "LOCAL MODE" operations),

12:5-29 (describing direct RF transmission embodiment between mobile device and POS terminal in local mode). Maes then requires that “[i]f the requested card information is found in memory, biometric verification must be performed” before the card information can be used. EX1004, 10:49-53; *see also id.*, 11:12-15, Fig. 5. The mobile device performs user verification in local mode “by comparing the current biometric voice data with the user’s voice models stored in memory 14.” EX1004, 10:58-62; *see also id.*, 10:66-11:8 (“In another embodiment of the present invention, a biometric sensor 40 of any known type may be used in lieu of, or in conjunction with the microphone, to collect biometric data to be processed by the biometric processor module 22 using known techniques, e.g., finger, thumb or palm print data, handwriting data, a retinal vascular pattern data or a combination thereof.”). A POSITA would have recognized that comparing incoming biometric data against “the user’s voice models stored in memory” (or stored data for other biometric modalities) to permit use of enrolled credit card information (*transaction information*) depends on the reference voice data already being bound to that particular user’s credit card information (*transaction information*) before the comparison is made, confirming the prior association between Maes’s biometric authentication information and the enrolled credit card information. EX1003, ¶137.

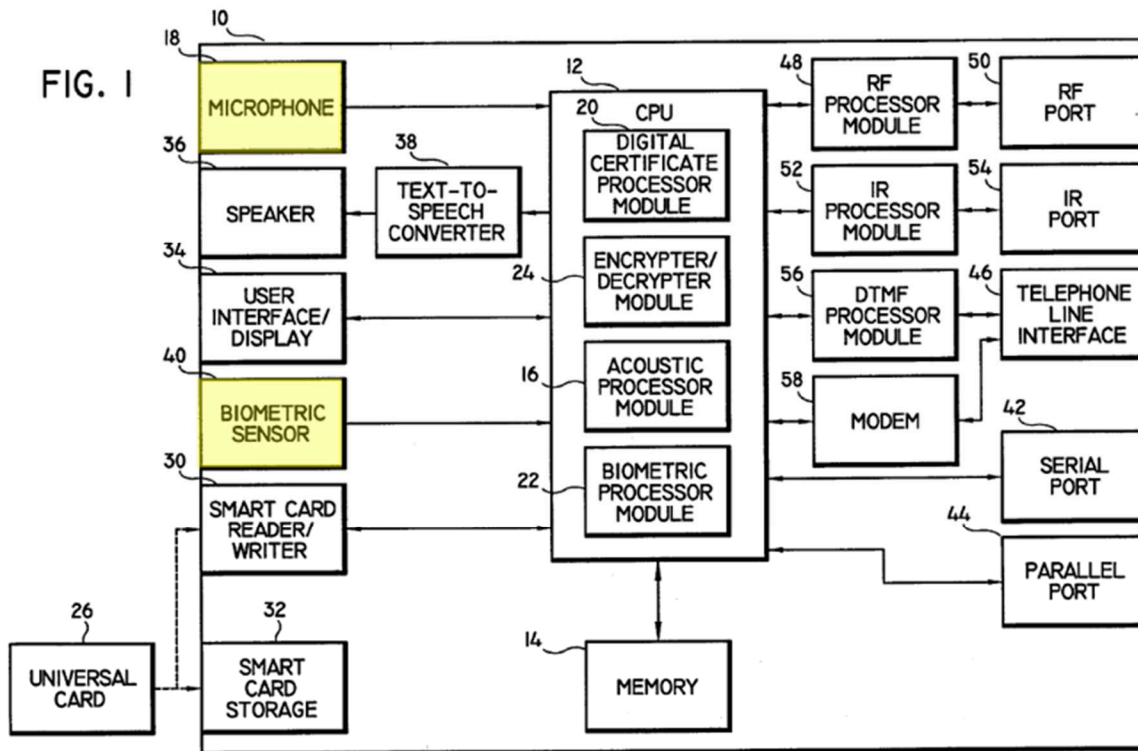
(f) [1.4]

Maes renders [1.4] obvious. EX1003, ¶¶138-141.

Maes's microphone 18 and biometric sensor 40, alternately or together, provide the claimed “*biometric reading device configured to read biometric information.*” EX1003, ¶139. Microphone 18 reads voice-based biometric information, while biometric sensor 40 reads other forms of biometric information. EX1004, 5:53-62, 10:53-61, 11:1-14.

For example, Maes explains that its mobile device includes “a microphone and local central processing unit (CPU) for processing voice commands and for processing biometric data to provide user verification.” EX1004, Abstract. “[U]sing voice activated commands to select the desired card, the microphone 18 functions as a biometric sensor for receiving biometric voice data.” EX1004, 10:53-57, Fig. 1.

Likewise, with respect to Fig. 1 (reproduced below), Maes describes a “biometric sensor 40 of any conventional type ... for collecting biometric data (other than voice data which is received by the microphone 18) such as a finger, thumb or palm print, a handwriting sample, a retinal vascular pattern, or a combination thereof, to provide biometric verification as an alternative to, or in addition to, voice biometric verification.” EX1004, 5:54-60. “This data is then processed by the biometric processor module 22 to provide user verification (*i.e.*, biometric security) prior to accessing the financial and personal information stored in memory 14.” *Id.*, 5:60-63; *see also id.*, Abstract, 5:54-63, 10:49-11:8, Figs. 1, 5.



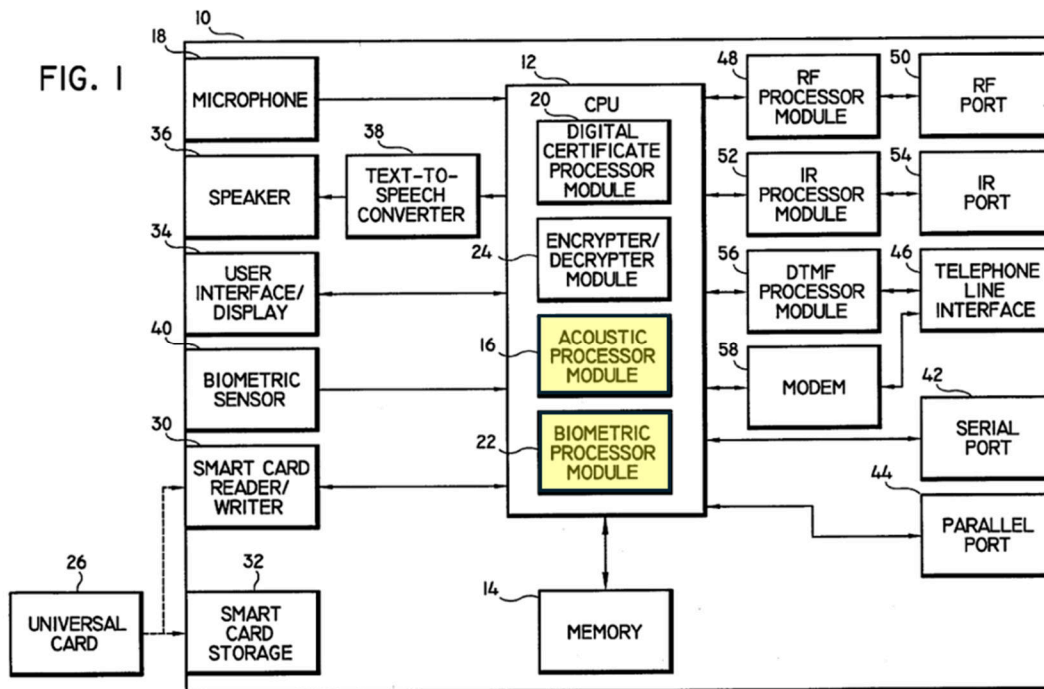
EX1004, Fig. 1 (highlighted).

(g) [1.5]

Maes renders [1.5] obvious. EX1003, ¶¶142-147.

Maes’s “acoustic processor module 16,” alternately or together with its “biometric processor module 22,” provide an “*authentication module*” of the mobile device. EX1003, ¶143. Maes discloses that “[t]he acoustic processor module 16 is [] used for performing local speaker verification.” EX1004, 5:7-8. Maes separately discloses that “the CPU 12 [] includes ... a biometric processor module 22 for processing biometric data in addition to, or alternative to voice data, to provide

user verification.” EX1004, 5:9-14. Maes ties these two modules together as alternately or together providing the same verification determination, stating that “[a]fter the biometric data is processed by the acoustic processing module 16 (when voice verification is utilized) or the biometric processor module 22 (when other biometric verification methods are used), or both, a determination is made as to whether the user is an authorized user (step 208).” EX1004, 11:9-13. A POSITA would have understood from these and related disclosures that either module alone, or the two operating together, can provide the authentication determination recited by [1.5] depending on whether voice-based biometrics, alternate biometric modalities, or both are employed. EX1003, ¶143.



EX1004, Fig. 1 (highlighted)

As discussed at [1.3.1]-[1.3.2] and [1.4], *supra*, Maes's memory 14 stores credit card information (***transaction information***) previously associated with the user's biometric records. Acoustic processor module 16 and/or biometric processor module 22 (***authentication module***) perform the claimed authentication by comparing biometric data newly read from the user against that previously stored, previously associated biometric record. EX1004, 10:58-62, Figs. 1, 3, 5. The device then conditions release of the selected credit card information for a transaction on the outcome of the comparison between the new and stored biometric records. *Id.*, 10:50-52.

In more detail, Maes discloses that "[i]f the requested card information is found in memory, biometric verification must be performed before the card information can be written to the Universal Card 26" for use in a transaction. EX1004, 10:50-52. As depicted in Fig. 5, user verification is similarly required before the card information will be retrieved from memory and decrypted for use in a transaction for those embodiments that involve direct transmission of card information from the mobile device to the POS terminal via short-range RF (without use of the Universal Card). EX1004, 12:5-29, Fig. 5.

