

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Francisco Martinez de Velasco Cortina, et al.
U.S. Patent No.: 10,706,412
Issue Date: July 7, 2020
Appl. Serial No.: 14/639,034
Filing Date: March 4, 2015
Title: SYSTEM AND METHODS 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. 10,706,412
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 '412 PATENT	2
A.	Summary	2
B.	Prosecution History.....	3
III.	LEVEL OF ORDINARY SKILL	4
IV.	CLAIM CONSTRUCTION—37 C.F.R. §42.104(b)(3)	4
V.	THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	5
A.	Ground 1A: Maes Renders Obvious Claims 1-3	6
1.	Maes (EX1004)	6
2.	Claim Analysis	7
B.	Ground 1B: Maes-Niwa Renders Obvious Claims 1-3	42
1.	Niwa (EX1005)	42
2.	The Maes-Niwa Combination	43
3.	Claim Analysis	46
C.	Ground 2: Maes-Bjorn Renders Obvious Claims 1-3	51
1.	Bjorn (EX1006).....	51
2.	The Maes-Bjorn Combination.....	53
3.	Claim Element Analysis.....	59
D.	Ground 3A: Maes-Walker Renders Obvious Claims 1-7	66
1.	Walker (EX1007)	66
2.	The Maes-Walker Combination	66
3.	Claim Element Analysis.....	67
E.	Ground 3B: Maes-Niwa-Walker Renders Obvious Claims 4-7	78
F.	Ground 3C: Maes-Bjorn-Walker Renders Obvious Claims 4-7.....	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).....	80
D.	Service Information	81

LIST OF EXHIBITS

EX1001	U.S. Patent No. 10,706,412 to de Velasco Cortina, et al. (the “’412 Patent”)
EX1002	The Prosecution History of the ’412 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	U.S. Patent No. 6,453,301 to Niwa (“Niwa”)
EX1006	U.S. Patent No. 6,035,398 to Bjorn (“Bjorn”)
EX1007	U.S. Patent No. 6,163,771 to Walker et al. (“Walker”)
EX1008	U.S. Patent Application Publication No. 2002/0011519 to Shults (“Shults”)
EX1009	RESERVED
EX1010	U.S. Patent No. 6,434,159 to Woodward, et al. (“Woodward”)
EX1011	U.S. Patent No. 6,848,048 to Holmes (“Holmes”)
EX1012	U.S. Patent No. 6,934,689 to Ritter et al. (“Ritter”)
EX1013	U.S. Patent No. 6,796,490 to Drummond et al. (“Drummond”)
EX1014	U.S. Patent Application Publication No. 2002/0157029 to French et al. (“French”)
EX1015	U.S. Patent No. 5,613,012 to Hoffman, et al. (“Hoffman”)
EX1016-1017	RESERVED

EX1018	U.S. Patent No. 6,028,950 to Merjanian ("Merjanian")
EX1019	U.S. Patent No. 6,125,192 to Bjorn, et al. ("Bjorn-192")
EX1020	U.S. Patent No. 6,337,919 to Dunton ("Dunton")
EX1021	U.S. Patent No. RE36,788E ("Mansvelt")
EX1022	U.S. Patent No. 6,098,053 ("Slater")
EX1023-1029	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
EX1035	U.S. Patent No. 5,698,836 to Fujioka ("Fujioka")
EX1036	U.S. Provisional Application No. 60/304,216 to Williamson, et al. ("Berardi Prov.")
EX1037	U.S. Patent Application Publication No. 2004/0049451 to Berardi, et al. ("Berardi App.")
EX1038	U.S. Patent No. 6,213,391 to Lewis ("Lewis")

EX1039 U.S. Patent No. 5,832,090 to Raspotnik (“Raspotnik”)

LISTING OF CLAIMS

Element	Claim Language
[1.pre]	A mobile device, comprising:
[1.1]	short range radio frequency (RF) circuitry;
[1.2.1]	a memory coupled to the short range RF circuitry and configured to store biometric authentication information and payment information,
[1.2.2]	wherein the biometric authentication information is associated with a user associated with the payment information;
[1.3]	a biometric reading device configured to read biometric information; and
[1.4.1]	one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device,
[1.4.2]	the one or more processors configured to execute instructions stored in the memory that, when executed by the one or more processors, causes the one or more processors to perform operations of:
[1.5.1]	establishing a connection with a point of sale (POS) device, via the short range RF circuitry,
[1.5.2]	wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,
[1.6]	prompting the user to provide biometric information to the biometric reading device,
[1.7]	authenticating that the biometric information read by the biometric reading device is associated with the user associated with the payment information based on the biometric authentication information stored in the memory,
[1.8]	in response to the authentication, generating a key,

[1.9]	securing the payment information stored in the memory, and
[1.10]	transmitting to the POS device, via the short range RF circuitry, the key and the secured payment information for use in the secure transaction.
[2]	The mobile device of claim 1, wherein the payment information is associated with a primary account number.
[3]	The mobile device of claim 1, wherein the biometric authentication information is stored separately from the secured payment information.
[4.pre]	A system, comprising:
[4.1]	a mobile device, comprising: short range radio frequency (RF) circuitry;
[4.2.1]	a memory configured to store biometric authentication information and payment information,
[4.2.2]	wherein the biometric authentication information is associated with a user associated with the payment information;
[4.3]	a biometric reading device configured to read biometric information;
[4.4.1]	one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device,
[4.4.2]	the one or more processors configured to execute instructions stored in the memory that, when executed by the one or more processors, causes the one or more processors to perform operations of:
[4.5.1]	establishing a connection with a point of sale (POS) device, via the short range RF circuitry,
[4.5.2]	wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,

[4.6]	prompting the user to provide biometric information to the biometric reading device,
[4.7]	authenticating that the biometric information read by the biometric reading device is associated with the user associated with the payment information based at least in part on the biometric authentication information stored in the memory,
[4.8]	in response to authenticating, generating a key,
[4.9]	securing the payment information stored in the memory, and
[4.10]	transmitting to the POS device, via the short range RF circuitry, the key and the secured payment information for use in the secure transaction;
[4.11]	the POS device comprising at least one memory and at least one processor operably coupled to the at least one memory of the POS device, the at least one memory of the POS device storing instructions that, when executed by the at least one processor of the POS device causes the at least one processor of the POS device to perform operations of:
[4.12]	receiving, from the mobile device, the secured payment information and the key; and
[4.13]	transmitting the key and the secure payment information based to a central database; and
[4.14]	the central database comprising at least one memory and at least one processor operably coupled to the memory of the central database, the at least one memory of the central database storing instructions that, when executed by the at least one processor of the central database causes the at least one processor of the central database to perform operations of:
[4.15]	receiving, from the POS, the secured payment information and the key; and

[4.16]	validating the key and the secured payment information to complete the secured transaction.
[5]	The system of claim 4, wherein the payment information is associated with a primary account number.
[6]	The system of claim 4, wherein the POS device includes an RF reader.
[7]	The system of claim 4, wherein the biometric authentication information is stored separately from the secured payment information.

Apple Inc. (“Apple”) and Samsung Electronics Co., Ltd. (“Samsung”) (collectively, “Petitioners”) petition for IPR of claims 1-7 (“Challenged Claims”) of U.S. Patent No. 10,706,412 (“the ’412 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 ’412 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, ¶¶1-32, 37-49, *generally*).

Ground	Claims	Prior Art Basis
1A	1-3	§103 - Maes (EX1004)
1B	1-3	§103 - Maes in view of Niwa (EX1005)
2	1-3	§103 - Maes in view of Bjorn (EX1006)
3A	1-7	§103 - Maes in view of Walker (EX1007)

Ground	Claims	Prior Art Basis
3B	4-7	§103 - Maes in view of Niwa and Walker
3C	4-7	§103 - Maes in view of Bjorn and Walker

The '412 Patent was filed on March 4, 2015 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-3C 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)
Niwa (EX1005)	01/23/2000	09/17/2002	§102(e)
Bjorn (EX1006)	11/14/1997	03/07/2000	§102(a), (b), (e)
Walker (EX1007)	08/28/1997	12/19/2000	§102(a), (b), (e)

II. THE '412 PATENT

A. Summary

The '412 Patent discloses an “RF cellular telephone [that] can 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 EX1003, ¶¶51-58.

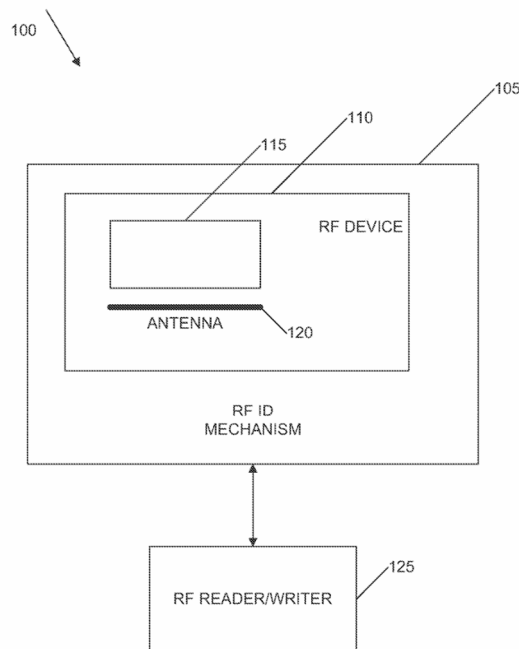


FIG. 1

EX1001, Fig. 1.

B. Prosecution History

The Office issued the '412 Patent on July 7, 2020. EX1002, 813-814; EX1003, ¶¶59-71. However, the Examiner mistakenly concluded that the prior art “do[es] not teach solely or in combination all of the claim limitations as disclosed in” the independent claims. EX1002, 816-819.

As demonstrated below, prior art that was of record during prosecution plainly discloses and renders obvious these and all other features of the Challenged Claims. *See, e.g.*, EX1004 (Maes), 2:53-4:64; EX1007 (Walker), 7:29-37, 8:11-14, 8:56-58,

Fig. 8; EX1002, 324; EX1001, Page 2 (listing “Maes” (EX1004) and “Walker” (EX1007) and confirming that Maes was not “cited by examiner”).

III. LEVEL OF ORDINARY SKILL

A person of ordinary skill in the art (“POSITA”) relating to the ’412 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
“payment information” (Claims 1-5, 7)	“information used to process a transaction that includes at least credit card information”

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

--	--

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, ¶72. Petitioners reserve the right to respond to any construction offered by Patent Owner or adopted by the Board.

V. THE CHALLENGED CLAIMS ARE UNPATENTABLE

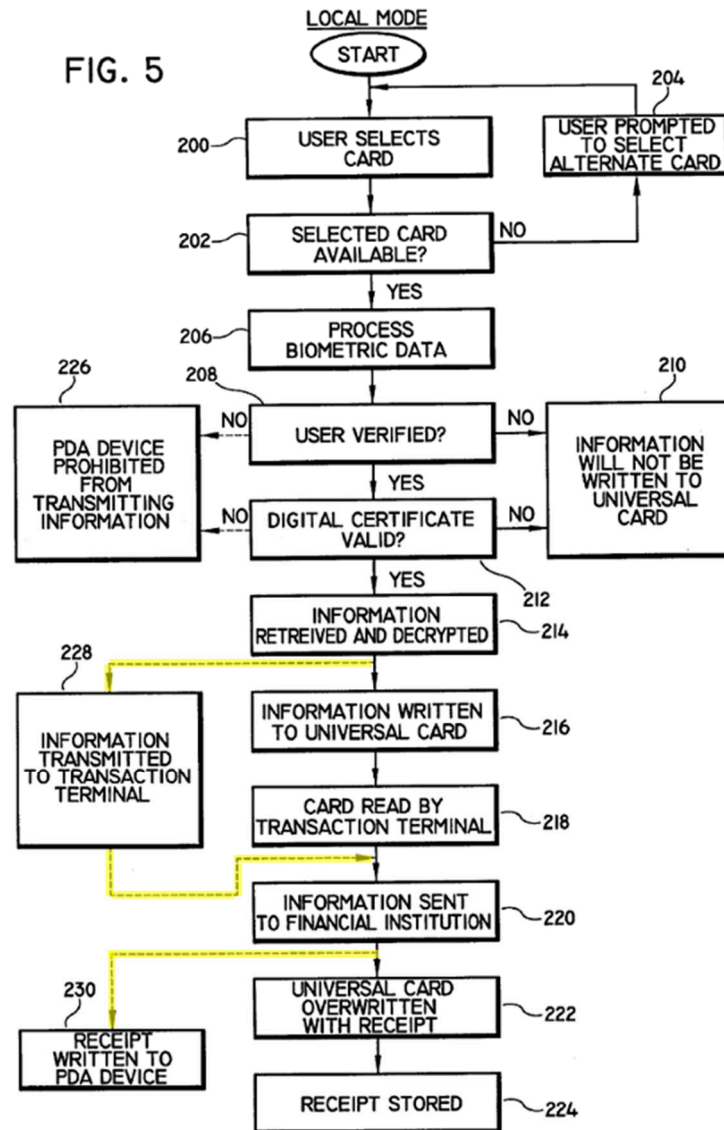
Grounds 1A-3C below demonstrate that the Challenged Claims of the '412 Patent would have been obvious to a POSITA before the Critical Date based on prior-art combinations involving Maes, Niwa, Bjorn, and Walker. Each of these references is analogous art in the same field as the '412 Patent (*e.g.*, secure transactions and communications) and/or reasonably pertinent to problem(s) purportedly addressed by the '412 Patent (*e.g.*, verifying or authenticating users in secure transactions). *See* EX1001, 1:7-12, 13:6-26, 14:4-11; EX1004, 1:10-17; EX1005, 5:51-6:58, Abst.; EX1006, 1:5-51, Abst.; EX1007, 1:6-10, 3:59-4:4, Abst.; EX1003, ¶¶85, 320-321.