Maes explains that comparison of the newly read biometric input to the stored biometric is performed by acoustic processor module 16 for the voice modality, stating that "[t]his biometric voice data is then sent to the acoustic processor module

16 wherein such data is processed (step 206) by comparing the current biometric voice data with the user's voice models stored in memory 14.” EX1004, 10:57-62. Maes describes the parallel operation for biometric processor module 22 when other biometric modalities are used, disclosing a biometric sensor 40 “to collect biometric data to be processed by the biometric processor module 22 using known techniques, e.g., finger, thumb or palm print data, handwriting data, a retinal vascular pattern data or a combination thereof.” EX1004, 10:66-11:5. Maes further discloses that “[i]f the user is not verified, the selected card information will not be written” for use in a transaction. EX1004, 11:13-15, Fig. 5. Thus, successful verification by acoustic processor module 16 and/or biometric processor module 22 allows the selected card information to be released for a transaction. EX1003, ¶146.

A POSITA would have understood the comparison performed by modules 16 and/or 22 to authenticate that the biometric information just read is associated with the transaction information at least because the comparison is made against the biometric record previously associated with that same user's account and credit card information at enrollment. EX1003, ¶147. Maes's mobile device thus authenticates that the biometric information just read is associated with transaction information in a manner that aligns exactly with the Patent Owner's explanation of such authentication to the examiner during prosecution. *See* EX1002, 41-42 (“The device can compare the biometric information input by the user with the stored biometric

authentication information, which has already been associated with the transaction information. As such, verification of the user's identity allows the device to also authenticate the user's authorization with respect to the stored transaction information.”).

(h) [1.6.1]

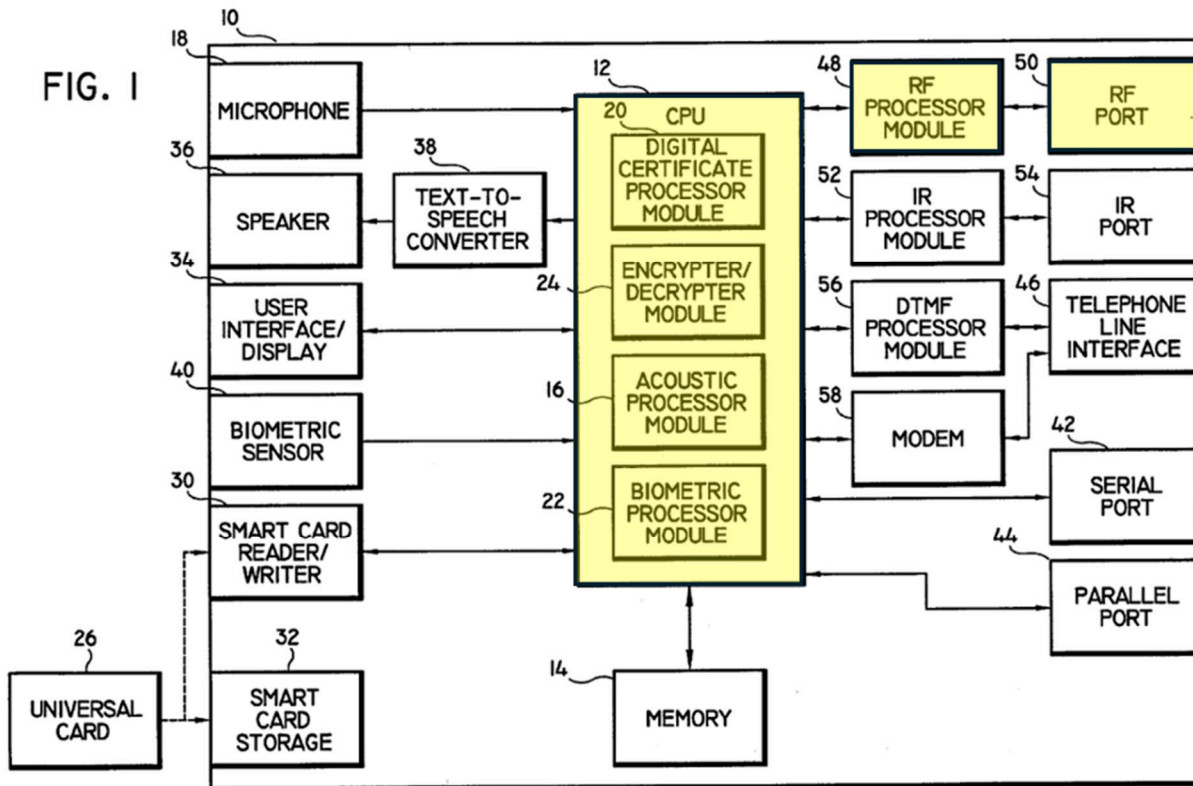
Maes renders [1.6.1] obvious. EX1003, ¶¶148-151.

Maes's CPU 12 alone or in coordination with RF processor module 48 and RF port 50, provides a “*transaction module*” as claimed. EX1003, ¶149. Maes identifies CPU 12 as the device's central controller, stating that “[t]he heart of the device is a central processing unit (CPU) 12, which controls the operations of the PDA device 10 via programs stored in a memory 14 and executed by the CPU 12.” EX1004, 5:1-4. As discussed at [1.2], *supra*, RF processor module 48 and RF port 50 are short range RF circuitry. *Supra*, [1.2]. For example, Maes discloses that “the device may preferably be equipped with an RF processor module 48, operatively connected between the CPU 12 and an RF port 50, for processing incoming RF information received by the RF port 50, and for generating transmission signals which are outputted from the RF port 50 using conventional constructions and techniques.” EX1004, 6:8-15. A POSITA would have understood that CPU 12 directs what data is sent, while RF processor module 48 and RF port 50 carry out the physical wireless transmission, so that CPU 12 acting through this RF pathway

provides selected credit card information (*transaction information*) for a transaction *via short range RF circuitry*. EX1003, ¶149.

Further illustrating this point, Maes discloses that CPU 12 retrieves the selected, stored credit card information from memory and the mobile device transmits it directly to the transaction terminal over the RF pathway. EX1004, 12:5-29; *see also id.*, 13:19-38 (“The selected card information ... would be transmitted to the POS terminal (via ... RF ...)”), Figs. 3, 5. Maes explains that “the invention may interact with electronic fund transfer systems or transaction terminals having wireless or direct communication capabilities without even having to use the Universal Card 26.” EX1004, 12:5-8. Maes then describes the RF pathway for the transmission, noting that “the consumer transaction may be performed by transmitting the selected card information directly from the PDA device to the ... POS transaction terminal through an established communication link L2 ... (i.e., via the ... RF port 50), rather than retrieving and writing card information to the Universal Card 26.” EX1004, 12:9-16. A POSITA would have understood the RF port 50 option in this passage to be the short range RF circuitry pathway, with CPU 12 as the component that retrieves the selected card data from memory and that directs its output through RF processor module 48 to RF port 50 for transmission to the terminal, thereby providing the transaction information via the short range RF circuitry for use in a transaction. EX1003, ¶150.

Maes further discloses that “the CPU 12 of the PDA device 10 will prohibit the selected card information from being retrieved and transmitted to the transaction terminal 80 if the user is not biometrically verified and/or if the digital certificate is not valid (step 226).” EX1004, 12:18-23. Further, according to Maes, “the PDA device 10 itself actually takes the place of the Universal Card 26 and, consequently, eliminates the need of having to first write the selected card information to the Universal Card 26 and then sweep the Universal Card 26 through the magnetic reader of the POS ... transaction terminal.” EX1004, 12:23-29. A POSITA would have recognized that CPU 12 provides the selected card information for use in a transaction, including controlling whether and when specific card information is retrieved and transmitted over the RF pathway. EX1003, ¶151.



EX1004, Fig. 1 (highlighted)

(i) [1.6.2]

Maes renders [1.6.2] obvious. EX1003, ¶¶152-155.

As discussed at [1.6.1], *supra*, Maes's CPU 12, alone or cooperating with RF processor module 48 and RF port 50, discloses the claimed "**transaction module**." Maes's transaction module retrieves the selected, stored credit card information and transmits it directly to the POS transaction terminal over the short-range RF link. EX1004, 12:5-16.

Element [1.6.2] adds that the provision of the transaction information occurs "when the biometric information read by the biometric reading device is successfully

authenticated as being associated with the transaction information by the authentication module.” EX1001, 23:3-8. Maes discloses this exact condition. Indeed, the same portion of Maes that describes the CPU 12’s role in retrieving and transmitting selected credit card information for a transaction further explains that “the CPU 12 of the PDA device 10 will prohibit the selected card information from being retrieved and transmitted to the transaction terminal 80 if the user is not biometrically verified and/or if the digital certificate is not valid (step 226).” EX1004, 12:18-23, Fig. 5. A POSITA would have understood the converse of this conditional statement, namely, that when the digital certificate is valid and the user is biometrically verified, CPU 12 retrieves and transmits the selected card information. EX1004, Fig. 5 (depicting card information transmitted from mobile device to POS terminal automatically when the user is verified); EX1003, ¶154.

Maes’s description of its local-mode of operation, which the column 12 direct-transmission embodiment modifies only at the output stage (see [1.6.1], *supra*), confirms that this triggering is automatic, and does not require any intervening user action between verification of the user and transmission of the selected card information. EX1003, ¶155. To this point, Maes discloses that “[i]f the user is verified, the digital certificate (previously obtained in the client/server mode) is retrieved from memory 14 and loaded into the digital certificate processor module 20.” EX1004, 11:15-18. “If the digital certificate is valid (i.e., unexpired) the

requested card information is then retrieved from memory 14 and stored in the encrypter/decrypter module 24,” with the selected card information “then decrypted by the encryption/decryption module 24 using an encryption key unique to the PDA device 10 (step 214)” before delivery. EX1004, 11:26-31. Maes’s process culminates in the mobile device’s transmission of selected card information via short-range RF. EX1004, 12:5-29, Fig. 5; *see also id.*, 13:19-38. Here, everything downstream of successfully matching the new biometric to the stored biometric is performed automatically by CPU 12 and its cooperating modules such that the selected card information is transmitted when the new biometric is successfully authenticated as being associated with the transaction information. EX1003, ¶155.

(j) [2]

Maes renders [2] obvious. EX1003, ¶¶156-157.

For example, Maes discloses that “[a] biometric sensor 40 of any conventional type may also be provided for collecting biometric data (other than voice data which is received by the microphone 18) such as a finger, thumb or palm print, a handwriting sample, a retinal vascular pattern, or a combination thereof, to provide biometric verification as an alternative to, or in addition to, voice biometric verification.” EX1004, 5:54-60; *see also id.*, 10:66-11:5 (“collect biometric data to be processed by the biometric processor module 22 using known techniques, e.g., finger, thumb or palm print data”). A POSITA would have understood biometric

sensor 40, configured to collect finger or thumb print data, to be a ***fingerprint reading device*** as recited in [2]. EX1003, ¶157; *supra*, [1.4].