A. Ground 1A: Maes Renders Obvious Claims 1-3

1. Maes (EX1004)

Maes describes 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; EX1003, ¶¶75-84.

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, 12:5-13.



EX1004, Fig. 5 (highlighting added).

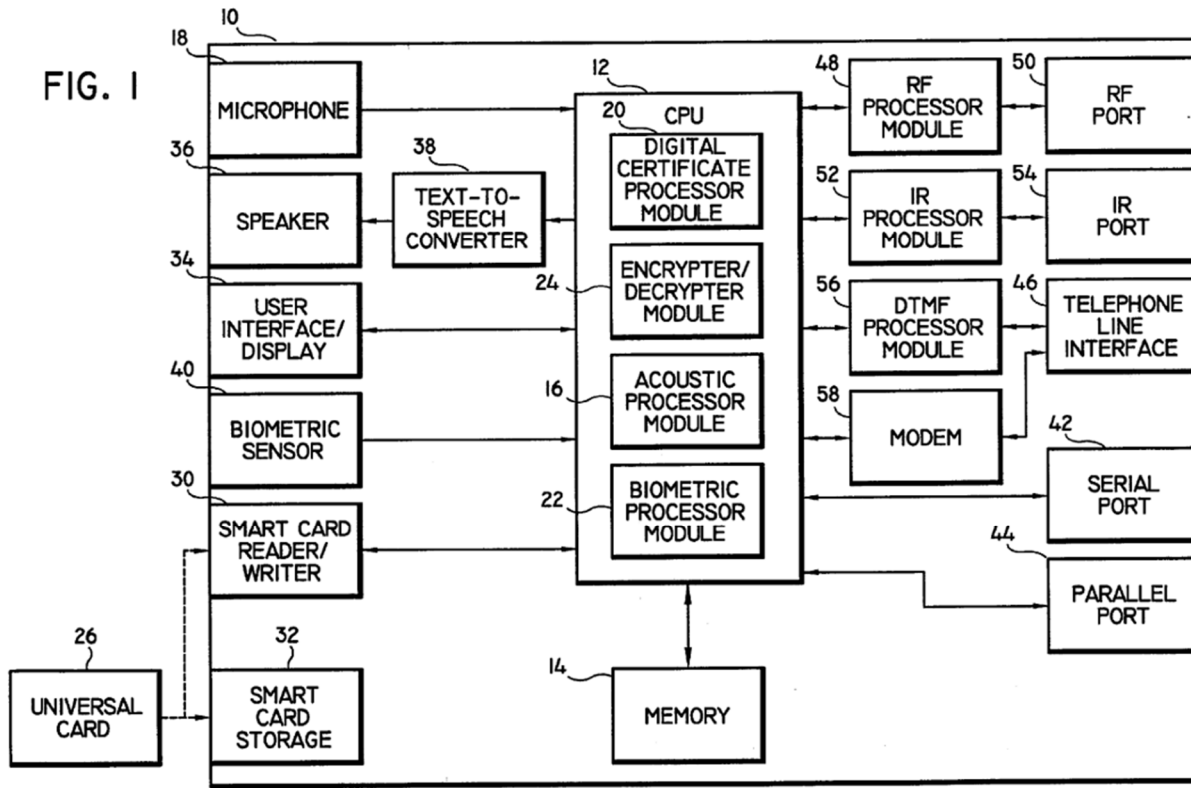
“Upon biometric verification ... selected card information” is “used to initiate a consumer transaction.” EX1004, Abstract.

2. Claim Analysis

(a) [1.pre]

Maes renders [1.pre] obvious. EX1003, ¶¶128-130.

For example, Maes discloses a “portable client PDA” (*mobile device*), e.g., PDA device 10 depicted in Fig. 1 below. EX1004, Abstract, 4:65-6:27; EX1003, ¶129.



EX1004, Fig. 1; EX1003, ¶129.

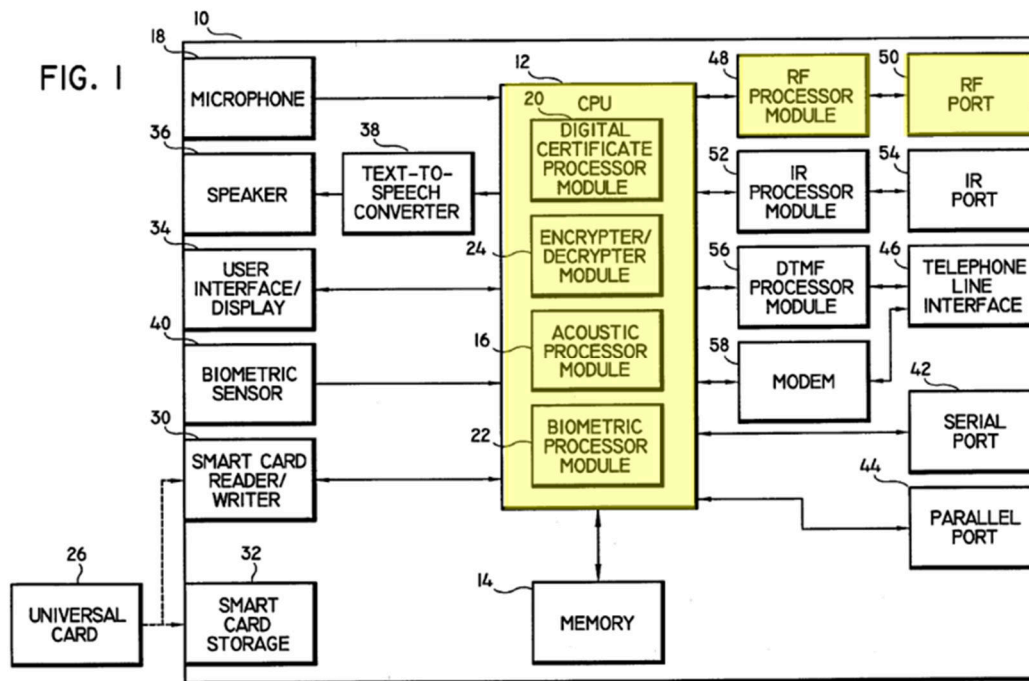
Maes’s PDA “provide[s] direct communication capability with peripheral devices (such as POS terminals).” EX1004, Abstract; *see also id.*, 6:8-19, 12:5-29, Fig. 3.

(b) [1.1]

Maes renders [1.1] obvious. EX1003, ¶¶131-134.

Maes's PDA device (*mobile device*) "is capable of transmitting or receiving information through wireless communications such as radio frequency (RF) and infrared (IR) 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 PDA 10 includes *short range radio frequency (RF) circuitry* such as RF port 50, RF processor module 48, and/or CPU 12. EX1003, ¶133.



EX1004, Fig. 1 (highlighted).

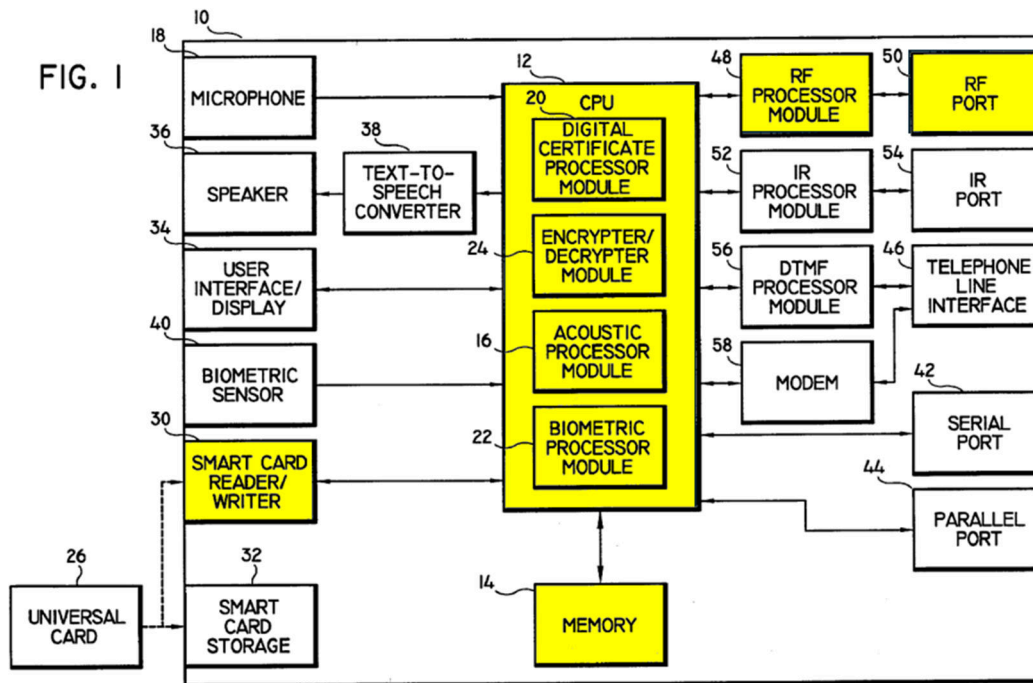
A POSITA would have understood Maes's RF circuitry to be *short-range* circuitry. EX1003, ¶134. Maes describes the RF link L2 as a direct wireless channel between the PDA held by the user and the POS transaction terminal 80. EX1004, 12:5-29. Maes expressly treats its RF port 50 and IR port 54 as interchangeable 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 used for a direct link between the PDA and a nearby transaction terminal is *short range*. EX1003, ¶134.

(c) [1.2.1]

Maes renders [1.2.1] obvious. EX1003, ¶¶135-140.

Maes discloses that the PDA device 10 (*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”).

In more detail, and 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 biometric processor module 22 for processing biometric data ... to provide user verification,” and “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, 5:8-17; *see also id.*, 5:18-24.



EX1004, Fig. 1 (highlighted).

As shown in Fig. 1 above, the *memory* (e.g., memory 14) of Maes’s *mobile device* (e.g., PDA device 10) is coupled to the *short-range RF circuitry* (e.g., RF processor module 48, RF port 50, and/or CPU 12) via CPU 12. EX1003, ¶138.

The “financial information” stored in memory 14 includes information for at least one credit card. EX1003, ¶139. 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 cards ... 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. Maes’s “selected card information” thus provides **payment information** stored in a **memory** (e.g., memory 14) of the PDA device 10 (**mobile device**) as claimed. *Supra*, §IV; EX1003, ¶139.

The “personal information” stored in memory 14 includes **biometric authentication information** for an authorized cardholder or user of the PDA device 10. EX1003, ¶140. 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 Maes’s PDA 10 memory (e.g., memory 14) stores **biometric authentication information** used by the biometric

processor module 22 to authenticate the user attempting a transaction. EX1003, ¶140. Additionally or alternatively, it would have been obvious to store **biometric authentication information** in the memory of the PDA for each of the biometric modalities contemplated in Maes, as doing so would beneficially allow the biometric processor module 22 to authenticate a user in local mode by comparing the input from biometric sensor 40 to reference biometric models for those modalities stored in the memory (just as Maes expressly discloses comparison of a spoken input into microphone 16 to the user's stored voice model). *Id.*

(d) [1.2.2]

Maes renders [1.2.2] obvious. EX1003, ¶¶141-147.

As noted above with respect to [1.2.1], Maes stores the user's biometric authentication information and the user's credit card information in the same memory 14 of PDA device 10, and verifies the user by "comparing the current biometric" with the biometric data "stored in memory 14." EX1004, 10:56-61; *supra*, [1.2.1]. Only upon verification against those models is the credit card information (**payment information**) selected for a transaction retrieved and decrypted "using an encryption key unique to the PDA device 10." EX1004, 11:9-15, 11:27-32, Fig. 5 (steps 200-208, 214, 226). Maes's **biometric authentication information** is thus associated with a **user** associated with that **payment**

information. Indeed, Maes maintains links between the verified user and particular cards as discussed below. EX1003, ¶142.

First, for example, where cards are loaded directly, “the PDA device 10 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”; a card that cannot be matched must be enrolled with the service provider. EX1004, 7:7-19. Each card in memory 14 is thus tied to the user whose biometric authentication information gates its access. EX1003, ¶143.

Second, the digital certificate, which is issued only upon verification of the enrolled user, is “encoded with the user requested limitations,” which include “the specific financial card information to be used” and “any constraints which exist for each enrolled card.” EX1004, 7:45-49, 10:1-7. In local mode, Maes’s PDA determines “whether the use of the selected card has been prohibited or limited by the user requested limitations of such card,” which a POSITA would have understood to involve checking an association between the verified user’s certificate and identified cards. EX1004, 11:19-23; EX1003, ¶144; *see also id.*, claims 10, 18.

Third, Maes discloses that the authorization number “generated upon user verification” is used “together with the unique Universal Card number 27” to verify the user, and the service provider verifies “that the authorization number corresponds

to User A's unique Universal Card number." EX1004, 12:34-39, 15:21-25; *see also id.*, 6:47-56, 13:1-5.

Maes's enrollment procedures further underscores these associations as the user's "credit card ... information," unique account number 27, and "biometric data such as voice prints (models) of the user" are stored together on central server 60 and used for "user verification." EX1004, 6:56-7:35, 8:52-56; EX1003, ¶146.