(k) [3]

Maes renders [3] obvious. EX1003, ¶¶158-161.

As discussed in connection with [1.3.1], *supra*, Maes discloses “***transaction information***” as enrolled credit card information stored in a memory of the mobile device and transmitted for use in a transaction. *Supra*, [1.3.1]; EX1003, ¶159. Maes discloses that the user enrolls this credit card data at the outset, stating that enrollment “involv[es] ... providing the service provider with the user’s credit card ... information so that such information can be verified with the financial institutions 70 that issued such cards.” EX1004, 6:62-65. Maes discloses that this same credit card information becomes the ***transaction information*** delivered for a purchase. Indeed, in local mode, “[t]he local mode of operation is commenced by the user selecting a pre-enrolled credit card that is stored in memory 14 (step 200),” using a voice command such as “I want to use my American Express Card.” EX1004, 10:32-36.

Maes further discloses that the process of first loading credit card data into the mobile device includes generating the stored ***transaction information*** from underlying credit card information. EX1003, ¶160. Specifically, Maes discloses two mechanisms loading credit card information in memory of the mobile device,

including (1) downloading from the central server or (2) “directly reading information contained on such cards through the smartcard reader/writer 30 of the PDA device 10.” EX1004, 7:1-18. The PDA “will compare the user ID of the credit cards with the user ID of the PDA device to verify the user so as to prevent a user from downloading the information from cards owned by another person into the user’s PDA device 10.” EX1004, 7:7-12.

From these and related descriptions, a POSITA would have understood that Maes discloses that the card information on the mobile device is *transaction information generated based at least in part on credit card information*, as recited in claim 3. EX1003, ¶161.

(I) [5]

Maes renders [5] obvious. EX1003, ¶¶162-165.

Maes discloses that “[t]he CPU 12 further includes an encrypter/decrypter module 24 for encrypting the personal and financial information before being stored in memory 14 and for decrypting such information when accessed by the user.” EX1004, 5:13-17. A POSITA would have understood encrypter/decrypter module 24 to be a “*security block*” as recited in [5]. Indeed, Maes’s encrypter/decrypter module 24 adds security by encrypting the credit card information (*transaction information*) loaded on the device for secure storage in memory 14 and decrypts the

credit card information for a transaction when the user is verified and the digital certificate is determined to be valid. EX1004, 5:13-18, 7:51-56, 11:27-29, Fig. 1; EX1003, ¶163.

Maes discloses that the encryption and thus securing of the credit card information on the device occurs before the credit card information is provided by the transaction module (*e.g.*, CPU 12 alone or in cooperation with RF processor module 48 and RF port 50, as established at [1.6.1]-[1.6.2], *supra*) for delivery over the short range RF link. EX1004, Figs. 3, 5. For example, Maes explains that encrypter/decrypter module 24 “encrypts the personal and financial information before being stored in memory 14.” EX1004, 5:14-17, Fig. 1-3. Maes further explains that the credit card information must be “RETRIEVED AND DECRYPTED” for use in a transaction before being “TRANSMITTED TO TRANSACTION TERMINAL” from the mobile device. EX1004, FIG. 5 (steps 214, 228); *see also id.*, 11:29-33 (“The selected card information is then decrypted by the encryption/decryption module 24 using an encryption key unique to the PDA device 10 (step 214).”), 12:5-29 (“transmitting the selected card information directly from the PDA device”), 5:13-17.

From these and related descriptions, a POSITA would have understood that Maes’s encrypter/decrypter module 24 (*security block*) is *configured to secure the*

transaction information before it is provided by the transaction module. EX1003, ¶165.

(m) [6]

Maes renders [6] obvious. EX1003, ¶¶166-167.

As discussed at [5], *supra*, Maes’s encrypter/decrypter module 24 (*security block*) performs its securing function specifically through encryption and decryption, stating that it is used “for encrypting the personal and financial information before being stored in memory 14 and for decrypting such information when accessed by the user.” EX1004, 5:13-17; *see also id.*, 11:29-31 (““[t]he selected card information is then decrypted by the encryption/decryption module 24 using an encryption key unique to the PDA device 10 (step 214).””), 10:11-15 (“may employ any known encryption technique or algorithm for the encryption/decryption process”). A POSITA would have understood a security block whose disclosed operation is encrypting and decrypting data using cryptographic keys to be a *cryptographic block* as recited in claim [6]. EX1003, ¶167.

(n) [8]

Maes renders [8] obvious. EX1003, ¶¶168-171.

As discussed above, Maes’s CPU 12, alone or together with RF processor module 48 and RF port 50 (*transaction module*) provides selected credit card information for a transaction via the short range RF circuitry. *Supra*, [1.6.1]-[1.6.2].

Maes explains that “the consumer transaction may be performed by transmitting the selected card information directly from the PDA device to the ... POS transaction terminal through an established communication link L2 ... (i.e., via ... the RF port 50), rather than retrieving and writing card information to the Universal Card 26.” EX1004, 12:9-16; *see also id.*, 13:34-38 (“via ... RF”).

While Maes discloses that the selected credit card information (*transaction information*) is transmitted from the mobile device to the POS terminal via RF, nowhere does Maes disclose any corresponding transmission of biometric information. *See e.g.*, EX1004, 12:9-23, 13:25-36, Fig. 5 . A POSITA would have understood Maes’s silence as to any transmission of biometric information for use in a transaction as reflecting the reality that only Maes’s credit card information (*transaction information*), but not the biometric information, is what the transaction module actually provides via RF in Maes’s framework. EX1003, ¶170.

Maes’s broader description of how biometric data is used confirms that its omission of any transmission of biometric information in local mode reflects a specific design choice to keep biometric information on device. EX1003, ¶171. Maes discloses that biometric data is captured and consumed entirely within the PDA’s own local-mode processing loop: “[t]his biometric voice data is then sent to the acoustic processor module 16 wherein such data is processed (step 206) by comparing the current biometric voice data with the user’s voice models stored in

memory 14.” EX1004, 10:58-62. That takes place using biometric data stored on memory 14 and the CPU 12 processing modules. *Supra*, [1.3.1]. The central server and financial institution then verify the user and determine whether to authorize a transaction based on the selected card information, assurances that the authorization number and card information could not be accessed without user verification and a valid digital certificate, and optionally further based on an electronic information file that accompanies the card information. EX1004, 12:5-13:38, Fig. 5. Neither the central server nor the financial institution process the biometric information just received from the user involved in the transaction, and thus the mobile device does not provide biometric information to the merchant, the financial institution, or central server. Indeed, there is no need to do so in the context of Maes’s system. EX1003, ¶171. At a minimum, a POSITA would have found it obvious not to transmit the biometric information because not transmitting it when the backend systems make no use of it would result in a more efficient and less time-consuming transmission of data over the short-range RF link during a transaction. *Id.*

(o) [9.pre]

Supra, [1.pre]; EX1003, ¶172.

(p) [9.1]

Supra, [1.1]; EX1003, ¶173.

(q) [9.2]

Supra, [1.2]; EX1003, ¶174.

(r) [9.3.1]

Supra, [1.3.1]; EX1003, ¶175.

(s) [9.3.2]

Supra, [1.3.2]; EX1003, ¶176.

(t) [9.4]

Supra, [1.4]; EX1003, ¶177.

(u) [9.5]

Supra, [1.5]; EX1003, ¶178.

(v) [9.6.1]

Supra, [1.6.1]; EX1003, ¶179.

(w) [9.6.2]

Supra, [1.6.2]; EX1003, ¶180.

(x) [9.7]

Supra, [5]; EX1003, ¶181.

(y) [10]

Supra, [2]; EX1003, ¶182.

(z) [11]

Supra, [3]; EX1003, ¶183.

(aa) [13]

Supra, [6]; EX1003, ¶184.

(bb) [15]

Supra, [8]; EX1003, ¶185.

(cc) [16.pre]

Maes renders [16.pre] obvious. EX1003, ¶¶186-187.

Maes discloses a “portable client PDA,” *e.g.*, PDA device 10 depicted in Fig. 1. EX1004, FIG. 1; *supra*, [1.pre]. Maes further discloses that “the functions and components of the PDA device 10 may be built into a cellular phone, whereby communication with the central server 60 may be achieved through a cellular communication channel, which may be analog or digital (*e.g.*, CDMA, GSM, etc.).” EX1004, 14:12-16. A POSITA would have understood from these and related descriptions that Maes discloses a ***cellular telephone***. EX1003, ¶187.

(dd) [16.1]

Supra, [1.1]; EX1003, ¶188.

(ee) [16.2]

Supra, [1.2]; EX1003, ¶189.

(ff) [16.3.1]

Supra, [1.3.1]; EX1003, ¶190.

(gg) [16.3.2]

Supra, [1.3.2]; EX1003, ¶191.

(hh) [16.4]

Supra, [1.4]; EX1003, ¶192.

(ii) [16.5]

Supra, [1.5]; EX1003, ¶193.

(jj) [16.6.1]

Supra, [1.6.1]; EX1003, ¶194.

(kk) [16.6.2]

Supra, [1.6.2]; EX1003, ¶195.

(ll) [17]

Supra, [2]; EX1003, ¶196.

(mm) [18]

Supra, [5]; EX1003, ¶197.

(nn) [19]

Supra, [6]; EX1003, ¶198.

(oo) [20]

Supra, [3]; EX1003, ¶199.

(pp) [23]

Supra, [8]; EX1003, ¶200.