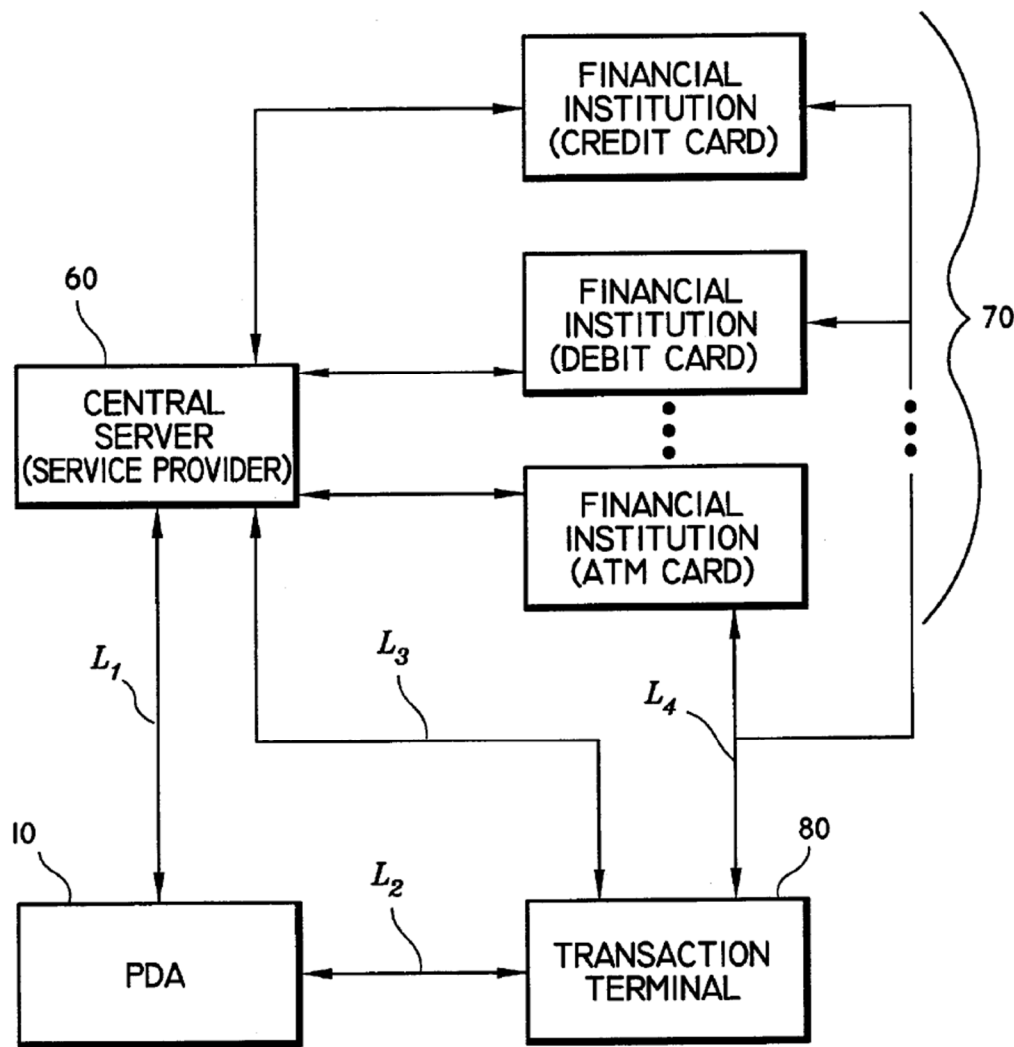


FIG. 3

EX1004, Fig. 3.

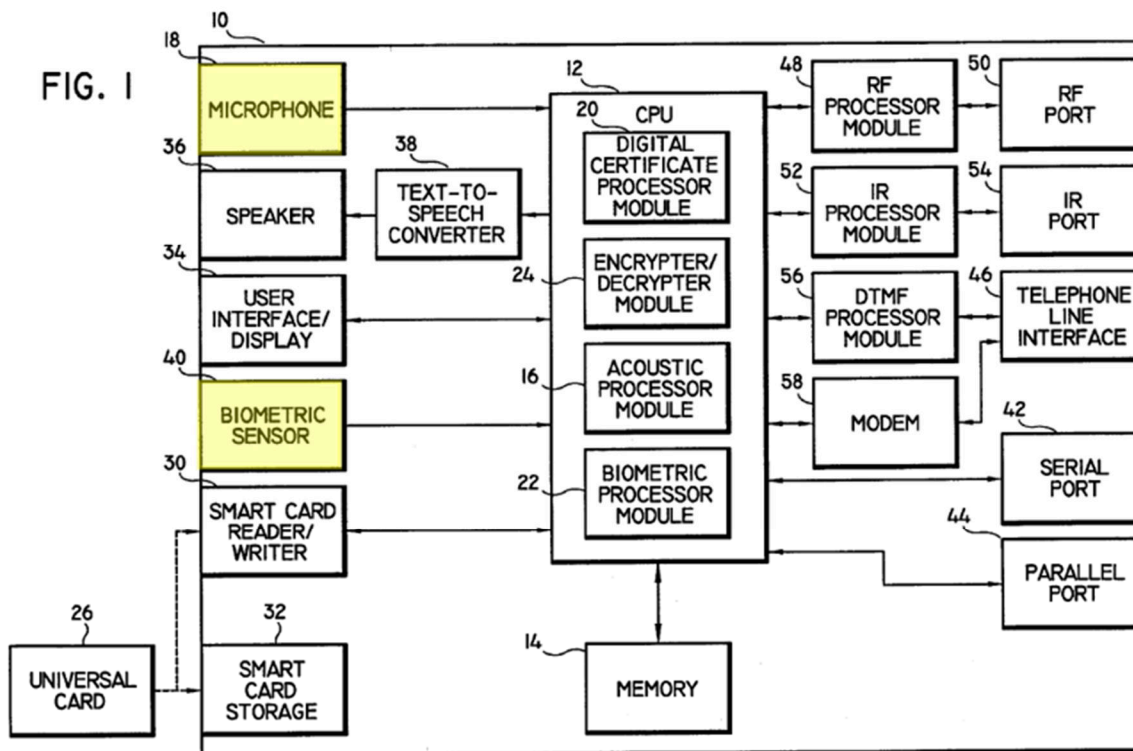
Accordingly, Maes's *biometric authentication information* is associated with a *user* associated with the *payment information*. EX1003, ¶147.

(e) [1.3]

Maes renders [1.3] obvious. EX1003, ¶¶148-151.

Maes discloses that the PDA 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.

Likewise, with respect to Fig. 1 (reproduced below), Maes describes a “microphone 18” and 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.



EX1004, Fig. 1 (highlighted).

From these and related descriptions, a POSITA would have understood that PDA 10 includes a biometric reading device configured to read biometric information. EX1003, ¶151; EX1004, Abstract, 5:54-63; Fig. 1; *see also id.*, 10:49-11:8, Fig. 5.

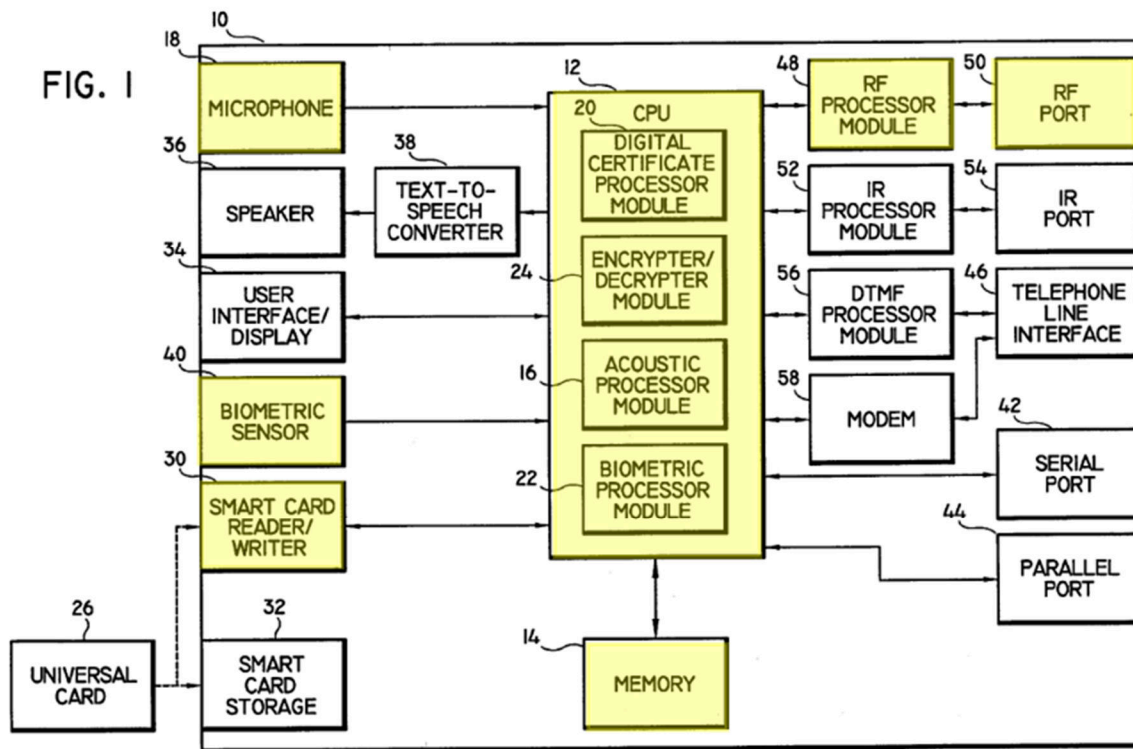
(f) [1.4.1]

Maes renders [1.4.1] obvious. EX1003, ¶¶152-155.

Maes's PDA includes a "local central processing unit (CPU) for processing ... biometric data to provide user verification," a "memory for storing financial and

personal information of the user,” and a “serial port and/or a parallel port so as to provide direct communication capability with peripheral devices (such as POS ... terminals),” for example, by “transmitting or receiving information through wireless communications such as radio frequency (RF) ... communication.” EX1004, Abstract.

Relatedly, with respect to Fig. 1 (reproduced below), Maes describes a “memory 14,” a “smartcard reader/writer 30,” a “RF processor module 48,” a “RF port 50,” a “microphone 18,” and “biometric sensor 40,” all of which are depicted as being operably coupled to “CPU 12,” which further includes an “acoustic processor module 16,” and a “biometric processor module 22.” EX1004, 4:65-6:27, Fig. 1.



EX1004, Fig. 1 (highlighted).

From these and related descriptions, a POSITA would have understood that Maes discloses *one or more processors* (e.g., CPU 12) operably coupled to the *memory* (e.g., memory 14 and/or Universal Card 26), *short range RF circuitry* (e.g., RF port 50 and/or RF processor module 48), and the *biometric reading device* (e.g., microphone 18 and/or biometric sensor 40). EX1003, ¶155.

(g) [1.4.2]

Maes renders [1.4.2] obvious. EX1003, ¶¶156-157.

For example, per Maes, “[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, Fig. 1.

(h) [1.5.1]

Maes renders [1.5.1] obvious. EX1003, ¶¶158-161.

Maes explains that “the consumer transaction [is] 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).” EX1004, 12:10-15; *generally id.*, 12:5-29, 13:34-38 (“transmitted to the POS terminal (via ... RF ...)”). At least insofar as the selected card information is transmitted over “an established communication link,” a POSITA would have understood that Maes’s PDA device 10 establishes a connection with the POS transaction terminal via the short range RF circuitry, as part of the process of performing the consumer transaction. EX1003, ¶159. Indeed, Maes’s description of the communication link L2 being “established” implies that the link L2 forms a connection between the PDA and the POS device that precedes the transmission of information for the transaction over the link. *Id.* In this regard, Maes’s description of establishing a connection is at least as detailed and relevant as the most analogous disclosures of this feature in the specification of the ’412 Patent. EX1001, 13:16-25

(merely describing data transfer that results when “a user with an RF cellular telephone approaches a POS with an RF reader/writer” with no more specific operations or protocol identified for “establishing a connection”). Moreover, establishing short-range RF connections was well known before the Critical Date and a POSITA would have found it obvious to use known techniques for establishing such a short-range RF connection when establishing Maes’s link L2 since they provide a “predictable solution” to a clear “design need” in Maes. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 405 (2007); EX1003, ¶159, citing EX1035, EX1036, EX1037.

(i) [1.5.2]

Maes renders [1.5.2] obvious. EX1003, ¶¶162-167.

Maes’s PDA device 10 (*mobile device*) establishes a short-range RF connection with a POS terminal (*POS device*) for conducting a secure transaction between the PDA device 10 and the POS terminal. *Supra*, [1.5.1]; *infra*, [1.10].

For example, Maes discloses techniques “relat[ing] to a portable information and transaction processing system and method and, more particularly, to a portable information and transaction processing system and method which utilizes digital certificate security and biometric authorization to provide personal verification prior to processing user requested financial transactions and personal information.” EX1004, 1:11-17. Maes explains that 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 L2 (step 228, Fig. 3) (*i.e.*, via the ... RF port 50)[]” *Id.*, 12:8-15; *see also id.*, Fig. 5. In some embodiments, “[t]he selected card information, as well as [an] encrypted information file, would be transmitted to the POS terminal (via the ... RF ...) and then transmitted in encrypted form directly to the processing financial institution together with the purchase details.” *Id.*, 13:34-38. From these and related disclosures, a POSITA would have understood that the RF connection between Maes’s PDA device 10 and the POS terminal was established to conduct a transaction. EX1003, ¶164.

A POSITA also would have understood that Maes’s connection facilitates a “secure” transaction. Indeed, Maes explicitly teaches that its system “utilizes digital certificate security and biometric authorization to provide personal verification prior to processing user requested financial transactions and providing personal information.” EX1004, 1:11-17. This security “protects against the unauthorized access to the user’s financial and personal information.” *Id.*, 4:7-10; *see also id.*, 13:19-23 (“afford[s] an additional level of security for user verification”), 13:24-38 (describing “encrypted” information transmitted from PDA device 10 to POS terminal).

Maes's system also provides an "authorization number" that further promotes the integrity and security of transactions. EX1003, ¶166. For example, Maes explains that "[t]he merchant can verify that local verification of the user has been properly obtained by ... transmitting the selected card information to the financial institution" in addition to an "authorization number" that "is generated upon user verification"; "[s]ince the authorization number is a function of the unexpired digital certificate that was obtained from the central server 60 in the client/server mode, the central server 60 [may then] inform the merchant that the user was properly verified" EX1004, 12:55-13:5; *see also id.*, 6:56-7:35, Fig. 3.

At least insofar as the authorization number generated for the transaction enables confirmation of user verification, this would have underscored a POSITA's understanding that the transaction is secure. EX1003, ¶167.

(j) [1.6]

Maes renders [1.6] obvious. EX1003, ¶¶168-175.

Maes explains that "[t]he local mode of operation" used for conducting a transaction "is commenced by the user selecting a pre-enrolled credit card that is stored in memory 14." EX1004, 10:29-33, Figs. 1, 5. "If the requested card information is found in memory, biometric verification must be performed" and "a biometric sensor 40 of any known type may be used in leu 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.” *Id.*, 12:49-13:5. Maes also explains that “the user is prompted (either by text on the user interface/display 34 or verbally through the text-to-speech converter 38 and speaker 36) to enter certain verification data.” EX1004, 8:13-16.

From these and related disclosures, a POSITA would have understood or at least found obvious prompting the user to provide biometric information to the biometric reading device as recited in [1.6]. EX1003, ¶169. Maes discloses that the user can be prompted to enter verification data, and biometric information is a form of verification data in Maes. *See e.g.*, EX1004, 8:13-16 (“the user is prompted”), 12:50 (“biometric verification must be performed”).

Further, prompting the user to provide biometric information to a biometric reading device was a well-known technique before the Critical Date. EX1003, ¶¶170-175. Such prompting would have been obvious to implement in Maes to ensure the user provides the biometric information necessary to complete the verification required to initiate a transaction and to inform the user of the appropriate time for providing the biometric information (*e.g.*, once the PDA device 10 is ready after the requested card information is found in memory). EX1003, ¶169 (citing corroborating references EX1015, 19:28-29, 19:30-31, 42:19-21, 43:45-48;

EX1018, claim 1, claim 8, claim 17, 11:30-32, 12:28-29; EX1019, 12:42-44, 16:51-53; EX1020, 1:11-12, 1:19-24).

(k) [1.7]

Maes renders [1.7] obvious. EX1003, ¶¶176-180.

Maes explains that biometric voice data obtained from microphone 18 is “sent to the acoustic processor module 16” for comparison “with the user’s voice models stored in memory 14.” EX1004, 10:57-61; *generally id.*, 10:48-11:8, Fig. 5. Similarly, “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” EX1004, 10:66-11:8. “After 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; *see also id.*, 5:60-63.

From these and related disclosures, a POSITA would have understood that Maes’s PDA device 10 authenticates that the ***biometric information*** read by the microphone 18 and/or the biometric sensor 40 is associated with an authorized user. EX1004, 6:56-7:35, 10:49-51, 14:42-46, Figs. 1, 3, 5; EX1003, ¶178. The authentication is based on the ***biometric authentication information*** stored in

memory 14 (which is compared against the newly read biometric information), and the authorized user is associated with the credit card information (*payment information*) stored in memory for the reasons discussed above in [1.2.2]. *Supra*, [1.2.2]; EX1003, ¶178.

As explained above with respect to [1.2.1] and [1.2.2], Maes expressly describes “a memory for storing financial and personal information of the user,” and for performing “biometric verification” of the user as part of secure transaction processes involving the user’s associated “card information.” *See* EX1004, Abstract, 6:56-7:35, Fig. 3. In that regard, the user’s “credit cards ... may be loaded into the PDA device 10 by directly reading information contained on such cards through the smartcard reader/writer 30,” in which case “the PDA device 10 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.” *Id.*, 7:3-19; EX1003, ¶179.

Maes further explains 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,” and that “[i]f the digital certificate is valid (*i.e.*, unexpired) the requested card information is then retrieved from memory 14” EX1004, 10:29-11:41; *see also id.*, 6:56-7:35, 10:49-51, 14:42-46, Figs. 1, 3, 5; EX1003, ¶180.

(i) [1.8]

Maes renders [1.8] obvious. EX1003, ¶¶181-184.

Maes's PDA device 10 generates an authorization number when the user is biometrically authenticated. EX1004, 5:60-63; 12:43-49, 12:63-65; EX1003, ¶182. According to Maes, "[t]he merchant can verify that local verification of the user has been properly obtained" by transmitting the "authorization number to [a] central server 60." EX1004, 12:55-13:1. "Since the authorization number is a function of the unexpired digital certificate that was obtained from the central server 60 in the client/server mode, the central server 60 [may then] inform the merchant that the user was properly verified" EX1004, 12:55-13:5; *see also id.*, 6:56-7:35, Fig. 3.

Maes's "authorization number" represents a "**key**" as claimed.² EX1003, ¶183. Indeed, Maes discloses that the "authorization number" (**key**) is derived from

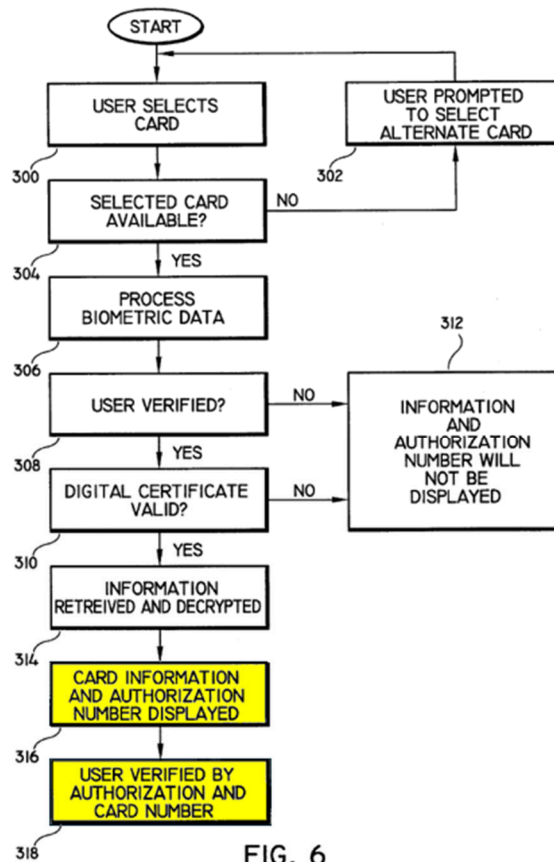
² The '412 Patent specification never expressly identifies any "key" that meets all the claimed functions, including being (i) generated in response to the authentication (Element [1.8]), (ii) provided to the merchant for use in a secure transaction (Element [1.10]), and (iii) validated by a central database along with payment information to complete a transaction (Element [4.16]). *See* EX1001, 2:32-39, 10:65-11:4, 12:5-18, 13:3-7, 14:55-61, 22:21-26 (describing cryptographic keys in contexts different from

a digital certificate and generated by the PDA once the *biometric information* (e.g. voice, fingerprint, or other biometric input) read by the *biometric reading device* (e.g., microphone 18 or biometric sensor 40) is determined to be associated with the user associated with the card information (*payment information*), which is achieved by comparing the read *biometric information* to the *biometric authentication information* (e.g., reference voice models or other reference biometric data) stored in *memory* (e.g., memory 14) (*in response to the authentication*). EX1004, 12:63-13:5 (“the merchant will be requested to provide the authorization number (which is generated upon user verification), in addition to the expiration date of the credit card ... [s]ince the authorization number is a function of the unexpired digital certificate that was obtained ... in the client/server mode, the central server 60 inform the merchant that the user was properly verified ...”), 6:42-55 (“an authorization number, which is unique to the current digital certificate, will be displayed on the PDA device 10 upon user verification”), 12:30-39 (“a merchant can confirm that the user passed local verification by using ... an authorization number which is based on the current valid digital certificate and generated upon user verification”), 14:47-

what is claimed); EX1003, ¶183. Maes’s authorization number as applied in this Petition nonetheless fulfills each of these claim requirements and functions as a key for authorizing a transaction. EX1004, 6:47-55, 12:30-13:5; EX1003, ¶183.

67 (“User B then obtains the authorization number produced by the PDA device of User A upon local verification”); EX1003, ¶183.

For instance, Maes discloses that “if the user is biometrically verified (step 308) and the PDA device 10 contains an unexpired digital certificate (step 310), the selected card information is retrieved from memory 14 and decrypted (step 314).” EX1004, 12:40-47; *see also id.*, Figs. 5-6. “The desired credit card information, as well as an authorization number, is then displayed on the user interface/display 34 (step 316)” and is “communicated to the merchant in order to process the transaction.” EX1004, 12:47-54. “If the selected card information corresponds to a credit card that was previously enrolled (*i.e.*, registered) with the service provider” the merchant will “upon transmitting the selected card information ... be requested to provide the authorization number (which is generated upon user verification), in addition to the expiration date of the credit card.” EX1004, 12:61-66. And, “[s]ince the authorization number is a function of the unexpired digital certificate that was obtained from the central server 60 in the client/server mode, the central server 60 inform the merchant that the user was properly verified (step 318).” EX1004, 13:1-5.



EX1004, Fig. 6.

(m) [1.9]

Maes renders [1.9] obvious. EX1003, ¶¶185-187.

To start, Maes discloses “securing the payment information stored in the memory” through its authorization-number mechanism. EX1003, ¶186. When a user is biometrically verified in the local operating mode, the PDA’s CPU retrieves the credit card information (*payment information*) selected for the transaction from memory and generates an authorization number (*key*) tied to the current, unexpired digital certificate. EX1004, 12:30-54; *supra*, [1.8]. This authorization number is

generated in response to the authentication (*supra*, [1.8]), and it functions as the credential that a merchant or transaction terminal must obtain and provide to the central server to confirm that the legitimate cardholder was authenticated before the card information may be used to complete a purchase. EX1004, 12:55-13:5. Because the transaction cannot be completed without producing this authorization number, the authorization number *secures* the card information. EX1003, ¶186. Indeed, it ensures the stored card information remains unusable in a transaction unless the party presenting it can also produce proof, in the form of the authorization number, that the biometrically-verified cardholder authorized its use. *Id.*

In addition, or in the alternative, Maes discloses securing the card information stored in memory by encrypting the card information for storage in memory 14 using encrypter/decrypter module 24. *See* EX1004, 5:14-17, 11:27-32, Fig. 1; *see also id.*, 12:43-49, 13:19-38, Fig. 5 (214), Fig. 6 (314). It also would have been obvious to secure the stored card information by applying a separate encryption to the card information after it is retrieved from memory to protect the information for transmission over the RF link. *See* EX1004, 13:19-38; EX1003, ¶187 (citing corroboration EX1005, 4:43-47, 6:3-4, EX1038, EX1039); *infra*, [1.10].

(n) [1.10]

Maes renders [1.10] obvious. EX1003, ¶¶188-200.

Maes discloses 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 RF port 50).” EX1004, 12:10-15; *generally id.*, 12:5-29, Figs. 1, 5, 6.

Maes also discloses communicating the “authorization number” (*key*) to the merchant “in order to process the transaction.” EX1004, 12:43-54 (“When operating the PDA device 10 in the local mode, if the user is biometrically verified (step 308) and the PDA device 10 contains an unexpired digital certificate (step 310), the selected card information is retrieved from memory 14 and decrypted (step 314). The desired credit card information, as well as an authorization number, is then displayed on the user interface/display 34 (step 316). This information can then be verbally communicated to the merchant in order to process the transaction.”), 12:66-13:5 (“The merchant will then transmit ... the displayed authorization number to the central server 60. Since the authorization number is a function of the unexpired digital certificate that was obtained from the central server 60 in the client/server mode, the central server 60 inform the merchant that the user was properly verified (step 318).”), Fig. 6.

Maes highlights examples where the authorization number is displayed and “verbally communicated to the merchant” to facilitate user verification through the

authorization number even when the merchant lacks an electronic transaction terminal. EX1004, 12:30-39. It would have been obvious that the authorization number could alternately be transmitted to the merchant from the PDA over a short-range RF link when the merchant has a suitable POS terminal with an RF reading device. EX1003, ¶¶191-191B. Indeed, Maes explicitly discloses that “[i]t is to be further appreciated 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” and that “the consumer transaction may be performed by transmitting ... directly from the PDA device to the ... POS transaction terminal through an established communication link L2 (step 228, Fig. 3) (*i.e.*, via ... the RF port 50), rather than retrieving and writing card information to the Universal Card 26.” EX1004, 12:5-29. Maes also describes the option of transmitting via short-range RF additional information about the user in a transaction request from the PDA to the POS terminal. EX1004, 13:33-38³.

³ At col. 13:34-38, Maes states that the selected card information and encrypted information file “would be transmitted to the POS terminal (via the Universal Card, RF or IR).” In Maes, the PDA is the device that has RF transmission capabilities. *See e.g.*, EX1004, 6:6-14, 12:5-29, Fig. 1. A POSITA would have understood Maes’s

Transmitting an authorization number along with the selected card information over RF mirrors these embodiments while maintaining Maes's existing framework for backend user verification using the authorization number. Adding an additional data item to an existing package of data transmitted over short-range RF in Maes's system would have been well within the technical grasp of a POSITA. EX1004, 12:5-13:38, Figs. 5-6; EX1003, ¶191, citing EX1038.

A POSITA would have had ample reason to configure Maes's PDA to transmit the authorization number to the POS terminal over short-range RF. EX1003, ¶194. Transmitting the authorization number electronically, rather than requiring the user to convey it verbally, would beneficially allow the authorization number to be used not only in transactions where the merchant lacks an electronic card reader, but also in transactions involving POS terminals with a suitable RF reader, since the authorization number can similarly aid in verifying the user regardless of whether it is communicated verbally or over RF. EX1003, ¶194.