B. Ground 1B: Maes-Dorf Renders Obvious Claims 4, 12, and 21

1. Dorf (EX1009)

Dorf discloses a “multifunction card system” that adds a loyalty-card function to a payment card alongside its debit, phone-card, and gift-certificate functions. EX1009, Abstract. Dorf explains that “the system 108 ... may provide a separate loyalty card much like a frequent flier card that can have points added at virtually any POS device 105.” EX1009, 9:27-31. Dorf discloses that this loyalty function can be product- or manufacturer-specific, stating that “[t]he card could be issued by a certain manufacturer to reward a customer with loyalty points for purchasing the manufacturer’s product, regardless of the retail location of the purchase.” EX1009, 9:33-36; *generally id.*, 9:25-10:6. Likewise, “the card could be issued by a particular retailer to reward customers for purchases made in the retailer’s location(s),” crediting points “for any purchase within the store” or for “special promotional items.” EX1009, 9:53-58. Dorf further discloses that loyalty points accumulated in this manner may be redeemed for value, disclosing redemption “for an item selected

from the group consisting of goods, services, discounts on goods and services, long distance telephone calling time value, and money value.” EX1009, 20:60-64.

2. The Maes-Dorf Combination (MDC)

Maes discloses a mobile device that stores information for multiple pre-enrolled “financial cards.” EX1004, 10:32-52, 12:9-23; *supra*, [1.3.1], [1.6.1]-[1.6.2]. Maes notes that the term “financial card” encompasses a wide range of payment cards, including “credit cards, ATM cards and direct debit cards.” EX1004, 1:50-54; *see also id.*, 2:25-27, 11:51-57. Maes does not provide an exhaustive list of different types of financial cards, as a POSITA would have been familiar with additional types not explicitly discussed in Maes. EX1003, ¶¶82-87. For example, as addressed above (*supra*, §V.B.1), Dorf describes a financial card having a “loyalty function.” EX1009, 9:25-10:6, 12:22-27, 20:60-64. A POSITA would have found it obvious to implement Maes’s system in accordance with Dorf’s suggestion for attaching a loyalty function to a financial card. EX1003, ¶¶82-87. Multiple reasons would have motivated a POSITA to pursue this Maes-Dorf combination (“MDC”). EX1003, ¶¶82-87.

First, Maes already stores multiple types of financial card data, but discloses no mechanism for rewarding continued use of a given card. Given that benefits of loyalty programs that were well-established before the Critical Date of the ’807 Patent, a POSITA would have found it obvious to use a card with a loyalty-function

in Maes's system to encourage use of particular financial cards through Maes's mobile-device based payment instrument. EX1004, 4:1-3, 5:24-27; EX1003, ¶¶82-87.

Second, attaching a loyalty-rewards balance to an existing payment card was, by the Critical Date, a widely recognized consumer convenience, as reflected in Dorf's own description of frequent-flier-style loyalty programs already in common use. EX1009, 9:27-29; EX1003, ¶¶82-87.

Third, Maes's own card data already extends to non-payment types, such as "access control cards ... cash cards ... calling cards ... and employee cards." EX1004, 5:24-27. Thus, attaching a loyalty-point field to a financial card's data was simply one further, obvious selection from the range of data types Maes's architecture was already designed to accommodate. EX1003, ¶¶82-87.

Fourth, attaching Dorf's known loyalty-point functionality to Maes's existing financial cards amounts to a simple substitution or addition of a known element for a predictable result (e.g., a loyalty function with point balance). *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007) ("The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results."). EX1003, ¶¶82-87.

A POSITA would have had a reasonable expectation of success pursuing MDC. EX1003, ¶¶82-87. Indeed, loyalty-point crediting functions, such as the one

Dorf discloses, were well known and conventional in the payment-card art long before the Critical Date. Accordingly, implementing a loyalty function on an existing financial card would have been a straightforward task. EX1003, ¶¶82-87.

3. Claim Element Analysis

(a) [4]

MDC renders [4] obvious. EX1003, ¶¶201-203.

As discussed above in Ground 1A, Maes discloses that the card information (*transaction information*) used in a transaction can be generated based at least in part on credit card information. *Supra*, Ground 1A at [3]. Maes further discloses that a range of different types of financial cards can be employed. EX1004, 1:50-54, 2:25-27, 2:50-57, 11:51-57.

Dorf further describes the well-known option of attaching a loyalty function to a financial card. *See e.g.*, EX1009, 9:25-10:6, 12:22-27, 20:60-64; *supra*, §V.B.1. A POSITA would have understood that the use of a loyalty function as suggested by Dorf with the types of financial cards described in Maes would result in generation of transaction information *based at least in part on rewards card information*, as recited in claim 4. EX1003, ¶203. For example, Dorf describes how a loyalty-point balance associated with the card allows cardholders to earn loyalty points as rewards for use of the card. EX1009, 9:33-36 (“reward a customer with loyalty points”), 9:9-13 (“award loyalty points”), 12:22-27. The transaction information in MDC is

generated based on rewards card information in the same fashion that transaction information is generated in Maes based on credit card information. EX1003, ¶203; *supra*, §V.B.2.

(b) [12]

Supra, [4]; EX1003, ¶204.

(c) [21]

Supra, [4]; EX1003, ¶205.

C. Ground 1C: Maes-Shults Renders Obvious Claims 7, 14, and 22

1. Shults (EX1008)

Shults describes “a hand-held apparatus incorporating both electronic identity and optical identity,” in which “[t]he electronic identity is provided by a radio-frequency electronic transponder 104.” EX1008, [0024]. In Shults, “when a customer presents apparatus 100 at scanner 312 or 314, the point-of-sale system 304, 306, 308 determines the identity (electronic or optical) and sends that identity information to server complex 302 ... to identify the particular customer and customer account associated with that apparatus.” EX1008, [0043]. Shults discloses that the electronic identity “is provided by a radio-frequency identification (RFID) circuit 104.” EX1008, [0030].

Per Shults, the apparatus can be “a portable cellular telephone or a personal digital assistant.” EX1008, [0009]. Shults further notes that “[t]he hand-held or portable aspect of apparatus 100 is particularly advantageous when it is used for purchasing or other types of financial transactions.” EX1008, [0024].

2. The Maes-Shults Combination (MSC)

Maes discloses that its PDA “may preferably be equipped with an RF processor module 48, operatively connected between the CPU 12 and an RF port 50, for processing incoming RF information received by the RF port 50, and for generating transmission signals which are outputted from the RF port 50 using conventional constructions and techniques.” EX1004, 6:9-15; *supra*, §V.A.1.

Maes further explains that “the consumer transaction may be performed by transmitting the selected card information directly from the PDA device to the ... POS transaction terminal through an established communication link ... via ... the RF port 50.” EX1004, 12:10-15.

Although Maes broadly describes the PDA having short-range RF circuitry, Maes does not expressly disclose the specific type of RF circuitry applied in the PDA (or cellular phone). EX1003, ¶¶90-99. Shults does. Specifically, Shults describes a hand-held apparatus in the form of “a portable cellular telephone or a personal digital assistant” whose “electronic identity is provided by a radio-frequency identification (RFID) circuit 104.” EX1008, [0009], [0030]; EX1003, ¶¶90-99. Shults’s RFID

circuit 104 is implemented with a conventional, commercially available system such as “a Texas Instruments TIRIS system,” “a ROADCHECK system from Mark IV Inc.,” or “an ASSET ID system from HID Corp.” EX1008, [0031]; EX1003, ¶¶90-99. Shults’s “hand-held or portable aspect of apparatus 100 is particularly advantageous when it is used for purchasing or other types of financial transactions.” EX1008, [0024].

A POSITA would have found it obvious to implement the RF circuitry in Maes’s mobile device using RFID in accordance with Shults’s teachings. EX1004, 6:9-15, 12:10-15; EX1008, [0024], [0030], [0031]; EX1003, ¶¶90-99. Multiple reasons would have motivated the combination. EX1003, ¶¶90-99.

First, a POSITA would have been motivated to use RFID in Maes’s device because Shults confirms that an RFID-based electronic identity is “particularly advantageous when it is used for purchasing or other types of financial transactions” and Maes’s PDA is used for exactly this purpose. EX1004, 6:9-15, 12:10-15; EX1008, [0024]; EX1003, ¶¶90-99.

Second, a POSITA would have been motivated to implement RFID in Maes’s device to enable transactions with existing point-of-sale systems without requiring modification to those systems. EX1003, ¶¶90-99. Shults explains that apparatus 100 “is intended to be used with existing point-of-sale systems to the maximum extent possible, without requiring significant modifications to the point-of-sale system.”

Adding Shults's circuit 104 allows the mobile device to transact with existing point-of-sale systems having "electronic scanner equipment 314," without substantial (or even any) modification to those systems. EX1008, [0037]; EX1003, ¶¶90-99.

Third, a POSITA would have been motivated to use RFID in Maes's device to achieve a cost-effective implementation using off-the-shelf, commercially available components. EX1003, ¶¶90-99. Indeed, Shults expressly teaches that RFID circuit 104 can be implemented with a conventional, commercially available system such as "a Texas Instruments TIRIS system," "a ROADCHECK system from Mark IV Inc.," or "an ASSET ID system from HID Corp." EX1008, [0031]; EX1003, ¶¶90-99.

Fourth, a POSITA would have been motivated to implement RFID in Maes's device because doing so merely involved the application of a known RF technique (e.g., RFID) that was both consistent with Maes's RF-based embodiments and well within the POSITA's technical grasp. *KSR*, 550 U.S. 398, 417, 421 (2007). A POSITA seeking to implement RF-based identification in Maes's mobile device would have looked to Shults's RFID circuit 104 as a familiar, readily available element performing its established function, requiring nothing more than ordinary skill to apply it as Maes's RF circuitry. EX1004, 6:9-15, 12:10-15; EX1008, [0030], [0031]; EX1003, ¶¶90-99.

The resulting Maes-Shults Combination (MSC) includes a mobile device (such as a PDA or cellular phone per Maes), whose RF circuitry (which uses “conventional constructions and techniques”) further includes Shults’s RFID circuit 104 (per Shults). *Supra*, §V.A.3; EX1004, 6:9-15, 12:10-15; EX1008, [0030], [0031]; EX1003, ¶¶90-99. MSC’s PDA operates as in Maes, including transmitting the selected card information to the POS transaction terminal via the RF port 50. *Supra*, §V.A.3; EX1004, 12:10-15; EX1003, ¶¶90-99.

A POSITA would have reasonably expected success applying RFID to Maes’s device, especially as Maes already contemplates the use of RF circuitry “using conventional constructions and techniques,” and Shults’s RFID circuit 104 represents such a conventional construction. EX1004, 6:9-15; EX1008, [0031]; EX1003, ¶¶90-99.

3. Claim Element Analysis

(a) [7]

MSC renders [7] obvious. EX1003, ¶¶206-208.

In MSC, Maes’s mobile device includes short-range RF circuitry (*see supra*, Ground 1A at [1.2]), and that circuitry further includes an RFID circuit consistent with Shults’s teachings. *Supra*, §§V.C.1-2, Ground 1A at [1.2]; EX1008, [0030]; EX1003, ¶207.

Therefore, a POSITA would have understood that in MSC, the mobile device's *short-range RF circuitry comprises an RFID device*. *Supra*, §V.C.2; EX1008, [0030]; EX1003, ¶208.

(b) [14]

Supra, [7]; EX1003, ¶209.

(c) [22]

Supra, [7]; EX1003, ¶210.

D. Ground 2A: Walker-Maes Renders Obvious Claims 1-3, 5-6, 8-11, 13, 15-20, 23

1. Walker (EX1007)

Walker proposes to address security vulnerabilities associated with conventional credit card numbers, which are typically re-used across many transactions, by providing a “single-use, transaction-specific financial account number” that stands in for the cardholder’s real account number for one transaction only. EX1007, 1:17-19, Abst.. Walker discloses two embodiments for producing single-use numbers. In the first, the cardholder’s device cryptographically derives a new number for each transaction on the fly. EX1007, 6:60-7:9.

In the second embodiment, rather than cryptographically generating a fresh number for each transaction, Walker’s device is provisioned with and draws from a pre-populated inventory of numbers. EX1007, 11:19-12:24, FIGS. 10-14. The

device's memory stores "a database with a list of Single-use credit card numbers and a flag for each number indicating whether the number has already been used." EX1007, 11:21-24. These numbers are "assigned to the cardholder by the credit card issuer." EX1007, 11:24-25. To obtain a number for use in a transaction, the cardholder authenticates with the device (e.g., via PIN or biometric input), and the device then searches its stored list. If an unused number remains, it is displayed to the cardholder, and if none remain, the cardholder is instructed to obtain a new device from the credit card issuer. EX1007, 11:58-59. The device then updates that entry's status from "not used" to "used." *Id.*; *generally id.*, 11:19-12:24, FIGS. 10-14; EX1003, ¶¶100-102.

2. The Walker-Maes Combination (WMC)

The Walker-Maes Combination ("WMC") includes (per Walker) a device 100, including its keypad 103, display screen 102, memory 104, central processor 101, and biometric interface 105. EX1007, 5:52-54, 5:58-61; EX1003, ¶¶103-114. In WMC, device 100 is (per Maes) implemented as a mobile device such as a PDA or cellular phone that includes RF cellular circuitry, the RF processor module 48 and RF port 50, and the encrypter/decrypter module 24, as well as other functionalities of CPU 12. EX1004, 2:23-30, 5:14-17, 6:8-15, 14:12-16; EX1003, ¶¶103-114. *Supra*, Ground 1A at [1.1], [1.2], [5], [6].

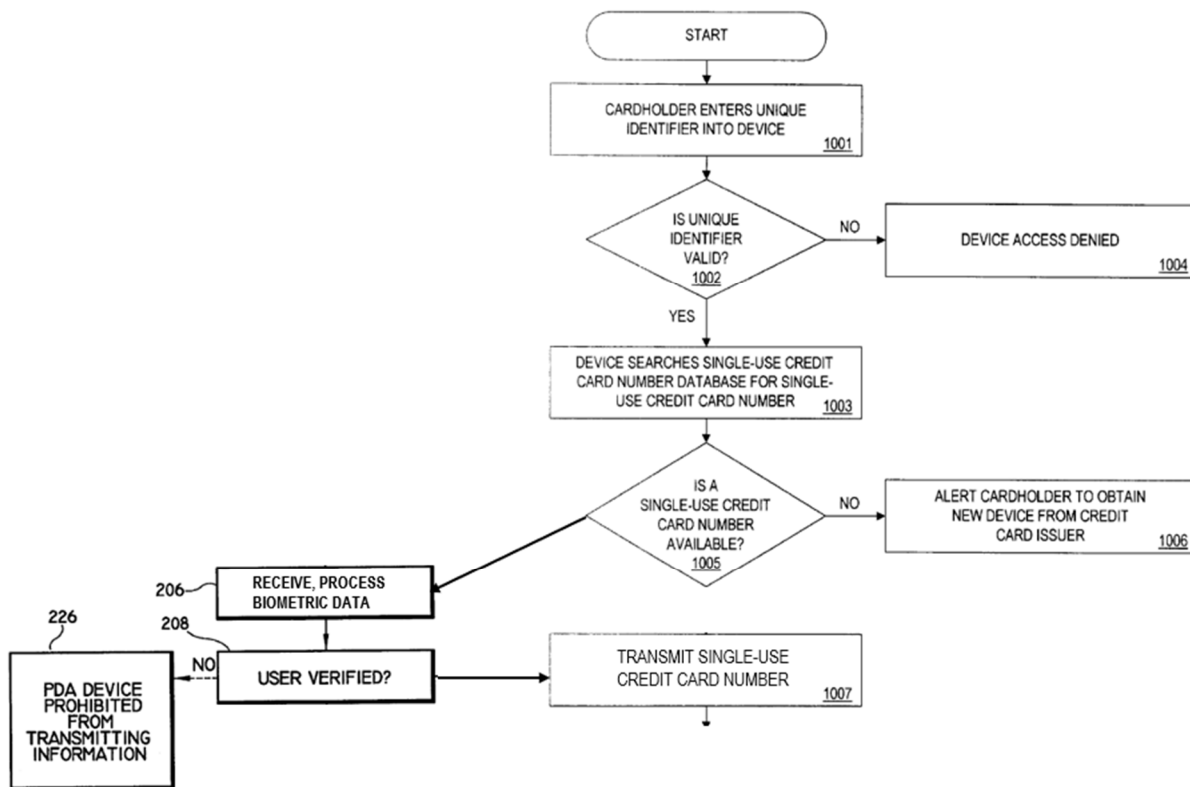
A POSITA would have been motivated to implement Walker's device 100 as a PDA or cellular phone, e.g., as described in Maes. EX1003, ¶¶103-114. A POSITA would have recognized that implementing device 100 as a PDA or cellular phone places the single-use credit card numbers on a device the cardholder carries and uses for other purposes, rather than requiring a separate dedicated device. EX1007, 11:21-25; EX1004, 14:2-7; EX1003, ¶¶103-114. Implementing device 100 as a PDA or cellular phone further supplies device 100 with the capability to provide the single-use credit card number over an RF link and to verify the cardholder biometrically at the time of the transaction, providing the advantages described below. EX1004, 6:8-15, 12:9-16, 12:18-23; EX1003, ¶¶103-114.

A POSITA would have reasonably expected success in implementing device 100 as a PDA as described in Maes. EX1003, ¶¶103-114. Indeed, Walker's device 100 and Maes's PDA device 10 are portable, cardholder-carried devices having a central processor and a memory storing financial information. Implementing device 100 as a PDA combines known elements according to known methods to yield the predictable result of a portable device used to complete a purchase. EX1007, 5:52-54, 11:21-25; EX1004, 3:22-27; EX1003, ¶¶103-114. *See KSR*, 550 U.S. at 416.

In WMC, device 100 obtains a single-use credit card number pre-stored in memory 104 by performing the method of Walker's FIG. 10 according to Walker's second embodiment. EX1007, 11:21-25, 11:46-56; *generally id.*, 11:19-12:51;

EX1003, ¶¶103-114. The cardholder enters a biometric identifier (step 1001); device 100 determines whether that identifier is valid for the device (step 1002) and denies access if it is not (step 1004); and if the identifier is valid, device 100 searches memory 104 for a single-use credit card number (step 1003) and determines whether one is available (step 1005). EX1007, 11:47-55; EX1003, ¶¶103-114. In Walker's FIG. 10 method, device 100 then displays that number on display screen 102 (step 1007). EX1007, 11:55-56; EX1003, ¶¶103-114.

Further in WMC, (per Maes) device 100 provides the single-use credit card number only if the cardholder is biometrically verified at the time of the transaction. EX1004, 12:9-16, 12:18-23, FIG. 5; EX1003, ¶¶103-114. Per Maes, before providing that number, device 100 receives the cardholder's biometric information through biometric interface 105, compares that information against the biometric authentication information stored in memory 104 (step 206), determines whether the cardholder is an authorized user (step 208), and withholds the number if the cardholder is not biometrically verified (step 226). EX1004, 10:54-61, 11:9-13, 12:18-23, FIG. 5; EX1007, 5:58-61; EX1003, ¶¶103-114. Additionally, per Maes, at step 1007, device 100 provides the single-use credit card number over RF port 50 rather than displaying it on display screen 102. EX1007, 11:55-56; EX1004, 12:9-16; EX1003, ¶¶103-114. The WMC process is illustrated in part below.



EX1004, FIG. 5 (excerpt, modified); EX1007, FIG. 10 (excerpt, modified);

EX1003, ¶¶103-114.

A POSITA would have been motivated to provide the single-use credit card number over RF port 50 in place of displaying it on display screen 102 at step 1007. EX1003, ¶¶103-114. In Walker, the cardholder reads the single-use credit card number from display screen 102 and conveys it to the merchant, with Walker explaining that “[i]n step 1101, the cardholder provides the merchant with a single-use credit card number displayed on the device (see step 1007 of FIG. 10).” EX1007,

12:21-23. A POSITA would have recognized that manually reading and re-entering a credit card number is slow and prone to transcription errors. EX1003, ¶¶103-114.

Maes avoids such manual handling, explaining that a consumer transaction “may be performed by transmitting the selected card information directly from the PDA device to the ... POS transaction terminal,” and that (in that embodiment) “the PDA device 10 itself actually takes the place of the Universal Card 26.” EX1004, 12:9-16, 12:23-29. Therefore, a POSITA would have been motivated to provide the single-use credit card number over the PDA’s RF port 50 instead of merely displaying it. EX1003, ¶¶103-114.

A POSITA would have reasonably expected success, because in WMC, device 100 includes RF processor module 48 and RF port 50 to enable such transmissions. EX1004, 6:8-15, 12:9-16; EX1003, ¶¶103-114.