RF-based transmission of the authorization number would also improve the security of the transaction, since verbal communication of the authorization number risks exposing it to unauthorized bystanders who may overhear it, whereas electronic

use of "RF" here to refer to an RF transmission from the PDA, consistent with Maes's recitation of "RF" as an alternative to the Universal Card and IR.

transmission obviates the need to speak the number aloud and allows it, along with other transmitted information, to be encrypted for additional protection. EX1003, ¶195 (citing corroborating exhibits EX1005, 4:43-47, 6:3-4; EX1004, 5:1-4, 5:14-17, 6:9-14, 13:33-38). Transaction efficiency for the user and the merchant would also be improved since transmitting it over the same communication channel that carries the selected card information would allow the user to convey all necessary transaction information using a single communication modality, and would eliminate the time and effort involved in manually reading the number to the merchant. EX1003, ¶195. It would also improve accuracy as electronic transmission would avoid the risk of human error in communicating or transcribing the authorization number. *Id.* Finally, the modification involves nothing more than the predictable application of a known technique, transmitting identifying information for a transaction over RF, which Maes already expressly teaches, to further include the authorization number, applied to a known device ready for improvement, yielding predictable results. *See KSR*, 550 U.S. at 416; EX1003, ¶195.

A POSITA also would have understood that the selected card information (*payment information*) transmitted from the PDA to the POS terminal is “*secured*” for several reasons. EX1003, ¶196. As discussed above, the authorization number (*key*) secures the card information by ensuring that it remains unusable in a transaction unless the party presenting it can also produce the authorization number

as proof that the biometrically verified cardholder authorized its use. EX1004, 12:30-13:5; *supra*, [1.9].

Moreover, the card information is stored in memory 14 in encrypted form, having been encrypted using an encryption key unique to the PDA. EX1004, 5:14-17, 11:23-40. The card information is decrypted for use in the transaction only in response to successful biometric verification of the user and validation of an unexpired digital certificate, both of which are performed locally at the PDA before the card information can be retrieved from memory. EX1004, 5:58-62, 11:14-29, 12:44-48. The CPU 12 is does not retrieve or transmit the card information over the RF link to the POS terminal unless both the biometric verification and digital certificate checks succeed, ensuring that unverified transmissions do not occur. EX1004, 12:18-23.

Finally, it would have been obvious to secure the card information used in a transaction by “transmit[ting] [it] in encrypted form.” EX1004, 13:34-38. A POSITA also would have been motivated to encrypt the card information transmitted over the RF link from the PDA to the POS device to improve security and prevent the information in the transmission from being intercepted in the clear by unauthorized actors. EX1004, 13:34-38; EX1003, ¶¶197-199 (citing corroborating exhibits EX1005, EX1038, EX1039).

For each of these reasons, Maes renders obvious transmitting from the PDA device (*mobile device*) to the POS terminal (*POS device*), *via the short range RF circuitry* (via the RF port), the *key* (authorization number) and the *secured payment information* (selected card information) for use in the secure transaction. EX1004, 12:10-15; EX1003, ¶200.

(o) [2]

Maes renders [2] obvious. EX1003, ¶¶201-204.

As explained at [1.2.1], Maes's selected card information is *payment information* as claimed. *Supra*, [1.2.1]. The selected card information can include information regarding a pre-enrolled credit card that the user selects for the transaction. EX1004, Abstract (“selecting one of the pre-enrolled credit cards that are stored in the PDA”); 2:23-30 (“a user can store his or her credit card ... (*i.e.*, financial) information”), 4:1-11, 6:61-67, 11:51-57; EX1003, ¶202.

Maes describes enrolling such a card by “providing the service provider with the user's credit card ... information.” EX1004, 6:64-65. And Maes recognizes that a payment card carries an account number, referring to “the account number provided on a credit card ...” EX1004, 6:40-41.

A POSITA would have understood the account number carried on the user's selected card — the number identifying the cardholder's account — to be associated with that card's “primary account number” (PAN), the standard term in the payment-

card art for the account number carried on a payment card. EX1003, ¶204 (corroborated by EX1021, 1:17-21 (“[R]emote banking generally involves the use of magnetic stripe cards, together with cheques or cash. The cards are encoded with information identifying holders of the cards. The information stored on the card is typically a primary account number (PAN).”); EX1022, 1:66-2:2 (“a Primary Account Number (PAN), [] is the embossed number on the card. The embossed number on the card is also stored on the magnetic stripe of the card”))).

(p) [3]

Maes renders [3] obvious. EX1003, ¶¶205-210.

As an initial matter, the “stored separately” limitation in claim 3 cannot mean that the biometric authentication information and the secured payment information are stored in separate memories because claim 3 depends from claim 1, and [1.2.1] and [1.9] require that both pieces of information be stored in the same “memory.” *Supra*, [1.2.1], [1.9]. It is sufficient, therefore, that the biometric authentication information and the secured payment information be stored separately in the same memory, such as in logically distinct regions of, or under distinct access controls, within that memory. EX1003, ¶206. This is consistent with the specification of the ‘412 Patent, which discloses a security-management unit and cryptographic block that gate access to memory using cryptographic keys (*see* EX1001, 5:32-37, 13:53-60), and describes that information contained on the RF device is “protected by

sundry cryptographic methods” (*id.* at 8:38-40), indicating that different categories of sensitive data can be logically segregated within a single memory such as through distinct access-control or cryptographic regimes. The specification nowhere discloses physically distinct memory chips for the biometric and payment information. EX1003, ¶206.

In Maes, biometric authentication information includes the user’s voice or other biometric data, which Maes stores in memory 14. EX1004, 10:60-62 (“comparing the current biometric voice data with the user’s voice models stored in memory 14”), 5:53-62 (describing alternative forms of biometric data). The secured payment information, *e.g.*, the user’s encrypted card information, is likewise stored in memory 14. EX1004, Abstract (“a memory for storing financial and personal information of the user”), 2:60-66, 3:20-24, 5:1-4, 5:14-17, 7:1-7, 11:24-29, 12:44-47; *supra*, [1.2.1], [1.9]. Maes secures that information by “encrypting the personal and financial information before being stored in memory 14.” EX1004, 5:14-17.

A POSITA would have understood that Maes’s voice models or alternative biometric data (***biometric authentication information***) and its encrypted card information (***secured payment information***) are stored in different locations of memory and are therefore stored separately from one another, as claim 3 requires. EX1003, ¶208. Indeed, the encrypted financial/card information and the biometric

data are stored separately and at distinct locations in memory to enable them to be accessed separately for their separate purposes described in Maes. *Id.*

Moreover, Maes discloses cryptographic separation of the payment information from the biometric authentication information within memory 14. Maes teaches 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, 5:14-17. The card information is thus stored in memory 14 in encrypted form, protected by “an encryption key unique to the PDA device 10.” EX1004, 11:24-29. The biometric authentication data, such as the user’s voice models and any fingerprint, palm print, handwriting, or retinal templates, is not described as being encrypted under that same key or protected under the same regime. Maes discloses that the biometric authentication data is instead accessed through a distinct processing path via the acoustic processor module 16 or the biometric processor module 22 for the purpose of user verification. EX1004, 5:1-17, 5:53-62, 11:9-14. The payment information and the biometric authentication information are therefore stored under distinct access-control regimes within memory 14. EX1003, ¶209.

Additionally, Maes discloses that access to the payment information is gated by an additional layer of protection in the form of the digital certificate that does not gate access to the biometric authentication information. Under Maes’s architecture,

biometric verification alone is not sufficient to access the stored card information. The PDA device 10 also requires a valid, unexpired digital certificate stored in memory 14, which is separately decrypted and validated by the digital certificate processor module 20 before the encrypter/decrypter module 24 will retrieve and decrypt the card information. EX1004, 7:41-52, 11:16-29. Biometric verification, by contrast, is performed directly against the stored biometrics without needing a valid digital certificate. EX1004, 11:9-14; Fig. 5 (steps 206-212). This access-control architecture further demonstrates how the payment and biometric information are “*stored separately*” within Maes’s memory 14. EX1003, ¶210.

B. Ground 1B: Maes-Niwa Renders Obvious Claims 1-3

1. Niwa (EX1005)

Like Maes, Niwa describes “[a] method of authorizing a commercial transaction between a customer and a provider of goods or services over a network, wherein the provider of goods or services requests that the customer provide authentication by activating a fingerprint identification device, and the provider of goods or services receives at least an authentication code of the customer over the network from the fingerprint identification device.” EX1005, Abstract; EX1003, ¶¶86-90.

Niwa explains that “[t]he card issues an authorization code only when the fingerprint of the customer 52 matches the stored fingerprint.” EX1005, 4:32-34.

In Niwa, “[d]ata transfer is ... conducted between the fingerprint identification device 50 . . . and the provider of goods and/or services 60, 62 or 64 (action 112).” EX1005, 5:63-67. “The data transfer preferably includes at least one of the authentication code, payor bank identification number, customer account number, and delivery address.” EX1005, 5:67-6:3. Niwa states that “[m]ost preferably, the data of this transfer are in encrypted form.” EX1005, 6:3-4; *see also id.*, 6:13-25, 6:54-58.

2. The Maes-Niwa Combination

Maes’s PDA transmits selected card information for a transaction over an RF link to a point-of-sale (POS) terminal. EX1004, 12:5-29; *supra*, §V.A.1. Maes teaches that the user can provide an authorization number for the transaction to the merchant, which the merchant in turn provides to a central server to verify the user in a process for authorizing the transaction. EX1004, 12:39-54, 12:65-13:5. In particular, Maes focuses on an example scenario where the user “verbally” conveys the authorization number to the merchant, such as where the merchant lacks an electronic POS terminal. EX1004, 12:39-54, Fig. 6.

To the extent Maes does not expressly disclose that the authorization number is transmitted from the PDA to the POS terminal over an RF link, Niwa complements Maes in teaching that not only payment information but also an authentication code (similar to Maes’s authorization number) can be electronically transmitted to a

merchant. *Supra*, §V.B.2. For example, Niwa describes a “[d]ata transfer ... conducted between [a] fingerprint identification device 50 . . . and [a] provider of goods and/or services 60, 62 or 64” where “[t]he data transfer preferably includes at least one of the authentication code, payor bank identification number, customer account number, and delivery address.” EX1005, 5:63-6:4,⁴ Fig. 3 (step 112). For a POS transaction, “the data (*e.g.*, at least one of the authentication code, payor bank identification number, customer account number, delivery address, etc.) would be provided to, for example, the merchant 70 ... at the point of sale.” EX1005, 6:54-58.

A POSITA would have found it obvious to implement Maes’s system in accordance with Niwa’s suggestion for transmitting payment information and an authorization number from a user device to a merchant for use in a transaction over an electronic channel. EX1003, ¶¶91-100. In the resulting Maes-Niwa Combination (MNC), Maes’s PDA transmits not only the selected card information but also the authorization number/code to the merchant’s POS terminal over an electronic channel in the form of Maes’s RF link. EX1003, ¶¶91-100. The merchant then provides both the selected card information and the authorization number to a

⁴ All emphasis in this Petition is added unless otherwise noted.

financial institution to authorize the transaction in accordance with Maes's teachings. EX1004, 12:57-66, 13:34-38.

Based on Niwa, a POSITA would have been motivated to configure the PDA in MNC to transmit the authorization number/code and selected card information to a POS terminal via short-range RF, for at least the same reasons a POSITA would have found it obvious to transmit the authorization number based on Maes alone, as described above in Ground 1A at [1.10]. *Supra*, Ground 1A, [1.10]; EX1003, ¶¶91-100. For example, a POSITA would have been motivated to combine Maes and Niwa because doing so would (1) enable beneficial use of the authorization number in transactions involving electronic POS terminals, not just those without electronic card readers, (2) increase transaction security by eliminating verbal communication of the number, preventing bystanders or listening devices from intercepting it, (3) enable encryption of information transmitted from the PDA for the transaction (including the authorization number), (4) improve point-of-sale efficiency and accuracy by letting the user convey all necessary transaction information through a single communication modality (Maes's RF link) rather than manually reading the number to the merchant, yielding a more frictionless experience expected to increase usage of Maes's technology, and (5) because the combination follows the familiar pattern from *KSR* in which a known technique (*e.g.*, Niwa's electronic transfer of an authentication code in a transaction) is applied to a known device ready for

improvement. *KSR*, 550 U.S. at 416; *see also* EX1004, 5:1-4, 5:14-17, 6:9-14, 13:33-38; EX1005, 4:43-47, 6:3-4. A POSITA also would have reasonably expected success implementing the combination. EX1003, ¶¶91-100; *see also supra*, Ground 1A, [1.10].

3. Claim Analysis

(a) [1.pre]

The Maes-Niwa Combination (“MNC”) described above (*supra*, §V.B.2) renders [1.pre] obvious in view of Maes’s disclosures for at least the reasons addressed above in Ground 1A. *Supra*, Ground 1A at [1.pre]; EX1003, ¶211.

(b) [1.1]

Supra, Ground 1A at [1.1]; EX1003, ¶212.

(c) [1.2.1]

Supra, Ground 1A at [1.2.1]; EX1003, ¶213.

(d) [1.2.2]

Supra, Ground 1A at [1.2.2]; EX1003, ¶214.

(e) [1.3]

Supra, Ground 1A at [1.3]; EX1003, ¶215.

(f) [1.4.1]

Supra, Ground 1A at [1.4.1]; EX1003, ¶216.

(g) [1.4.2]

Supra, Ground 1A at [1.4.2]; EX1003, ¶217.

(h) [1.5.1]

Supra, Ground 1A at [1.5.1]; EX1003, ¶218.

(i) [1.5.2]

Supra, Ground 1A at [1.5.2]; EX1003, ¶219.

(j) [1.6]

Supra, Ground 1A at [1.6]; EX1003, ¶220. Additionally, Niwa discloses “prompt[ing] [a] customer 52 to authenticate himself by activating the fingerprint identification device 50.” EX1005, 5:47-50; *see also id.*, 5:43-6:4, 6:48-58, 7:26-37, 7:56-58, 8:26-34, 8:50-54, Figs. 3, 5-6. It would have been obvious to integrate Niwa’s teaching in this regard in Maes such that MNC’s PDA would prompt the user to provide biometric information to the biometric reading device of the PDA at a POS transaction. EX1003, ¶220. A POSITA would have been motivated to do so to assist the user in knowing when to provide a biometric input to the PDA in local mode at the point of sale, which would improve the process flow of the transaction. *Id.* A POSITA would have reasonably expected success as Maes’s PDA already includes a display and other mechanisms to facilitate prompting. *Id.*; *supra*, Ground 1A at [1.6].