Additionally, to improve security, in WMC, a POSITA would have been motivated to perform transaction-time biometric verification (per Maes) in addition to device-access authorization (per Walker). EX1003, ¶¶103-114. Maes explains that “[a]nother disadvantage in using financial cards is that consumers are not fully protected from the unauthorized use of lost or stolen cards.” EX1004, 2:1-3. In WMC, device 100 is implemented as a PDA, and a POSITA would have recognized that after the cardholder activates the PDA and before a transaction is attempted, the PDA may be lost, stolen, or otherwise come into the possession of another person

without the cardholder's permission. EX1007, 5:56-61, 11:49-52; EX1004, 2:1-3, 2:23-30; EX1003, ¶¶103-114.

In response, Maes explains that the stored card information is not transmitted unless the user is biometrically verified at the time of the transaction, stating that “the CPU 12 of the PDA device 10 will prohibit the selected card information from being retrieved and transmitted to the transaction terminal 80 if the user is not biometrically verified and/or if the digital certificate is not valid (step 226).” EX1004, 12:18-23, FIG. 5; EX1003, ¶¶103-114. A POSITA would therefore have been motivated to require the cardholder to present biometric information again immediately before device 100 provides the single-use credit card number (per Maes), so that provision confirms the identity of the person actually transacting. EX1003, ¶¶103-114.

Further, WMC retains both Walker's and Maes's determinations, and each serves a distinct role. EX1003, ¶¶103-114. Walker's determination at step 1002 governs access to device 100, with Walker explaining that “[t]he device determines whether the identifier is valid for the device (step 1002); if not, access to the device is denied (step 1004).” EX1007, 11:49-52. The transaction-time verification drawn from Maes governs release of the single-use credit card number used in a transaction, with Maes explaining that “the CPU 12 of the PDA device 10 will prohibit the selected card information from being retrieved and transmitted to the transaction

terminal 80 if the user is not biometrically verified and/or if the digital certificate is not valid (step 226).” EX1004, 12:18-23. In WMC, device 100 performs both, and provides the single-use credit card number only if the cardholder is biometrically verified at the time of the transaction. EX1007, 11:49-52; EX1004, 12:18-23; EX1003, ¶¶103-114.

A POSITA would have reasonably expected success. EX1003, ¶¶103-114. Device 100 (per Walker) already includes biometric interface 105 for receiving the cardholder’s biometric information, and memory 104 already holds the biometric authentication information against which device 100 evaluates it. EX1007, 5:58-61, 11:47-52; *see also id.*, 12:18-23; EX1003, ¶¶103-114.

3. Claim Element Analysis

(a) [1.pre]

WMC renders [1.pre] obvious. EX1003, ¶¶211-214.

Walker describes “a device 100 for generating a single-use credit card number in accordance with this invention.” EX1007, 5:49-51. Walker further explains that “[t]his device is preferably a smart card,” and that “[t]he device has a keypad 103, a display screen 102, a memory 104 and a central processor 101.” EX1007, 5:51-54.

Maes describes “a portable information and transaction processing device (‘personal digital assistant’ or ‘PDA’) in which a user can store his or her credit card[] ... (i.e., financial) information, as well as personal information.” EX1004,

2:23-30. “Moreover, the functions and components of the PDA device 10 may be built into a cellular phone.” EX1004, 14:11-16.

In WMC, Walker’s device 100 is implemented as a PDA or cellular phone consistent with Maes’s teachings. EX1007, 5:49-51; EX1004, 2:23-30; EX1003, ¶214. WMC retains the keypad 103, display screen 102, memory 104 and central processor 101 Walker describes. EX1007, 5:51-54; EX1003, ¶214.

(b) [1.1]

Supra, Ground 1A at [1.1]; EX1003, ¶215. The Walker-Maes device includes Maes’s RF cellular circuitry. *Id.*

(c) [1.2]

Supra, Ground 1A at [1.2]; EX1003, ¶216. The Walker-Maes device includes Maes’s short-range RF circuitry. *Id.*

(d) [1.3.1]

WMC renders [1.3.1] obvious. EX1003, ¶¶217-221.

Walker explains that “the device memory 104 includes a database with a list of single-use credit card numbers and a flag for each number indicating whether the number has already been used,” and that “[t]he single-use credit card numbers are assigned to the cardholder by the credit card issuer.” EX1007, 11:21-25. The pre-stored single-use credit card numbers include ***transaction information***. EX1007, 11:21-25; EX1003, ¶218. Walker notes that various techniques for generating

single-use numbers can be used, including embedding within each single-use number *transaction information* in the form of a credit-card account number A. EX1007, 11:26-45. Walker permits card issuers to assign account numbers (*transaction information*) for credit card accounts in any suitable fashion, including assigning unique account numbers to different users. *Id.*; *see also id.*, 1:20-21, 6:54-59, 6:66-7:1, 8:20-26, Fig. 8.

Walker further explains that “the device may include a biometric interface 105, and be activated by the input of a suitable biometric record such as the cardholder’s fingerprint.” EX1007, 5:58-61. Walker states that “[i]n step 1001, the cardholder enters his unique identifier (for example, a PIN or biometric data) into the device.” EX1007, 11:47-49. Walker adds that “[t]he device determines whether the identifier is valid for the device (step 1002); if not, access to the device is denied (step 1004).” EX1007, 11:49-52. Thus, device 100 determines the validity of an “identifier” that is the biometric data the cardholder enters. EX1007, 11:47-52; EX1003, ¶219. A POSITA would have understood, or at minimum found obvious, that device 100 determines whether entered biometric data is valid for the device by comparing it to stored biometric authentication information. EX1007, 11:47-52; EX1003, ¶219. It further would have been understood or obvious that memory 104 holds the reference biometric information. EX1003, ¶219.

To the extent Walker does not expressly recite storing that reference information, Maes does. *Supra*, Ground 1A at [1.3.1]. Maes describes processing biometric data “by comparing the current biometric voice data with the user’s voice models stored in memory 14.” EX1004, 10:57-61. Applying Maes’s suggestion to store the reference biometric authentication information in the memory of Walker’s device would have been obvious to permit the user’s current biometric input to be compared with the stored reference biometric authentication information on device in an efficient manner without needing to access off-device storage. EX1003, ¶220.

Therefore, in WMC, it would have been obvious for the memory (e.g., memory 104) to store both the biometric authentication information and the single-use credit card numbers. EX1007, 11:21-25, 11:47-52; EX1004, 10:57-61; EX1003, ¶221.

(e) [1.3.2]

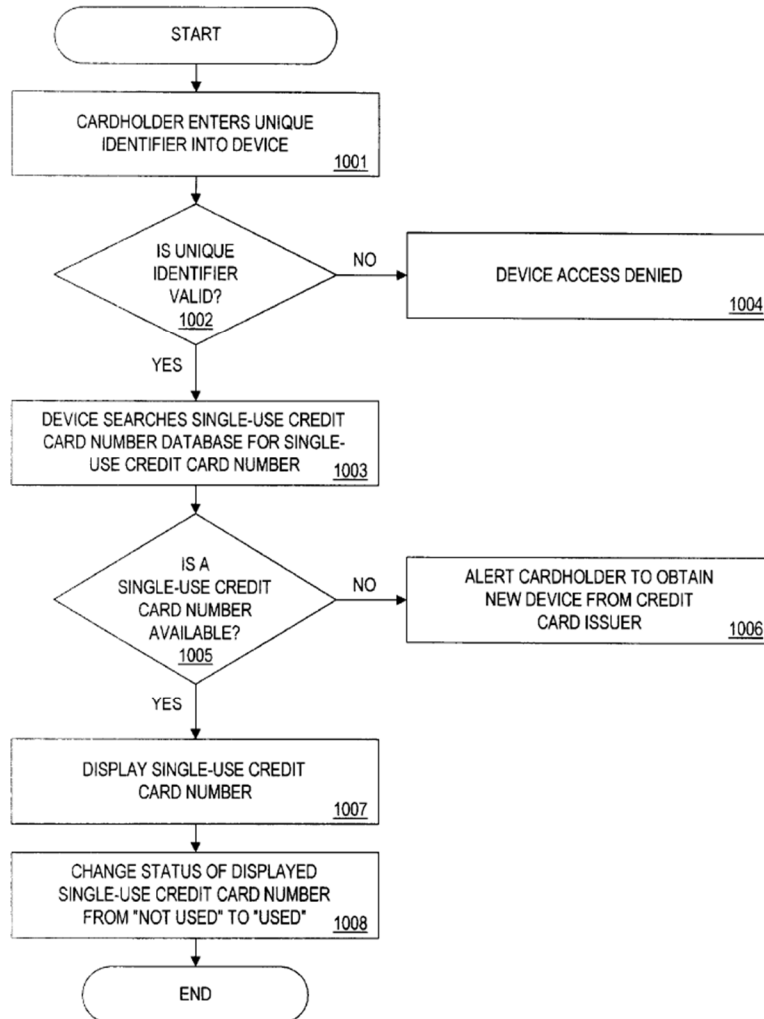
WMC renders [1.3.2] obvious. EX1003, ¶¶222-226.

In Walker, the biometric authentication information and the transaction information are stored in advance on the same device for the same user. EX1003, ¶223. Walker explains that the single-use credit card numbers including account numbers (*transaction information*) held in memory 104 “are assigned to the cardholder by the credit card issuer.” EX1007, 11:21-25. Memory 104 also holds the biometric authentication information against which device 100 evaluates the

identifier the cardholder enters. *Supra*, [1.3.1]. Because Walker refers throughout to a single cardholder who possesses device 100, holds the numbers assigned to that cardholder, and enters an identifier valid for that device, a POSITA would have understood that the cardholder who enters that identifier is the same cardholder to whom the issuer assigned the stored numbers. EX1007, 11:21-25, 11:47-52; EX1003, ¶223.

Walker further explains that “[i]f the identifier is valid, the device searches the single-use credit card number database in the device memory 104 for a single-use credit card number (step 1003).” EX1007, 11:52-54. Because step 1003 searches a database of numbers held in memory 104, and step 1002 evaluates the entered identifier against biometric authentication information held in memory 104, a POSITA would have understood that both are present in memory 104 before the cardholder enters an identifier at step 1001 (which precedes steps 1002 and 1003). EX1007, 11:21-25, 11:47-54; EX1003, ¶224. The biometric authentication information and single-use card number database, including the account numbers, are also associated insofar as Walker only permits access to the device, and therefore to the account numbers, if the user is biometrically authenticated by comparison of a user’s current biometric to the reference biometric stored in memory. EX1007, 5:58-61, 6:19-29, 11:46-52. Likewise, per Maes, in WMC, the biometric authentication information is used in the transaction-time user verification operation.

The stored biometric authentication information thus functionally gates access to the single-use card numbers (including the account number in the single-user numbers) based on the association. EX1003, ¶224. It would have been obvious for the device to store data linking the biometric authentication information to the single-user numbers (including the account number) to enable more efficient authentication and access to the single-use numbers. *Id.*



EX1007, FIG. 10.

Maes corroborates Walker's approach. *Supra*, Ground 1A at [1.3.2].

Therefore, in WMC, memory 104 stores, in advance and for the same cardholder, the biometric authentication information and the transaction information. EX1007, 11:21-25, 11:47-54; EX1004, 10:49-51; EX1003, ¶226.

Accordingly, the biometric authentication information has been previously associated with the transaction information. EX1003, ¶226.

(f) [1.4]

WMC renders [1.4] obvious. EX1003, ¶¶227-230.

Walker explains that “the device may include a biometric interface 105, and be activated by the input of a suitable biometric record such as the cardholder’s fingerprint.” EX1007, 5:58-61. Walker further states that “[i]n step 1001, the cardholder enters his unique identifier (for example, a PIN or biometric data) into the device.” EX1007, 11:47-49. Because biometric interface 105 receives the cardholder’s fingerprint as input to device 100, a POSITA would have understood that biometric interface 105 reads biometric information and is therefore a biometric reading device. EX1007, 5:58-61, 11:47-49; EX1003, ¶228.

Maes corroborates Walker’s approach. *Supra*, Ground 1A at [1.4].

Therefore, in WMC, biometric interface 105 is a biometric reading device configured to read biometric information. EX1007, 5:58-61, 11:47-49; EX1004, 5:54-60; EX1003, ¶230.

(g) [1.5]

WMC renders [1.5] obvious. EX1003, ¶¶231-237.

During prosecution, the applicant explained that the device compares the biometric information the user inputs against stored biometric authentication

information that was previously associated with the transaction information, writing that “[t]he device can compare the biometric information input by the user with the stored biometric authentication information, which has already been associated with the transaction information.” EX1002, 41. The applicant added that “verification of the user’s identity allows the device to also authenticate the user’s authorization with respect to the stored transaction information.” EX1002, 41. The applicant placed that comparison on the device itself, explaining that “in other embodiments, the biometric reading device is included in the mobile device, thus enabling the authentication process to be performed entirely on the device.” EX1002, 41-42.

WMC performs those steps. EX1003, ¶233. The biometric authentication information stored in memory 104 has been previously associated with the transaction information stored in memory 104. *Supra*, [1.3.2].

Per Walker, WMC includes the component that performs that comparison, explaining that “[t]he device has a keypad 103, a display screen 102, a memory 104 and a central processor 101.” EX1007, 5:52-54; EX1003, ¶234. Walker further explains that “[i]n step 1001, the cardholder enters his unique identifier (for example, a PIN or biometric data) into the device,” and that “[t]he device determines whether the identifier is valid for the device (step 1002); if not, access to the device is denied (step 1004).” EX1007, 11:47-52. Because device 100 determines at step 1002 whether the biometric data entered at step 1001 is valid, and makes that

determination against the biometric authentication information held in memory 104, a POSITA would have understood that central processor 101 compares the biometric information read by biometric interface 105 against the biometric authentication information stored in memory. EX1007, 5:51-54, 11:47-52; EX1003, ¶234. *Supra*, [1.3.1].

Per Maes, WMC performs that comparison again when the cardholder attempts a transaction and withholds the transaction information unless the comparison succeeds. EX1003, ¶235. *Supra*, §V.D.2. Maes describes “a biometric processor module 22 for processing biometric data in addition to, or alternative to voice data, to provide user verification.” EX1004, 5:8-14. Maes explains that “the CPU 12 of the PDA device 10 will prohibit the selected card information from being retrieved and transmitted to the transaction terminal 80 if the user is not biometrically verified and/or if the digital certificate is not valid (step 226).” EX1004, 12:18-23. Because Maes prohibits the stored card information from being retrieved and transmitted to transaction terminal 80 unless the user is biometrically verified against the biometric authentication information stored in memory 14, a POSITA would have understood that Maes performs its biometric verification when the user attempts to perform a transaction and permits the stored card information to be provided only when that verification succeeds. EX1004, 12:18-23; EX1003, ¶235. *Supra*, Ground 1A at [1.5].

In WMC, when the cardholder attempts to perform a transaction, central processor 101 compares the biometric information read by biometric interface 105 against the biometric authentication information stored in memory 104 and prohibits the transaction information from being provided if that comparison does not succeed. EX1007, 5:51-54, 11:47-52; EX1004, 12:18-23; EX1003, ¶236. Further, in WMC, a successful comparison confirms that the biometric information read by biometric interface 105 matches the biometric authentication information in memory 104. EX1007, 11:47-52; EX1003, ¶236. That biometric authentication information was previously associated with the transaction information in memory 104. EX1007, 11:21-25; EX1003, ¶236. *Supra*, [1.3.2]. Central processor 101 therefore authenticates that the biometric information read by biometric interface 105 is associated with the transaction information and does so based at least in part on the biometric authentication information stored in memory 104 (*supra*, [1.3.1]). EX1007, 11:47-52; EX1004, 12:18-23; EX1003, ¶236. A POSITA would therefore have understood that central processor 101 (which performs the biometric comparison) is an authentication module. EX1003, ¶236.

Therefore, in WMC, central processor 101 provides an authentication module configured to authenticate, during a transaction, that the biometric information read by biometric interface 105 is associated with the transaction information, based at

least in part on the biometric authentication information stored in memory 104. EX1007, 5:51-54, 11:47-52; EX1004, 12:18-23; EX1003, ¶237.

(h) [1.6.1]

WMC renders [1.6.1] obvious. EX1003, ¶¶238-242.

Walker explains that “[i]f a single-use credit card number is available (step 1005), it is displayed on the device display screen 102 (step 1007)”. EX1007, 11:55-56. Walker further explains that “[i]n step 1101, the cardholder provides the merchant with a single-use credit card number displayed on the device (see step 1007 of FIG. 10).” EX1007, 12:21-23. Because device 100 retrieves the single-use credit card number from memory 104 (step 1003) and that number is provided to the merchant to complete the transaction (step 1007), a POSITA would have understood that device 100 provides the transaction information for use in a transaction. EX1007, 11:52-56, 12:21-23; EX1003, ¶239.

Per Maes, WMC transmits the transaction information over a short range RF link. EX1003, ¶240. Maes explains that “the consumer transaction may be performed by transmitting the selected card information directly from the PDA device to the ... POS transaction terminal through an established communication link L2 (step 228, FIG. 3) (i.e., via the serial port 42, the parallel port 44 modem 42, the IR port 54 or the RF port 50), rather than retrieving and writing card information to the Universal Card 26.” EX1004, 12:9-16. Maes further explains that “the device may preferably

be equipped with an RF processor module 48, operatively connected between the CPU 12 and an RF port 50, for processing incoming RF information received by the RF port 50, and for generating transmission signals which are outputted from the RF port 50 using conventional constructions and techniques.” EX1004, 6:8-15. RF port 50 and RF processor module 48 are short range RF circuitry. EX1003, ¶240. *Supra*, [1.2].

In WMC, device 100 provides the single-use credit card number retrieved at step 1003 to the transaction terminal over RF port 50, in place of displaying it on display screen 102 at step 1007. EX1007, 11:52-56; EX1004, 6:8-15, 12:9-16; EX1003, ¶241. *Supra*, §V.D.2. Because central processor 101 passes that number to RF processor module 48, which generates the transmission signals output from RF port 50, a POSITA would have understood that those components are a transaction module. EX1004, 6:8-15; EX1003, ¶241.

Therefore, in WMC, a transaction module provides the transaction information via short range RF circuitry for use in a transaction. EX1007, 11:52-56, 12:21-23; EX1004, 6:8-15, 12:9-16; EX1003, ¶242.

(i) [1.6.2]

WMC renders [1.6.2] obvious. EX1003, ¶¶243-246.

In Walker, device 100 retrieves the stored transaction information only after the cardholder’s biometric information is determined valid, with Walker explaining

that “[t]he device determines whether the identifier is valid for the device (step 1002); if not, access to the device is denied (step 1004),” and that “[i]f the identifier is valid, the device searches the single-use credit card number database in the device memory 104 for a single-use credit card number (step 1003).” EX1007, 11:49-54. *Supra*, [1.5].

Per Maes, WMC makes a complementary determination when the cardholder attempts a transaction. EX1003, ¶245. *Supra*, §V.D.2. Maes explains that “the CPU 12 of the PDA device 10 will prohibit the selected card information from being retrieved and transmitted to the transaction terminal 80 if the user is not biometrically verified and/or if the digital certificate is not valid (step 226).” EX1004, 12:18-23. Because Maes prohibits the stored card information from being retrieved and transmitted to transaction terminal 80 unless the user is biometrically verified against the biometric authentication information stored in memory 14, a POSITA would have understood that Maes performs its biometric verification when the user attempts to perform a transaction and permits the stored card information to be provided only when that verification succeeds. EX1004, 12:18-23; EX1003, ¶245.

In WMC, the transaction module provides the single-use credit card number over RF port 50 only when the authentication (performed by central processor 101 for that transaction) of the cardholder’s biometric information succeeds at the time of the transaction. EX1007, 11:52-56; EX1004, 12:18-23; EX1003, ¶246. *Supra*,

[1.5], [1.6.1]. Therefore, in WMC, the transaction module provides the *transaction information* (the single-use credit card number's account number) when central processor 101 successfully authenticates that the cardholder's biometric information matches the biometric authentication information previously associated with that transaction information (*successfully authenticated as being associated with the transaction information by the authentication module*). EX1007, 11:49-54; EX1004, 12:18-23; EX1003, ¶246.