(k) [1.7]

Supra, Ground 1A at [1.7]; EX1003, ¶221.

(l) [1.8]

Supra, Ground 1A at [1.8]; EX1003, ¶222.

(m) [1.9]

Supra, Ground 1A at [1.9]; EX1003, ¶223. In addition, per Niwa, MNC secures the stored credit card information (***payment information***) by encrypting it for transmission over Maes's RF link. EX1005, 4:43-47, 6:3-4 ("Most preferably, the data of this transfer are in encrypted form."); *see also* EX1004, 5:1-4, 5:14-17, 6:9-14, 13:33-38; *infra*, [1.10]; *supra*, §V.B.2; Ground 1A at [1.9]-[1.10]; EX1003, ¶223.

(n) [1.10]

MNC renders [1.10] obvious. EX1003, ¶¶224-230.

To start, Maes discloses 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 RF port 50).” EX1004, 12:10-15; *generally id.*, 12:5-29, Figs. 1, 5, 6.

Maes also discloses communicating the "authorization number" to the merchant "in order to process the transaction." EX1004, 12:43-54 ("[I]f the user is

biometrically verified (step 308) and the PDA device 10 contains an unexpired digital certificate (step 310), the selected card information is retrieved from memory 14 and decrypted (step 314). The desired credit card information, as well as an authorization number, is then displayed on the user interface/display 34 (step 316). This information can then be verbally communicated to the merchant in order to process the transaction.”), 12:66-13:5 (“The merchant will then transmit the Universal Card number 27 and the displayed authorization number to the central server 60.”), Fig. 6.

Like Maes, Niwa discloses “[a] fingerprint identification device 50 ... which contains information about the owner of the device, the payor bank, the functional account number, etc. The fingerprint identification device 50 includes a microprocessor, memory, and fingerprint sensor 51 which are interconnected and programmed in order to compare a fingerprint of the customer 52 with a stored fingerprint of that customer 52. The card issues an authorization code only when the fingerprint of the customer 52 matches the stored fingerprint.” EX1005, 4:24-34, Fig. 2; *see also id.*, 5:51-6:47, Fig. 1; *supra*, §V.A.2.

Niwa further teaches that “[d]ata transfer is then conducted between the fingerprint identification device 50 ... and the provider of goods and/or services 60, 62 or 64.” EX1005, 5:63-67. “The data transfer preferably includes at least one of the authentication code, payor bank identification number, customer account

number, and delivery address. Most preferably, the data of this transfer are in encrypted form.” *Id.*, 5:67-6:4. This data transfer can also be made “at the point of sale, for example, at brick and mortar stores, 70, 72[.]” *Id.*, 6:48-58. For POS transactions, “the data” including “the authentication code” “would be provided to, for example, the merchant 70 and/or service provider 72 at the point of sale.” *Id.*

Niwa’s authentication code is highly similar to Maes’s authorization number. EX1003, ¶229. Indeed, both are generated only if the user successfully passes biometric authentication, and both are used by a service provider or financial institution to assess the legitimacy of a transaction request in a process for determining whether to authorize the requested transaction. EX1005, 6:23-26; EX1004, 12:30-13:5. Niwa further teaches that the authentication code can be electronically transferred and provided to the merchant together with other payment information for a transaction. EX1005, 6:48-58.

For the reasons addressed in detail above (*supra*, §V.B.2), a POSITA would have found it obvious to apply Niwa’s suggestion for electronically transferring an authorization number/authentication code to Maes’s system such that Maes’s PDA device 10 would transmit the authorization number/authentication code (**key**) along with the selected card information (**payment information**) to the POS device for use in a transaction via Maes’s short-range RF circuitry. EX1003, ¶230 (citing corroborating exhibits EX1008, EX1035-EX1039). The card information is secured

for each of the reasons discussed above in Ground 1A at [1.9]-[1.10] and Ground 1B at [1.9]. *See* Ground 1A at [1.9]-[1.10]; Ground 1B at [1.9]; EX1005, 6:3-4; EX1004, 13:28-38; EX1003, ¶230.

(o) [2]

Supra, Ground 1A at [2]; EX1003, ¶231.

(p) [3]

Supra, Ground 1A at [3]; EX1003, ¶232.

C. Ground 2: Maes-Bjorn Renders Obvious Claims 1-3

1. Bjorn (EX1006)

Bjorn describes “cryptographic key generation using biometric data.” EX1006, 1:1-2. Bjorn explains that its techniques “relate[] to cryptography, and more specifically, to the generation of a unique cryptographic key using biometric data.” EX1006, 1:5-7; EX1003, ¶¶101-104.

In Bjorn, a message is created from a received fingerprint and “[a] message digest function is applied to the message to create a cryptographic key.” EX1006, 1:42-46, 1:50-51. Bjorn states that “[f]or one embodiment, a one-way hash function or message digest function is used to create the hash.” EX1006, 3:45-52.

With reference to Fig. 3 (reproduced below), Bjorn explains that “[a]t block 320, a template is created for the user.” EX1006, 4:21-23. “For one embodiment, the fingerprint template is a digital image of the fingerprint.” EX1006, 8:32-33. “At

block 325, the template is hashed.” EX1006, 4:25. Bjorn adds that “[f]or one embodiment, this hash is the cryptographic key.” EX1006, 4:25-26. Bjorn further states that “[t]his cryptographic key is identified with the specific fingerprint, and thus with a specific user.” EX1006, 4:28-30. “At block 335, the template is stored,” although “[t]he cryptographic key itself is not stored anywhere on the system.” EX1006, 4:47-48. Bjorn notes that “the template is stored in a database, or other more centralized location.” EX1006, 4:47, 4:51-53.

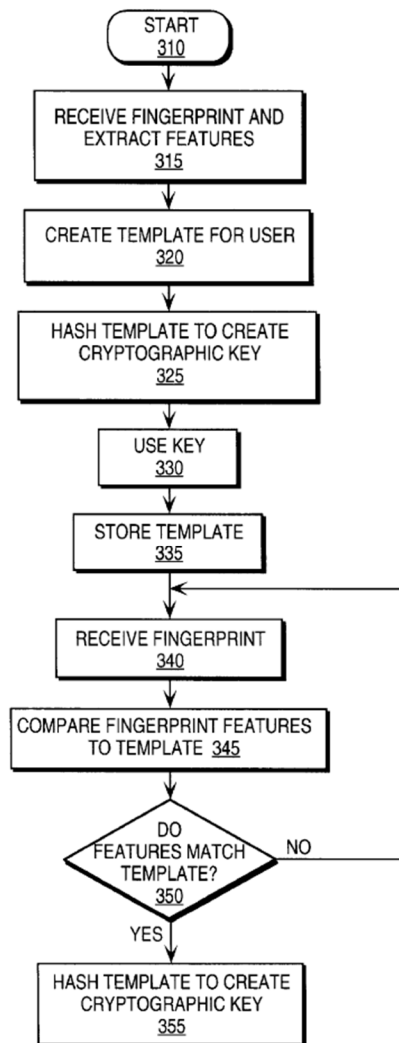


FIG. 3

According to Bjorn, “if [a] new fingerprint matches the template” then the system “appl[ies] the message digest function to the stored template to generate the cryptographic key.” EX1006, claim 3. Thus, “[a]t block 355, the template is again hashed to create a cryptographic key.” EX1006, 5:10-11. Bjorn explains that “[s]ince the template was used to generate the first cryptographic key, the same key is generated.” EX1006, 5:11-12. Bjorn’s cryptographic key can then be used in a cryptographic function to encrypt or decrypt desired data item(s). EX1006, 4:38-45; *see also id.*, 5:15-6:23 & Fig. 4 (describing alternate embodiment in which the cryptographic key is generated from aspects of the fingerprint other than those from which the template is formed), Figs. 5-8 (describing uses of the key with a digital certificate).

2. The Maes-Bjorn Combination

The Maes-Bjorn Combination (“MBC”) integrates, in Maes, Bjorn’s technique for generating a cryptographic key from biometric data such as a user’s fingerprint. *Supra*, §V.C.1; EX1003, ¶¶105-118. In MBC, Maes’s encrypted information file (*see* EX1004, 13:19-39), which Maes’s PDA device 10 transmits to the merchant’s POS terminal along with payment information for a POS transaction, is modified to include a cryptographic key generated in accordance with Bjorn’s techniques (*e.g.*, as described with respect to Figs. 3 or 4 of Bjorn) in response to biometric authentication of the user (*e.g.*, in response to determining that the user’s

fingerprint obtained at the POS matches a stored fingerprint, per Bjorn steps 350 or 460) . EX1004, 8:32-34, 13:19-39; EX1003, ¶¶105-118. In the combined Maes-Bjorn device, Bjorn's block-355/470 key regeneration is triggered by the local biometric verification Maes already performs on the PDA. EX1006, 5:3-12, Figs. 3-4; EX1004, 5:54-57, 11:9-13; EX1003, ¶¶105-118.

Multiple reasons would have motivated a POSITA to implement the combination, with a reasonable expectation of success, as the combination is a natural extension of what Maes and Bjorn each already teach. EX1003, ¶¶105-118. Maes expressly describes the encrypted information file as containing “unique identifying information pertaining to the consumer including, but not limited to, ... the consumer's name and account number.” EX1004, 13:26-32. Maes thus contemplates that additional unique identifying information, beyond name and account number, may be included to enable “the financial institution (e.g., credit card company) [to] verify the identity of the consumer during a purchase transaction.” EX1004, 13:20-24; EX1003, ¶¶105-118.

Bjorn's cryptographic key is precisely such information. EX1003, ¶¶105-118. Bjorn teaches “generat[ing] a unique cryptographic key using biometric data” from a user's fingerprint and applying a message digest function to produce the key. EX1006, 1:5-8, 4:26-33, Abstract; *supra*, §V.C.1. Bjorn further teaches that “[t]his cryptographic key is identified with the specific fingerprint, and thus with a specific

user.” EX1006, 4:29-31. A POSITA would thus have recognized that Bjorn’s key is exactly the type of “unique identifying information” that Maes contemplates could be included in the encrypted information file that would allow the financial information to verify the identity of the consumer in a secure transaction. EX1004, 13:26-30; EX1003, ¶¶105-118. Bjorn’s key would supplement the user’s name and account number in the file or would provide an obvious substitution for the name and/or account number, since each serves to identify the user. EX1003, ¶¶105-118.

A POSITA would have sought to include Bjorn’s key in Maes’s information file to strengthen the financial institution’s ability to verify the user. EX1004, 13:22-24; EX1003, ¶¶105-118. The “name and account number” example file contents given in Maes may be uniquely associated with a user, but they are less secure because they are not typically closely held secrets. An unauthorized holder of a lost or stolen card could readily obtain the cardholder’s name and account number from public sources (e.g., mail theft, data breaches, or skimming devices), so name and account number alone would not always reliably confirm that the presenter is the authorized user. EX1004, 13:22-24, 13:30-32; EX1003, ¶¶105-118. Bjorn’s key, by contrast, is derived from the user’s fingerprint rather than the card. This key uniquely identifies the authorized user in a way not obtainable by an unauthorized holder, as it supplies an identifier not otherwise available from the card, better ensuring MBC

will not authorize a transaction unless the presenter is the authorized user. EX1004, 13:22-24; EX1006, 4:28-30; EX1003, ¶¶105-118.

The combination also would have been obvious considering that Maes and Bjorn also each independently teach fingerprint-based authentication. EX1003, ¶¶105-118. Maes's sensor may collect data from "a finger, thumb or palm print," among other biometrics. EX1004, 5:53-58; see also id., 11:1-5. Bjorn likewise generates its key from fingerprint data. EX1006, Abstract, 1:5-8. Incorporating Bjorn's key thus requires no conceptual departure, it merely uses fingerprint data Maes already collects for an additional, complementary purpose. EX1003, ¶¶105-118.

A POSITA also would have turned to Bjorn because its approach improves security by maintaining no persistent copy of the key on the device EX1006, 4:47-48 ("The cryptographic key itself is not stored anywhere on the system."). The key must instead be produced each time it is required. EX1006, 5:8-12. Regenerating the key only upon successful fingerprint verification advances Maes's aim of biometric security that "protects against the unauthorized access to the user's financial and personal information" and reduces the risk of the key leaking. EX1004, 4:9-10; EX1003, ¶¶105-118.

Maes's enrollment process already stores biometric data including fingerprint data at the central server. EX1004, 7:24-31, 5:53-59. A POSITA would have

understood that enrolling a fingerprint template as Bjorn teaches requires no change to Maes's architecture. EX1004, 5:56-59, 7:28-31; EX1006, 3:14-15; EX1003, ¶¶105-118. In MBC, Maes's POS terminal transmits the encrypted file to the institution, where comparison and verification take place, with the template stored there, as Bjorn teaches may be "a database, or other more centralized location." EX1004, 13:34-38, 13:22-24; EX1006, 4:47, 4:51-53; EX1003, ¶¶105-118.

Bjorn teaches that hashing the stored template reproduces the same key. EX1006, 5:10-12 ("[T]he template is again hashed to create a cryptographic key," and "[s]ince the template was used to generate the first cryptographic key, the same key is generated."); EX1003, ¶¶105-118. In MBC, consistent with Bjorn's teachings, the PDA regenerates the key from the template for inclusion in the encrypted information file, so that the financial institution may compare the regenerated key from the file to the reference key to verify that the user engaged in the transaction is the authorized user associated with the account. EX1004, 13:34-38; EX1006, 5:10-12, 4:28-30; EX1003, ¶¶105-118. A POSITA thus would have been motivated to generate a key for inclusion in Maes's information file according to Bjorn's techniques because Bjorn's techniques allow the key to be accurately regenerated at the PDA despite potential variations in the fingerprint read by the device at the point of sale, such that the financial institution can perform a straightforward comparison

between the new key and the reference key to reliably verify the user's identity. EX1004, 2:1-13, 12:61-63; EX1003, ¶¶105-118.

A POSITA would have been further motivated to integrate Bjorn's techniques because its key is fully functional in standard cryptographic operations, including encryption and decryption already contemplated by Maes. EX1003, ¶¶105-118. Bjorn confirms that its fingerprint-derived key can serve as a private key in a public-key cryptosystem to sign or encrypt documents, generated using well-known functions such as MD5. EX1006, 3:56-58, 4:31-33, 4:36-45. This is significant because Maes's system relies on encryption to safeguard a variety of information. EX1004, 9:52-56, 11:29-34, 10:11-14; *see also id.*, 5:15-19. A POSITA would have selected Bjorn's key for these operations, since the key can only be regenerated upon successful fingerprint verification, ensuring decryption of the digital certificate occurs only upon a matching fingerprint. EX1006, 5:1-13; EX1004, 3:31-40, 9:52-56; EX1003, ¶¶105-118.

A POSITA would have reasonably expected success. EX1003, ¶¶105-118. Maes and Bjorn are directed to the same field of secure electronic transactions employing biometric authentication and cryptographic techniques, and each uses conventional components (*e.g.*, fingerprint sensors, hash functions such as MD5, and standard encryption/decryption modules). *See* EX1006, 3:24-35, 3:44-58, 4:19-20; EX1004, 5:15-19, 10:11-14.

3. Claim Element Analysis

(a) [1.pre]

The Maes-Bjorn Combination (“MBC”) described above (*supra*, §V.C.2) renders [1.pre] obvious in view of Maes’s disclosures for at least the reasons addressed above in Ground 1A. *Supra*, Ground 1A at [1.pre]; EX1003, ¶233.

(b) [1.1]

Supra, Ground 1A at [1.1]; EX1003, ¶234.

(c) [1.2.1]

MBC renders [1.2.1] obvious. EX1003, ¶¶235-237.

As discussed, per Maes, the memory of the PDA (*mobile device*) is coupled to the *short-range RF circuitry* and is configured to store credit card information (*payment information*) for use in transactions. EX1004, 5:8-24, 7:1-7; *supra*, Ground 1A at [1.2.1]; EX1003, ¶236.

Further, in MBC, per Bjorn, the information stored in memory further includes a “fingerprint template” representing an authorized user’s fingerprint scan. EX1006, 4:21-24 (“At block 320, a template is created for the user.”), 4:47-53 (“At block 335, the template is stored.”), Fig. 3; *see also* 5:31-39, 5:49-54, Fig. 4. Bjorn describes various information that can be included in the fingerprint template, each of which renders obvious the claimed “*biometric authentication information*,”

including “a digital image of the fingerprint.” EX1006, 8:32-34; *see also id.*, 14:3-4 (“comparing the fingerprint image to the fingerprint template”).⁵

(d) [1.2.2]

Supra, Ground 1A at [1.2.2]; EX1003, ¶238.

(e) [1.3]

Supra, Ground 1A at [1.3]; EX1003, ¶239.

(f) [1.4.1]

Supra, Ground 1A at [1.4.1]; EX1003, ¶240.

(g) [1.4.2]

Supra, Ground 1A at [1.4.2]; EX1003, ¶241.

(h) [1.5.1]

Supra, Ground 1A at [1.5.1]; EX1003, ¶242.

⁵ For embodiments where the fingerprint template is a “digital image of the fingerprint,” a POSITA would have understood that Bjorn’s processes described with respect to Figs. 3-4 could omit extracting features from the fingerprint. It would have been obvious to a POSITA in this case to perform a comparison between the received fingerprint (blocks 340/450) and the fingerprint image in the stored template (blocks 345/455). EX1006, 8:32-34, 14:3-4.

(i) [1.5.2]

Supra, Ground 1A at [1.5.2]; EX1003, ¶243.

(j) [1.6]

Supra, Ground 1A at [1.6]; EX1003, ¶244. Additionally, Bjorn describes “the fingerprint is received from user,” which would be received in response to a prompt according to Maes’s teachings. EX1006, 4:60-63 & Fig. 3 (step 340), 5:61-64 & Fig. 4 (step 450).

(k) [1.7]

Supra, Ground 1A at [1.7]; EX1003, ¶245. Additionally, Bjorn describes authenticating the user by comparing data from a current scan of the user’s fingerprint to a stored template, and determining whether they match. EX1006, 4:64-5:9 & Fig. 3 (steps 345, 350), 5:65-6:10 & Fig. 4 (steps 455, 460).

(l) [1.8]

MBC renders [1.8] obvious. EX1003, ¶¶246-250.

Bjorn describes generating a cryptographic **key** in response to authentication. For example, as shown in Fig. 3, Bjorn discloses key generation at step 355 in response to determining a match between the user’s current fingerprint and fingerprint data of an authorized user stored in a template:

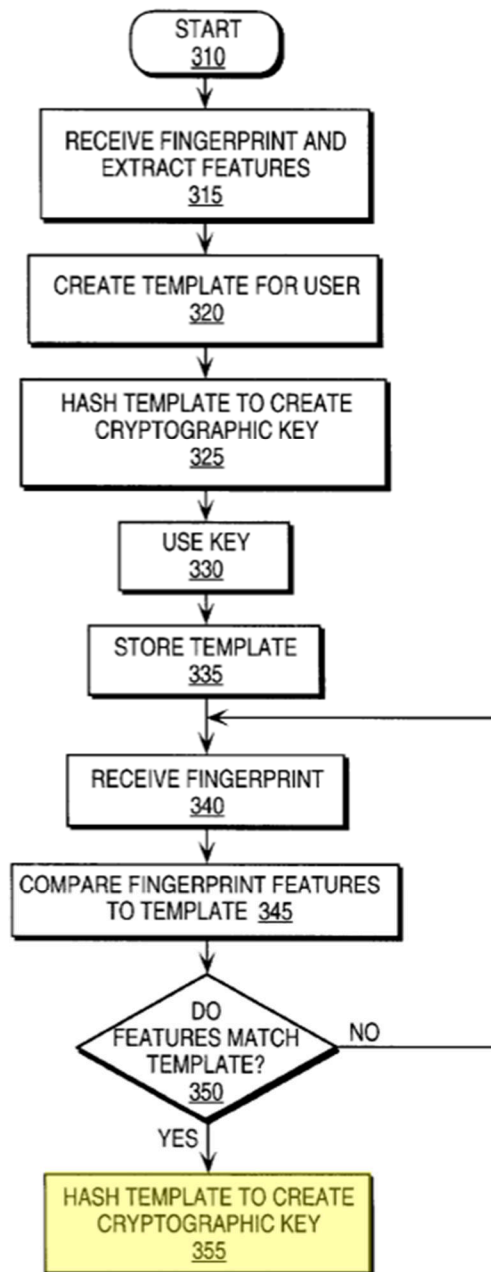


FIG. 3

EX1006, Fig. 3 (annotated)

See also EX1006, 4:60-5:13, 5:61-6:23 & Fig. 4; *supra*, §V.C.1.

Bjorn does not store or otherwise retain the cryptographic key: “[t]he cryptographic key itself is not stored anywhere on the system.” EX1006, 4:47-48).

Instead, the key is produced when needed, and only in response to successfully authenticating the user based on a fingerprint match. EX1006, 5:8-12; EX1003, ¶249.

As addressed in detail above (*supra*, §V.C.2), it would have been obvious to implement Maes in accordance with Bjorn's teachings regarding generation of a cryptographic key based on biometric information. EX1003, In MBC, Bjorn's key generation is triggered by local biometric verification consistent with Maes's biometric verification on the PDA, and as similarly described with respect to Figs. 3 and 4 of Bjorn (*e.g.*, blocks 340-355 and 450-470). EX1006, 5:3-12, Figs. 3-4; EX1004, 5:54-57, 11:9-13; *supra*, §V.C.2; EX1003, ¶250.

(m) [1.9]

Supra, Ground 1A at [1.9]; EX1003, ¶251.

(n) [1.10]

MBC renders [1.8] obvious. EX1003, ¶¶252-254.

For example, Maes discloses the PDA transmitting the selected card information (***payment information***) to a POS terminal via short-range RF circuitry for use in a secure transaction: "The selected card information[] ... would be transmitted to the POS terminal (via ... RF ...) and then transmitted in encrypted form directly to the processing financial institution together with the purchase details" (EX1004, 13:34-38); "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 ... via the ... RF port 50” (EX1004, 12:5-29, Figs. 3, 5). Maes further discloses that the information transmitted via RF from the PDA to the POS terminal can include an “encrypted information file” that “contain[s] unique identifying information pertaining to the consumer” for use in validating consumer in the transaction. EX1004, 13:24-38.

For the reasons addressed in detail above (*supra*, §V.C.2), it would have obvious to include a cryptographic key (*key*), generated in accordance with Bjorn’s techniques and in response to the authentication, in the “encrypted information” that Maes teaches is transmitted from the PDA to the POS terminal via RF. *Supra*, §V.C.2, IV.A; EX1003, ¶254. In MBC, the PDA thus transmits to the POS device via RF both Bjorn’s cryptographic key (*key*) in the encrypted information file and the selected card information (*payment information*) for use in the transaction. *Id.* The selected card information remains secure at least insofar as it is transmitted in encrypted form⁶ and insofar as it is protected by other security measures such as

⁶ For example, Maes discloses that “the PDA device 10 can be programmed to download the selected card information in encrypted form” and “then transmitted in

biometric verification and digital certificate conditions that render the card information ineffective to complete a transaction if the biometric verification is unsuccessful and/or if the digital certificate is expired or its other conditions are not satisfied. EX1004, 9:65-10:17, 11:18-27, 13:24-39. The transaction is likewise secured by these and related measures described in Maes and Bjorn. *Id.*

(o) [2]

Supra, Ground 1A at [2]; EX1003, ¶255.

(p) [3]

Supra, Ground 1A at [3]; EX1003, ¶256.

encrypted form directly to the processing financial institution.” EX1004, 13:24-39. This stands in contrast to other embodiments where the card information is first decrypted. *See e.g., id.*, 11:27-35. For RF transmission, the encrypted card information would be transmitted from the PDA rather than the Universal Card. *Id.*, 12:5-29, 13:36; *supra*, Footnote **Error! Bookmark not defined.** Transmitting card information in encrypted form was also well known and would have been obvious to secure the transaction against unauthorized actors. EX1003, ¶254 (corroborated by EX1005, 5:67-6:4).

D. Ground 3A: Maes-Walker Renders Obvious Claims 1-7

1. Walker (EX1007)

Walker discloses a portable smart card device for generating transaction-specific, single-use credit card numbers to enhance security in credit card transactions. EX1007, Abstract, 1:6-10, 5:49-60, 6:61-7:3, 7:37-45, 8:9-36, 10:10-21, Figs. 1, 8; EX1003, ¶119.

2. The Maes-Walker Combination

The Maes-Walker Combination (“MWC”) implements Maes’s biometrically verified RF-based transactions with a single-use credit card number as taught in Walker.⁷ EX1003, ¶¶120-125. A POSITA would have been motivated to integrate Walker’s single-use credit card numbers into Maes’s RF-based system because (1) Maes expressly seeks to protect against unauthorized card use yet still transmits static card information in the clear over an RF link, leaving it vulnerable to interception and (2) Walker’s single-use number directly solves this vulnerability by preventing reuse or replay of intercepted data, reflecting the predictable application of a known technique to improve a similar device in the same way, with a predictable

⁷ In MWC, Walker supplies teachings that render obvious claims 4-7 and their additional limitations directed to the POS device and central database regardless of whether Walker’s single-use numbers are applied in the combination.

benefit. A POSITA would have reasonably expected success given that the underlying cryptographic techniques were well known before the critical date. EX1004, 2:1-5, 6:24-29, 12:19-34; EX1007, 2:55-64, 3:59-64, 6:30-38, 6:61-7:3, 7:36-45, 10:10-21; EX1003, ¶¶120-125.

3. Claim Element Analysis

(a) [1.pre]

The Maes-Walker Combination (“MWC”) described above (*supra*, §V.D.2) renders [1.pre] obvious in view of Maes’s disclosures for the reasons addressed above in Ground 1A. *Supra*, Ground 1A at [1.pre]; EX1003, ¶257.

(b) [1.1]

Supra, Ground 1A at [1.1]; EX1003, ¶258.

(c) [1.2.1]

Supra, Ground 1A at [1.2.1]; EX1003, ¶259. Walker further discloses ***payment information*** in the form of a credit card account number A stored in memory of a user device. EX1007, 1:20-21, 6:54-59, 6:66-7:1, 8:19-20, Fig. 8 (step 803); *see also id.*, 7:49-61, Fig. 1.

(d) [1.2.2]

Supra, Ground 1A at [1.2.2]; EX1003, ¶260.

(e) [1.3]

Supra, Ground 1A at [1.3]; EX1003, ¶261.

(f) [1.4.1]

Supra, Ground 1A at [1.4.1]; EX1003, ¶262.

(g) [1.4.2]

Supra, Ground 1A at [1.4.2]; EX1003, ¶263.

(h) [1.5.1]

Supra, Ground 1A at [1.5.1]; EX1003, ¶264.

(i) [1.5.2]

Supra, Ground 1A at [1.5.2]; EX1003, ¶265.

(j) [1.6]

Supra, Ground 1A at [1.6]; EX1003, ¶266.

(k) [1.7]

Supra, Ground 1A at [1.7]; EX1003, ¶267.

(l) [1.8]

MWC renders [1.8] obvious. EX1003, ¶¶268-272.