(j) [2]

WMC renders [2] obvious. EX1003, ¶¶247-250.

In WMC, Walker's biometric interface 105 is the biometric reading device. *Supra*, [1.4]. Walker explains that "the device may include a biometric interface 105, and be activated by the input of a suitable biometric record such as the cardholder's fingerprint." EX1007, 5:58-61. Because biometric interface 105 receives the cardholder's fingerprint as the biometric record input to device 100, a POSITA would have understood that biometric interface 105 is a fingerprint reading device. EX1007, 5:58-61; EX1003, ¶248.

Maes corroborates Walker's approach. *Supra*, Ground 1A at [2].

Therefore, in WMC, the biometric reading device is a fingerprint reading device. EX1007, 5:58-61; EX1004, 10:66-11:5; EX1003, ¶250.

(k) [3]

WMC renders [3] obvious. EX1003, ¶¶251-253.

The account number in the single-use credit card numbers (WMC's transaction information) incorporate the cardholder's credit card account number. EX1007, 11:21-25, 11:32-36; EX1003, ¶252. *Supra*, [1.3.1]. Walker explains that "the credit card company would decide upon the size of the nonce (N bits), the account number (A bits), and the size of the IV (m bits) so that $n+a+m=r$," and that "[t]he account number would include those bits assigned by the central authority." EX1007, 11:32-36. A POSITA would have understood that a cardholder's credit card account number is credit card information. EX1003, ¶252.

Therefore, in WMC, the transaction information is generated based at least in part on credit card information. EX1007, 11:32-36; EX1003, ¶253.

(l) [5]

Supra, Ground 1A at [5]; EX1003, ¶254.

(m) [6]

Supra, Ground 1A at [6]; EX1003, ¶255.

(n) [8]

WMC renders [8] obvious. EX1003, ¶¶256-258.

WMC's transaction module provides the single-use credit card number's account number (*transaction information*) via the short range RF circuitry for use in the transaction. *Supra*, [1.6.1].

In WMC, neither the transaction module nor any other component of the mobile device transmits the biometric information for use in a transaction. EX1003, ¶258. Walker explains that “[t]he device determines whether the identifier is valid for the device (step 1002); if not, access to the device is denied (step 1004).” EX1007, 11:49-52. Because device 100 determines whether the identifier the cardholder enters is valid *for the device*, a POSITA would have understood and found obvious that the biometric data entered at step 1001 is evaluated within device 100 and is not output from device 100. EX1007, 11:47-52; EX1003, ¶258. *Supra*, [1.5]; *supra*, Ground 1A at [8].

(o) [9.pre]

Supra, Ground 2A at [1.pre]; EX1003, ¶259.

(p) [9.1]

Supra, Ground 2A at [1.1]; EX1003, ¶260.

(q) [9.2]

Supra, Ground 2A at [1.2]; EX1003, ¶261.

(r) [9.3.1]

Supra, Ground 2A at [1.3.1]; EX1003, ¶262.

(s) [9.3.2]

Supra, Ground 2A at [1.3.2]; EX1003, ¶263.

(t) [9.4]

Supra, Ground 2A at [1.4]; EX1003, ¶264.

(u) [9.5]

Supra, Ground 2A at [1.5]; EX1003, ¶265.

(v) [9.6.1]

Supra, Ground 2A at [1.6.1]; EX1003, ¶266.

(w) [9.6.2]

Supra, Ground 2A at [1.6.2]; EX1003, ¶267.

(x) [9.7]

Supra, Ground 2A at [5]; EX1003, ¶268.

(y) [10]

Supra, Ground 2A at [2]; EX1003, ¶269.

(z) [11]

Supra, Ground 2A at [3]; EX1003, ¶270.

(aa) [13]

Supra, Ground 2A at [6]; EX1003, ¶271.

(bb) [15]

Supra, Ground 2A at [8]; EX1003, ¶272.

(cc) [16.pre]

WMC renders [16.pre] obvious. EX1003, ¶¶273-275.

Maes explains that “the functions and components of the PDA device 10 may be built into a cellular phone, whereby communication with the central server 60 may be achieved through a cellular communication channel, which may be analog or digital (e.g., CDMA, GSM, etc.).” EX1004, 14:12-16. *Supra*, Ground 1A at [16.pre].

In WMC, Walker’s device 100 is implemented as a PDA built according to Maes’s teachings. *Supra*, [1.pre]. Because Maes describes the functions and components of PDA device 10 being built into a cellular phone, a POSITA would have understood that such a device 100 is a cellular telephone. EX1004, 14:12-16; EX1003, ¶275. *Supra*, [1.1].

(dd) [16.1]

Supra, Ground 2A at [1.1]; EX1003, ¶276.

(ee) [16.2]

Supra, Ground 2A at [1.2]; EX1003, ¶277.

(ff) [16.3.1]

Supra, Ground 2A at [1.3.1]; EX1003, ¶278.

(gg) [16.3.2]

Supra, Ground 2A at [1.3.2]; EX1003, ¶279.

(hh) [16.4]

Supra, Ground 2A at [1.4]; EX1003, ¶280.

(ii) [16.5]

Supra, Ground 2A at [1.5]; EX1003, ¶281.

(jj) [16.6.1]

Supra, Ground 2A at [1.6.1]; EX1003, ¶282.

(kk) [16.6.2]

Supra, Ground 2A at [1.6.2]; EX1003, ¶283.

(ll) [17]

Supra, Ground 2A at [2]; EX1003, ¶284.

(mm) [18]

Supra, Ground 2A at [5]; EX1003, ¶285.

(nn) [19]

Supra, Ground 2A at [6]; EX1003, ¶286.

(oo) [20]

Supra, Ground 2A at [3]; EX1003, ¶287.

(pp) [23]

Supra, Ground 2A at [8]; EX1003, ¶288.

E. Ground 2B: Walker-Maes-Dorf Renders Obvious Claims 4, 12, and 21

1. The Walker-Maes-Dorf Combination (WMDC)

Walker discloses single-use credit card numbers that can be used for credit card transactions. *Supra*, Ground 2A, [1.3.1]. Walker does not disclose an exhaustive list of payment card types that its single use numbers could be used for, but Dorf explains that payment cards can be attached to a loyalty program. *Supra*, §V.B.1. A POSITA would have found it obvious to attach a loyalty program like that described in Dorf to the credit card accounts disclosed in Walker, and a POSITA would have been motivated and reasonably expected success in pursuing this Walker-Maes-Dorf combination (WMDC) for substantially similar reasons to those discussed above in Ground 1B. *Supra*, §V.B.2.

2. Claim Element Analysis

(a) [4]

WMDC renders [4] obvious for reasons analogous to Ground 1B, at [4]. EX1003, ¶289. In WMDC, the single-use card numbers are associated with a loyalty program for a rewards card, and the single-use card number is thus generated based at least in part on rewards card information. EX1009, 9:25-10:6, 12:22-27, 20:60-64; EX1003, ¶289.

(b) [12]

Supra, Ground 2B at [4]; EX1003, ¶290.

(c) [21]

Supra, Ground 2B at [4]; EX1003, ¶291.

F. Ground 2C: Walker-Maes-Shults Renders Obvious Claims 7, 14, and 22

1. The Walker-Maes-Shults Combination (WMSC)

The Walker-Maes-Shults Combination (WMSC) is WMC (Ground 2A), further modified in view of Shults's teachings such that the RF circuitry in WMC's mobile device is implemented using an RFID device. *Supra*, §V.C.1-2; EX1008, [0030]; EX1003, ¶¶116-117. For the reasons described in §V.C.2, a POSITA would have been motivated to add Shults's RFID circuit to WMC's mobile device and would have reasonably expected success. *Supra*, §V.C.2; EX1003, ¶¶116-117.

WMSC mobile device otherwise operates as in WMC, including transmitting the single-use credit card number to a POS terminal via short range RF circuitry. *Supra*, §V.D.2; EX1008, [0030]; EX1003, ¶¶116-117.

2. Claim Element Analysis

(a) [7]

WMSC renders [7] obvious for reasons analogous to Ground 1C, at [7]. EX1008, [0030]; EX1003, ¶292.

(b) [14]

Supra, Ground 2C at [7]; EX1003, ¶293.

(c) [22]

Supra, Ground 2C at [7]; EX1003, ¶294.

VI. PAYMENT OF FEES—37 C.F.R. §42.103

Petitioners authorize the Patent and Trademark Office to charge any fees to Deposit Account No. 06-1050.

VII. MANDATORY NOTICES—37 C.F.R. § 42.8(a)(1)

A. Real Party-In-Interest—37 C.F.R. § 42.8(b)(1)

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

B. Related Matters—37 C.F.R. § 42.8(b)(2)

Petitioners are not aware of any disclaimers, reexamination certificates or petitions for inter partes review for the '807 Patent. The '807 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—37 C.F.R. § 42.8(b)(3)

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: IPR50095-0308IP1@fr.com	Nicholas Stephens, Reg. No. 74,320 Andrew B. Patrick, Reg. No. 63,471 Jeremy J. Monaldo, Reg. No. 58,680 Craig A. Deutsch, Reg. No. 69,264 Usman A. Khan, Reg. No. 70,439 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 IPR50095-0308IP1@fr.com

D. Service Information

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

Petitioners consent to electronic service by email at IPR50095-0308IP1@fr.com.

Respectfully submitted,

Dated: September 18, 2026

/W. Karl Renner/

W. Karl Renner, Reg. No. 41,265
Nicholas Stephens, Reg. No. 74,320
Andrew B. Patrick, Reg. No. 63,471
Jeremy J. Monaldo, Reg. No. 58,680
Craig A. Deutsch, Reg. No. 69,264
Usman A. Khan, Reg. 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. IPR2026-00499)

Counsel for Petitioners

CERTIFICATION UNDER 37 CFR § 42.24

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter partes* Review totals 13,953 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated: September 18, 2026

/W. Karl Renner/

W. Karl Renner, Reg. No. 41,265
Nicholas Stephens, Reg. No. 74,320
Andrew B. Patrick, Reg. No. 63,471
Jeremy J. Monaldo, Reg. No. 58,680
Craig A. Deutsch, Reg. No. 69,264
Usman A. Khan, Reg. 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 CFR §§ 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