In MWC, Maes's PDA generates and transmits, in response to successful biometric authentication, a Walker-based single-use credit card number, formed by encrypting a nonce N with a private key K and initialization variable IV, and concatenating the resulting encrypted nonce C with the IV and account number A, such that the encrypted nonce C (or, alternatively, the entire single-use number including C) provides a “*key*” that the financial institution uses to authorize or deny

the transaction. EX1004, 9:52-10:5, 10:49-56, 11:15-19, 12:20-27, 12:40-52, 12:65-67; EX1007, 5:58-61, 6:15-27, 6:56-7:20, 8:9-19, 8:41-9:10, 11:46-52, Figs. 3B, 7, 8, 9A-9B; EX1003, ¶¶269-272; EX1002, 324, 387. Walker's single-use number directly embeds the user's credit card account number A. *Id.*

(m) [1.9]

MWC renders [1.9] obvious. EX1003, ¶¶273-275.

Maes discloses that the PDA “includes a memory for storing financial and personal information of the user” and that “selected card information is retrieved from memory 14 and decrypted (step 314)” prior to being furnished for the transaction. EX1004, 12:43-49. In MWC, per Maes, the payment information (*e.g.*, account number A for a selected credit card) is thus secured in memory through encryption. EX1003, ¶274; *see also supra*, Ground 1A at [1.9].

Per Walker, the account number A is also secured by virtue of being rendered useless without a validly paired encrypted nonce and IV, and by being stored in memory in connection with a valid nonce and IV and associated private key. EX1003, ¶275. *See e.g.*, EX1007, 7:1-3 (“knowledge of the account number does not allow an attacker to generate a valid single-use credit card number”), 6:61-7:1, 7:28-36, Figs. 1, 9A-9B.

(n) [1.10]

MWC renders [1.10] obvious. EX1003, ¶¶276-277.

As discussed above in the overview of MWC and in connection with [1.8], MWC's PDA generates and transmits to a POS terminal, in response to biometric authentication of the user, a single-use card number generated in accordance with Walker's teachings, where an encrypted nonce C (*key*) and an account number A for the selected credit card (*secured payment information*) are both included in the single-use card number (alternate *key*). EX1004, 12:5-29 ("transmitting the selected card information directly from the PDA device to the ... POS transaction terminal" via RF), 13:34-38; EX1007, 7-3:8 ("single-use credit card number is transmitted to a merchant"), 8:31-36, 8:19-25; *supra*, Ground 3A at [1.8]; §V.D.2; EX1003, ¶277. As discussed, the secured account number A in the transmitted single-use number includes at least credit card information. EX1007, 1:20-21, 6:54-59, 6:66-7:1; EX1003, ¶277; *supra*, [1.2.1].

(o) [2]

Supra, Ground 1A at [2]; EX1003, ¶278. Walker further discloses that the account number A can be "an unchanging identifier for the cardholder which is stored in a database maintained by the card issuer" and that the single-use number "is preferably a 16-digit number that can be recognized as a conventional credit card number." EX1007, 7:54-59, 6:35-38, 6:66-7:1; EX1003, ¶278.

(p) [3]

Supra, Ground 1A at [3]; EX1003, ¶279.

(q) [4.pre]

Supra, Ground 1A at [1.pre]; EX1003, ¶¶280-281.

Maes discloses a system that includes at least a mobile device (*e.g.*, PDA), a merchant's POS terminal, and server(s) of a service provider and/or financial institution. EX1004, Fig. 1; *supra*, §V.A.1; In the combination, Walker further discloses a system comprising a user device (*e.g.*, device 100), a POS terminal, and server(s) of a financial institution such as a card issuer. EX1007, 5:3-13, 6:4-14, Figs. 1, 2, 3A, 4; EX1003, ¶281.

(r) [4.1]

Supra, Grounds 1A/3A at [1.pre]-[1.1]; EX1003, ¶282.

(s) [4.2.1]

Supra, Grounds 1A/3A at [1.2.1]; EX1003, ¶283.

(t) [4.2.2]

Supra, Grounds 1A/3A at [1.2.2]; EX1003, ¶284.

(u) [4.3]

Supra, Grounds 1A/3A at [1.3]; EX1003, ¶285.

(v) [4.4.1]

Supra, Grounds 1A/3A at [1.4.1]; EX1003, ¶286.

(w) [4.4.2]

Supra, Grounds 1A/3A at [1.4.2]; EX1003, ¶287.

(x) [4.5.1]

Supra, Grounds 1A/3A at [1.5.1]; EX1003, ¶288.

(y) [4.5.2]

Supra, Grounds 1A/3A at [1.5.1]-[1.5.2]; EX1003, ¶289.

(z) [4.6]

Supra, Grounds 1A/3A at [1.6]; EX1003, ¶290.

(aa) [4.7]

Supra, Grounds 1A/3A at [1.7]; EX1003, ¶291.

(bb) [4.8]

Supra, Grounds 1A/3A at [1.8]; EX1003, ¶292.

(cc) [4.9]

Supra, Grounds 1A/3A at [1.9]; EX1003, ¶293.

(dd) [4.10]

Supra, Grounds 1A/3A at [1.10]; EX1003, ¶294.

(ee) [4.11]

MWC renders [4.11] obvious. EX1003, ¶¶295-298.

Maes discloses a POS terminal (***POS device***) that receives, processes, and transmits information electronically for a transaction. *See e.g.*, EX1004, 12:5-9, 11:41-43, Fig. 3; EX1003, ¶296. Walker similarly describes a “merchant’s

authorization terminal” and references a “MERCHANT’s CENTRAL PROCESSOR.” EX1007, 6:49-50, Figs. 3A (merchant 302), 4, 12.

Walker further expressly discloses devices implemented with a conventional program-execution architecture, in which the CPU executes instructions stored in memory to perform the device’s operations. EX1007, 5:63-6:3; *id.* at 7:10-17, Figs. 3A, 4. It would have been obvious to implement Maes’s POS terminal (*POS device*) in MWC according to this conventional program-execution architecture as taught in Walker as this configuration would have beneficially enabled the POS terminal to achieve its disclosed processing functions using widely available electronics/computing hardware. EX1003, ¶297. Indeed, Maes explicitly describes a similar structure for the PDA. EX1004, 5:1-4, Fig. 1; *supra*, Ground 1A at [1.4.2].

(ff) [4.12]

MWC renders [4.12] obvious. EX1003, ¶¶299-300.

As discussed above with respect to [1.10] in each of Grounds 1A and 3A, Maes and Maes-Walker render obvious the PDA (*mobile device*) transmitting the secured payment information and the key to the POS terminal (*POS device*) such that POS terminal receives the secured payment information and the key. EX1004, 12:5-29, 13:19-38, Fig.3; *supra*, Ground 1A at [1.10], Ground 3A at [1.10]; EX1003, ¶300.

(gg) [4.13]

MWC renders [4.13] obvious. EX1003, ¶¶301-303.

For example, Maes discloses that “[t]he merchant will [] transmit ... the displayed authorization number to the central server 60.” EX1004, 12:65-13:5. Additionally, “[t]he selected card information ... would be transmitted to the POS terminal ... and then transmitted in encrypted form directly to the processing financial institution together with the purchase details”; *see also id.*, Fig. 3, 12:55-63, 11:38-43. In MWC, the POS terminal receives the authorization number directly from the PDA over an RF link, and thus transmits the authorization number to the central server 60. *Supra*, §§V.D.2, V.A.2.[1.10].

MWC’s POS terminal transmits the *secured payment information* (e.g., Maes’s selected card information in first mapping; Walker’s account number A in second mapping) and the *key* (e.g., Maes’s authorization number in first mapping; Walker’s encrypted nonce C per in second mapping) to a *central database* of the central server 60 and financial institution 70. *Supra*, Ground 1A at [1.8], [1.10]; Ground 3A at [1.8], [1.10]; *infra*, [4.14]; EX1003, ¶303.

(hh) [4.14]

MWC renders [4.14] obvious. EX1003, ¶¶304-306.

Maes’s central server 60 together with financial institution 70 provide a “*central database*” as claimed. EX1003, ¶305. To the extent the “*central database*”

is a single entity, consolidating the functions of Maes's central server 60 and financial institution 70 into a single database system would have been obvious to achieve well known and predictable benefits of centralization, including lower overhead costs, reduced coordination costs, and reduced latency in communicating between otherwise distant systems. *Id.*; *KSR*, 550 U.S. at 416 (“the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results”); *In re Larson*, 340 F.2d 965, 968 (CCPA 1965) (consolidation of separate components is “merely a matter of obvious engineering choice”); EX1003, ¶305.

Further, per Walker's teachings, it would have been obvious for the central database in MWC (*e.g.*, central server 60/financial institution 70) to include a processor (*e.g.*, central processing unit (CPU)) and memory (*e.g.*, ROM 404, RAM 403). EX1007, 7:9-26, 7:20-45, Figs. 5-7. The memory device can store “a program adapted to be executed by the processing unit.” *Id.*, 4:28-31; EX1003, ¶306. This would have been obvious given that Maes explicitly describes a similar structure for the PDA. EX1004, 5:1-4, Fig. 1; *supra*, Ground 1A at [1.4.2].

(ii) [4.15]

MWC renders [4.15] obvious. EX1003, ¶¶307-309.

For example, Maes discloses that “[t]he merchant will [] transmit ... the displayed authorization number to the central server 60.” EX1004, 12:65-13:5.

Additionally, “[t]he selected card information ... would be transmitted to the POS terminal ... and then transmitted in encrypted form directly to the processing financial institution together with the purchase details”; *see also id.*, Fig. 3, 12:55-63, 11:38-43.

The central server 60 and financial institution 70 (*central database*) thus receive from the POS the *secured payment information* (e.g., the selected card information in first mapping; account number A in second mapping) and the *key* (e.g., authorization number per Maes in first mapping; encrypted nonce C per Walker when the single-use number is used in second mapping). *Supra*, Ground 1A at [1.8], [1.10]; Ground 3A at [1.8], [1.10]; EX1003, ¶309.

(jj) [4.16]

MWC renders [4.16] obvious. EX1003, ¶¶310-312.

For implementations involving use of Maes’s authorization number, Maes’s discloses central server 60 validates the authorization number to confirm that the user was properly verified at the PDA device 10. EX1004, 12:65-13:5; *see also id.*, 12:55-13:5, Fig. 3. Financial institution 70 validates the transmitted card information by decrypting it using an account-specific key and returns an authorization to the merchant if the user is verified, completing the secured transaction. EX1004, 13:47-56.

For implementations involving use of Walker's single-use number, Walker discloses the issuer validating the encrypted nonce C (**key**) and the account number (**secured payment information**) to complete the secured transaction. EX1007, 8:36-9:3, Figs. 9A-9B; EX1003, ¶312.

(kk) [5]

Supra, Grounds 1A & 3A at [2]; EX1003, ¶313.

(ll) [6]

MWC renders [6] obvious. EX1003, ¶¶314-316.

For example, Maes discloses that the PDA and POS device communicate over an RF link, and that the PDA transmits information for a transaction received by the PDA via RF. EX1004, 3:34-37, 6:8-15, 7:66-8:11, 12:5-29, 13:34-38, Abstract. From these disclosures, a POSITA would have understood the merchant's terminal (**POS device**) to include an RF reader. EX1003, ¶315. Indeed, an RF reader would be inherent or obvious for the POS device to receive the information that Maes expressly discloses is transmitted to the POS device from the PDA via RF. *Id.*, citing EX1008, EX1039.

(mm) [7]

Supra, Grounds 1A/3A at [3]; EX1003, ¶317.

**E. Ground 3B: Maes-Niwa-Walker Renders Obvious Claims
4-7**

The Maes-Niwa-Walker Combination (MNWC) further modifies the Maes-Niwa Combination (MNC) from Ground 1B (*supra*, §V.B) in view of Walker by integrating in MNC Walker’s teachings regarding details of a POS device and central database as discussed above in Ground 3A with respect to the Maes-Walker Combination (MWC). *Supra*, §V.D. It would have been obvious to implement MNWC for at least the reasons addressed above in Ground 3A (*supra*, §V.D.2), and MNWC would have rendered obvious claims 4-7 and their constituent elements for at least the reasons addressed above with respect to elements [4.11.1]-[4.16] in Ground 3A (*supra*, §V.D.3).⁸ EX1003, ¶¶126, 318.

**F. Ground 3C: Maes-Bjorn-Walker Renders Obvious Claims
4-7**

The Maes-Bjorn-Walker Combination (MBWC) further modifies the Maes-Bjorn Combination (MBC) from Ground 2 (*supra*, §V.C) in view of Walker by integrating in MBC Walker’s teachings regarding details of a POS device and central database as discussed above in Ground 3A with respect to the Maes-Walker

⁸ MNWC does not integrate Walker’s teachings regarding a single-use credit card number. MNWC instead relies on Maes’s authorization number as the claimed “key” as detailed above in Ground 1A. EX1003, ¶318.

Combination (MWC). *Supra*, §V.D. It would have been obvious to implement MBWC for at least the reasons addressed above in Ground 3A (*supra*, §V.D.2), and MBWC would have rendered obvious claims 4-7 and their constituent elements for at least the reasons addressed above with respect to elements [4.11.1]-[4.16] in Ground 3A (*supra*, §V.D.3).⁹ EX1003, ¶¶126, 319.

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 '412 Patent. The '412 Patent is the subject of civil actions *Mobility IP Holdings, Inc. v. Apple Inc.*, No. 7:26-cv-00075 (W.D. Tex.

⁹ MBWC does not integrate Walker's teachings regarding a single-use credit card number. MBWC instead relies on Maes's authorization number as the claimed "key" as detailed above in Ground 1A. EX1003, ¶319.

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: IPR50095-0310IP1@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 IPR50095-0310IP1@fr.com

D. Service Information

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

Petitioners consent to electronic service by email at IPR50095-0310IP1@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. IPR2026-00501)

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 13,966 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